



CryptoAuthLib

v3.7.5

---

<b>1 CryptoAuthLib - Microchip CryptoAuthentication Library</b>	<b>1</b>
1.1 Introduction	1
1.2 Examples	2
1.3 Configuration	2
1.4 Release notes	3
1.5 Host Device Support	3
1.6 CryptoAuthLib Architecture	3
1.7 Directory Structure	3
1.8 Tests	3
1.9 Using CryptoAuthLib (Microchip CryptoAuth Library)	4
1.9.1 Incorporating CryptoAuthLib in a Linux project using USB HID devices	4
<b>2 License</b>	<b>5</b>
<b>3 IP Protection with Symmetric Authentication</b>	<b>7</b>
3.1 User Considerations	7
3.2 Examples	7
<b>4 PKCS11 Application Information</b>	<b>9</b>
4.1 Setting up cryptoauthlib as a PKCS11 Provider for your system (LINUX)	9
4.1.1 Update libp11 on the system. The version should be at minimum 0.4.10	9
4.1.2 Build and Install cryptoauthlib with PKCS11 support	10
4.1.3 Configuring the cryptoauthlib PKCS11 library	10
4.1.4 Using p11-kit-proxy	11
4.1.5 Without using p11-kit-proxy	11
4.1.6 Testing	12
<b>5 Application Support</b>	<b>13</b>
<b>6 Secure boot using ATECC608</b>	<b>15</b>
6.1 Implementation Considerations	16
6.2 Examples	16
<b>7 Contribution Guidelines</b>	<b>17</b>
<b>8 openssl directory - Purpose</b>	<b>19</b>
<b>9 Python CryptoAuthLib module</b>	<b>21</b>
9.1 Introduction	21
9.1.1 Code Examples	21
9.2 Installation	21
9.2.1 CryptoAuthLib python module can be installed through Python's pip tool:	21
9.2.2 To upgrade your installation when new releases are made:	21
9.2.3 If you ever need to remove your installation:	21
9.3 What does python CryptoAuthLib package do?	21

9.4 Supported hardware . . . . .	22
9.5 Supported devices . . . . .	22
9.6 Using cryptoauthlib python module . . . . .	22
9.7 In Summary . . . . .	23
9.7.1 Step I: Import the module . . . . .	23
9.7.2 Step II: Initilize the module . . . . .	23
9.7.3 Step III: Use Cryptoauthlib APIs . . . . .	23
9.8 Code portability . . . . .	23
9.9 Cryptoauthlib module API documentation . . . . .	23
9.9.1 help() command . . . . .	23
9.9.2 dir() command . . . . .	23
9.10 Code Examples . . . . .	23
9.11 Tests . . . . .	24
9.12 Release notes . . . . .	24
<b>10 Python CryptoAuthLib Module Testing</b>	<b>25</b>
10.1 Introduction . . . . .	25
10.1.1 Running . . . . .	25
10.1.2 Test options . . . . .	25
<b>11 Microchip Cryptoauthlib Release Notes</b>	<b>27</b>
11.1 Release v3.7.5 (06/26/2024) . . . . .	27
11.1.1 New Features . . . . .	27
11.1.2 Fixes . . . . .	27
11.1.3 API Changes . . . . .	27
11.2 Release v3.7.4 (03/08/2024) . . . . .	28
11.2.1 New Features . . . . .	28
11.2.2 Fixes . . . . .	28
11.3 Release v3.7.3 (01/31/2024) . . . . .	28
11.3.1 New Features . . . . .	28
11.3.2 Fixes . . . . .	28
11.4 Release v3.7.2 (01/19/2024) . . . . .	28
11.4.1 New Features . . . . .	28
11.4.2 Fixes . . . . .	29
11.4.3 API Changes . . . . .	29
11.5 Release v3.7.1 (12/15/2023) . . . . .	29
11.5.1 New Features . . . . .	29
11.5.2 Fixes . . . . .	29
11.5.3 API Changes . . . . .	29
11.6 Release v3.7.0 (09/08/2023) . . . . .	29
11.6.1 New Features . . . . .	29
11.6.2 Fixes . . . . .	30
11.6.3 API Changes . . . . .	30

11.7 Release v3.6.1 (07/14/2023)	30
11.7.1 New Features	30
11.7.2 Fixes	30
11.8 Release v3.6.0 (04/04/2023)	30
11.8.1 New Features	30
11.8.2 Fixes	31
11.8.3 API Changes	31
11.9 Release v3.5.1 (03/26/2023)	31
11.9.1 New Features	31
11.10 Release v3.5.0 (03/14/2023)	31
11.10.1 New Features	31
11.11 Release v3.4.3 (12/23/2022)	31
11.11.1 New Features	31
11.11.2 Fixes	31
11.12 Release v3.4.2 (12/04/2022)	32
11.12.1 Fixes	32
11.13 Release v3.4.1 (11/11/2022)	32
11.13.1 Fixes	32
11.14 Release v3.4.0 (10/27/2022)	32
11.14.1 New Features	32
11.14.2 Fixes	33
11.15 Release v3.3.3 (10/06/2021)	33
11.15.1 New features	33
11.15.2 Fixes	33
11.16 Release v3.3.2 (06/20/2021)	33
11.16.1 New features	33
11.16.2 Fixes	34
11.17 Release v3.3.1 (04/23/2021)	34
11.17.1 New features	34
11.17.2 Fixes	34
11.18 Release v3.3.0 (01/22/2021)	34
11.18.1 API Updates	34
11.18.2 New features	35
11.18.3 Fixes	35
11.19 Release v3.2.5 (11/30/2020)	35
11.19.1 New features	35
11.19.2 Fixes	35
11.20 Release v3.2.4 (10/17/2020)	35
11.20.1 New features	35
11.20.2 Fixes	36
11.21 Release v3.2.3 (09/12/2020)	36
11.21.1 New features	36

11.21.2 Fixes	36
11.22 Release v3.2.2 (07/28/2020)	36
11.22.1 New Features	36
11.22.2 Fixes	36
11.23 Release v3.2.1 (06/29/2020)	36
11.23.1 Fixes	36
11.24 Release v3.2.0 (06/10/2020)	37
11.24.1 New features	37
11.24.2 Known issues	37
11.25 Release v3.1.1 (03/06/2020)	37
11.26 Release v3.1.0 (02/05/2020)	37
11.27 Release 11/22/2019	38
11.28 Release 08/30/2019	38
11.29 Release 05/17/2019	38
11.30 Release 03/04/2019	38
11.31 Release 01/25/2019	38
11.32 Release 01/04/2019	38
11.33 Release 10/25/2018	39
11.34 Release 08/17/2018	39
11.35 Release 07/25/2018	39
11.36 Release 07/18/2018	39
11.37 Release 03/29/2018	39
11.38 Release 01/15/2018	40
11.39 Release 11/22/2017	40
11.40 Release 11/17/2017	40
11.41 Release 07/01/2017	40
11.42 Release 01/08/2016	41
11.43 Release 9/19/2015	42
<b>12 Security Policy</b>	<b>43</b>
12.1 Supported Versions	43
12.2 Reporting a Vulnerability	43
<b>13 Deprecated List</b>	<b>45</b>
<b>14 Module Index</b>	<b>47</b>
14.1 Modules	47
<b>15 Namespace Index</b>	<b>49</b>
15.1 Namespace List	49
<b>16 Hierarchical Index</b>	<b>51</b>
16.1 Class Hierarchy	51

<b>17 Data Structure Index</b>	<b>57</b>
17.1 Data Structures . . . . .	57
<b>18 File Index</b>	<b>63</b>
18.1 File List . . . . .	63
<b>19 Module Documentation</b>	<b>73</b>
19.1 TNG API (tng_) . . . . .	73
19.1.1 Detailed Description . . . . .	74
19.1.2 Function Documentation . . . . .	75
19.2 Basic Crypto API methods (atcab_) . . . . .	80
19.2.1 Detailed Description . . . . .	89
19.2.2 Function Documentation . . . . .	89
19.3 Configuration (cfg_) . . . . .	163
19.4 ATCADevice (atca_) . . . . .	163
19.4.1 Detailed Description . . . . .	164
19.4.2 Function Documentation . . . . .	164
19.5 ATCAIface (atca_) . . . . .	166
19.5.1 Detailed Description . . . . .	168
19.5.2 Enumeration Type Documentation . . . . .	168
19.5.3 Function Documentation . . . . .	168
19.6 Certificate manipulation methods (atcacert_) . . . . .	174
19.6.1 Detailed Description . . . . .	179
19.6.2 Macro Definition Documentation . . . . .	179
19.6.3 Typedef Documentation . . . . .	181
19.6.4 Enumeration Type Documentation . . . . .	182
19.6.5 Function Documentation . . . . .	184
19.7 Basic Crypto API methods for CryptoAuth Devices (calib_) . . . . .	205
19.7.1 Detailed Description . . . . .	209
19.7.2 Function Documentation . . . . .	209
19.8 Software crypto methods (atcac_) . . . . .	216
19.8.1 Detailed Description . . . . .	216
19.9 Hardware abstraction layer (hal_) . . . . .	216
19.9.1 Cryptoauthlib HAL Architecture . . . . .	216
19.9.2 CryptoAuthLib Supported HAL Layers . . . . .	217
19.9.3 Detailed Description . . . . .	223
19.9.4 Macro Definition Documentation . . . . .	223
19.9.5 Function Documentation . . . . .	224
19.10 Host side crypto methods (atcah_) . . . . .	255
19.10.1 Detailed Description . . . . .	260
19.11 JSON Web Token (JWT) methods (atca_jwt_) . . . . .	260
19.12 mbedTLS Wrapper methods (atca_mbedtls_) . . . . .	260
19.12.1 Detailed Description . . . . .	261

19.12.2 Typedef Documentation . . . . .	261
19.12.3 Function Documentation . . . . .	261
19.13 Attributes (pkcs11_attrib_) . . . . .	263
19.13.1 Detailed Description . . . . .	271
19.13.2 Function Documentation . . . . .	271
19.13.3 Variable Documentation . . . . .	273
<b>20 Namespace Documentation</b>	<b>277</b>
20.1 cryptoauthlib Namespace Reference . . . . .	277
20.1.1 Detailed Description . . . . .	277
20.2 cryptoauthlib.atcab Namespace Reference . . . . .	277
20.2.1 Detailed Description . . . . .	280
20.2.2 Function Documentation . . . . .	280
20.3 cryptoauthlib.atcacert Namespace Reference . . . . .	327
20.3.1 Detailed Description . . . . .	327
20.3.2 Function Documentation . . . . .	328
20.4 cryptoauthlib.atcaenum Namespace Reference . . . . .	332
20.4.1 Detailed Description . . . . .	333
20.5 cryptoauthlib.atjwt Namespace Reference . . . . .	333
20.5.1 Detailed Description . . . . .	333
20.6 cryptoauthlib.device Namespace Reference . . . . .	333
20.6.1 Detailed Description . . . . .	333
20.7 cryptoauthlib.exceptions Namespace Reference . . . . .	334
20.7.1 Detailed Description . . . . .	334
20.8 cryptoauthlib.iface Namespace Reference . . . . .	335
20.8.1 Detailed Description . . . . .	335
20.8.2 Function Documentation . . . . .	335
20.9 cryptoauthlib.library Namespace Reference . . . . .	337
20.9.1 Detailed Description . . . . .	338
20.9.2 Function Documentation . . . . .	338
20.10 cryptoauthlib.sha206_api Namespace Reference . . . . .	344
20.10.1 Detailed Description . . . . .	344
20.10.2 Function Documentation . . . . .	344
20.11 cryptoauthlib.status Namespace Reference . . . . .	349
20.11.1 Detailed Description . . . . .	349
20.11.2 Function Documentation . . . . .	349
20.12 cryptoauthlib.tng Namespace Reference . . . . .	350
20.12.1 Detailed Description . . . . .	350
20.12.2 Function Documentation . . . . .	350
20.13 test_device Namespace Reference . . . . .	354
20.13.1 Detailed Description . . . . .	354
20.13.2 Variable Documentation . . . . .	354

20.14 test_iface Namespace Reference . . . . .	356
20.14.1 Detailed Description . . . . .	356
<b>21 Data Structure Documentation</b>	<b>357</b>
21.1 _ascii_kit_host_context Struct Reference . . . . .	357
21.2 cryptoauthlib.iface._ATCACUSTOM Class Reference . . . . .	357
21.2.1 Detailed Description . . . . .	358
21.2.2 Field Documentation . . . . .	358
21.3 cryptoauthlib.iface._ATCAHID Class Reference . . . . .	358
21.3.1 Detailed Description . . . . .	359
21.3.2 Field Documentation . . . . .	359
21.4 cryptoauthlib.iface._ATCAI2C Class Reference . . . . .	359
21.4.1 Detailed Description . . . . .	360
21.4.2 Field Documentation . . . . .	360
21.5 cryptoauthlib.iface._ATCAIfaceParams Class Reference . . . . .	361
21.5.1 Detailed Description . . . . .	361
21.5.2 Field Documentation . . . . .	361
21.6 cryptoauthlib.iface._ATCAKIT Class Reference . . . . .	362
21.6.1 Detailed Description . . . . .	362
21.6.2 Field Documentation . . . . .	362
21.7 cryptoauthlib.iface._ATCASPI Class Reference . . . . .	363
21.7.1 Detailed Description . . . . .	363
21.7.2 Field Documentation . . . . .	363
21.8 cryptoauthlib.iface._ATCASWI Class Reference . . . . .	364
21.8.1 Detailed Description . . . . .	364
21.8.2 Field Documentation . . . . .	364
21.9 cryptoauthlib.iface._ATCAUART Class Reference . . . . .	365
21.9.1 Detailed Description . . . . .	365
21.9.2 Field Documentation . . . . .	365
21.10 cryptoauthlib.library._CtypeIterator Class Reference . . . . .	366
21.10.1 Detailed Description . . . . .	366
21.11 _kit_host_map_entry Struct Reference . . . . .	366
21.11.1 Detailed Description . . . . .	366
21.12 cryptoauthlib.iface._U_Address Class Reference . . . . .	367
21.12.1 Detailed Description . . . . .	367
21.12.2 Field Documentation . . . . .	367
21.13 cryptoauthlib.device.AesEnable Class Reference . . . . .	368
21.13.1 Detailed Description . . . . .	368
21.13.2 Field Documentation . . . . .	368
21.14 cryptoauthlib.exceptions.AssertionFailure Class Reference . . . . .	368
21.14.1 Detailed Description . . . . .	368
21.15 cryptoauthlib.atcab.atca_aes_cbc_ctx Class Reference . . . . .	369



21.15.1 Detailed Description . . . . .	369
21.15.2 Field Documentation . . . . .	369
21.16 <a href="#">cryptoauthlib.atcab.atca_aes_ccmac_ctx Class Reference</a> . . . . .	369
21.16.1 Detailed Description . . . . .	370
21.16.2 Field Documentation . . . . .	370
21.17 <a href="#">cryptoauthlib.atcab.atca_aes_ccm_ctx Class Reference</a> . . . . .	370
21.17.1 Detailed Description . . . . .	370
21.17.2 Field Documentation . . . . .	370
21.18 <a href="#">cryptoauthlib.atcab.atca_aes_cmac_ctx Class Reference</a> . . . . .	371
21.18.1 Detailed Description . . . . .	371
21.18.2 Field Documentation . . . . .	371
21.19 <a href="#">cryptoauthlib.atcab.atca_aes_ctr_ctx Class Reference</a> . . . . .	372
21.19.1 Detailed Description . . . . .	372
21.19.2 Field Documentation . . . . .	372
21.20 <a href="#">cryptoauthlib.atcab.atca_aes_gcm_ctx Class Reference</a> . . . . .	372
21.20.1 Detailed Description . . . . .	373
21.20.2 Field Documentation . . . . .	373
21.21 <a href="#">atca_check_mac_in_out Struct Reference</a> . . . . .	373
21.21.1 Detailed Description . . . . .	374
21.21.2 Field Documentation . . . . .	374
21.22 <a href="#">atca_decrypt_in_out Struct Reference</a> . . . . .	374
21.22.1 Detailed Description . . . . .	374
21.23 <a href="#">atca_delete_in_out Struct Reference</a> . . . . .	374
21.23.1 Detailed Description . . . . .	375
21.24 <a href="#">atca_derive_key_in_out Struct Reference</a> . . . . .	375
21.24.1 Detailed Description . . . . .	375
21.25 <a href="#">atca_derive_key_mac_in_out Struct Reference</a> . . . . .	375
21.25.1 Detailed Description . . . . .	376
21.26 <a href="#">atca_device Struct Reference</a> . . . . .	376
21.26.1 Detailed Description . . . . .	376
21.26.2 Field Documentation . . . . .	376
21.27 <a href="#">atca_diversified_key_in_out Struct Reference</a> . . . . .	377
21.27.1 Detailed Description . . . . .	377
21.28 <a href="#">atca_evp_ctx Struct Reference</a> . . . . .	377
21.29 <a href="#">atca_gen_dig_in_out Struct Reference</a> . . . . .	377
21.29.1 Detailed Description . . . . .	378
21.30 <a href="#">atca_gen_key_in_out Struct Reference</a> . . . . .	378
21.30.1 Detailed Description . . . . .	379
21.31 <a href="#">atca_hal_kit_phy_t Struct Reference</a> . . . . .	379
21.31.1 Field Documentation . . . . .	379
21.32 <a href="#">atca_hal_list_entry_t Struct Reference</a> . . . . .	380
21.32.1 Detailed Description . . . . .	380

21.32.2 Field Documentation	380
21.33 atca_hal_shm_t Struct Reference	380
21.34 atca_hmac_in_out Struct Reference	380
21.34.1 Detailed Description	381
21.35 cryptoauthlib.atcab.atca_hmac_sha256_ctx Class Reference	381
21.35.1 Detailed Description	381
21.36 atca_i2c_host_s Struct Reference	382
21.37 atca_iface Struct Reference	382
21.37.1 Detailed Description	382
21.37.2 Field Documentation	382
21.38 atca_include_data_in_out Struct Reference	383
21.38.1 Detailed Description	383
21.39 atca_io_decrypt_in_out Struct Reference	383
21.40 atca_mac_in_out Struct Reference	383
21.40.1 Detailed Description	384
21.41 atca_mbedtls_eckey_s Struct Reference	384
21.41.1 Detailed Description	384
21.42 atca_nonce_in_out Struct Reference	384
21.42.1 Detailed Description	385
21.43 atca_plib_i2c_api Struct Reference	385
21.44 atca_resp_mac_in_out Struct Reference	385
21.44.1 Detailed Description	386
21.45 atca_secureboot_enc_in_out Struct Reference	386
21.46 atca_secureboot_mac_in_out Struct Reference	386
21.47 atca_session_key_in_out Struct Reference	386
21.47.1 Detailed Description	387
21.48 atca_sha256_ctx Struct Reference	387
21.49 cryptoauthlib.atcab.atca_sha256_ctx Class Reference	387
21.49.1 Detailed Description	387
21.49.2 Field Documentation	388
21.50 atca_sign_internal_in_out Struct Reference	388
21.50.1 Detailed Description	389
21.51 atca_spi_host_s Struct Reference	389
21.52 atca_temp_key Struct Reference	389
21.52.1 Detailed Description	389
21.53 atca_uart_host_s Struct Reference	390
21.54 atca_verify_in_out Struct Reference	390
21.54.1 Detailed Description	390
21.55 atca_verify_mac Struct Reference	390
21.56 atca_write_mac_in_out Struct Reference	391
21.56.1 Detailed Description	391
21.57 cryptoauthlib_mock.atcab_mock Class Reference	391

21.58 atcac_aes_cmac_ctx Struct Reference . . . . .	396
21.59 atcac_aes_gcm_ctx Struct Reference . . . . .	396
21.60 atcac_hmac_ctx Struct Reference . . . . .	396
21.61 atcac_pk_ctx Struct Reference . . . . .	396
21.62 atcac_sha1_ctx Struct Reference . . . . .	396
21.63 atcac_sha2_256_ctx Struct Reference . . . . .	396
21.64 atcac_x509_ctx Struct Reference . . . . .	397
21.65 atcacert_build_state_s Struct Reference . . . . .	397
21.65.1 Detailed Description . . . . .	397
21.66 atcacert_cert_element_s Struct Reference . . . . .	397
21.66.1 Detailed Description . . . . .	398
21.67 cryptoauthlib.atcacert.atcacert_cert_element_t Class Reference . . . . .	398
21.67.1 Detailed Description . . . . .	399
21.67.2 Field Documentation . . . . .	399
21.68 atcacert_cert_loc_s Struct Reference . . . . .	399
21.68.1 Detailed Description . . . . .	399
21.69 cryptoauthlib.atcacert.atcacert_cert_loc_t Class Reference . . . . .	399
21.69.1 Detailed Description . . . . .	400
21.70 cryptoauthlib.atcacert.atcacert_cert_sn_src_t Class Reference . . . . .	400
21.70.1 Detailed Description . . . . .	401
21.71 cryptoauthlib.atcacert.atcacert_cert_type_t Class Reference . . . . .	401
21.71.1 Detailed Description . . . . .	402
21.72 cryptoauthlib.atcacert.atcacert_comp_data_t Class Reference . . . . .	402
21.72.1 Detailed Description . . . . .	402
21.72.2 Field Documentation . . . . .	403
21.73 cryptoauthlib.atcacert.atcacert_date_format_t Class Reference . . . . .	403
21.73.1 Detailed Description . . . . .	404
21.74 atcacert_def_s Struct Reference . . . . .	404
21.74.1 Detailed Description . . . . .	404
21.75 cryptoauthlib.atcacert.atcacert_def_t Class Reference . . . . .	404
21.75.1 Detailed Description . . . . .	405
21.76 atcacert_device_loc_s Struct Reference . . . . .	405
21.76.1 Detailed Description . . . . .	405
21.77 cryptoauthlib.atcacert.atcacert_device_loc_t Class Reference . . . . .	405
21.77.1 Detailed Description . . . . .	406
21.77.2 Field Documentation . . . . .	406
21.78 cryptoauthlib.atcacert.atcacert_device_zone_t Class Reference . . . . .	406
21.78.1 Detailed Description . . . . .	407
21.79 cryptoauthlib.atcacert.atcacert_std_cert_element_t Class Reference . . . . .	407
21.79.1 Detailed Description . . . . .	408
21.80 atcacert_tm_utc_s Struct Reference . . . . .	408
21.80.1 Detailed Description . . . . .	408

21.81	<a href="#">cryptoauthlib.atcacert.atcacert_tm_utc_t Class Reference</a>	408
21.81.1	Detailed Description	409
21.81.2	Field Documentation	409
21.82	<a href="#">cryptoauthlib.atcacert.atcacert_transform_t Class Reference</a>	409
21.82.1	Detailed Description	410
21.83	<a href="#">cryptoauthlib.iface.ATCADeviceType Class Reference</a>	410
21.83.1	Detailed Description	411
21.84	<a href="#">cryptoauthlib.atcaenum.AtcaEnum Class Reference</a>	411
21.84.1	Detailed Description	412
21.85	<a href="#">ATCAHAL_t Struct Reference</a>	412
21.85.1	Detailed Description	412
21.86	<a href="#">atcal2Cmaster Struct Reference</a>	412
21.86.1	Detailed Description	413
21.87	<a href="#">ATCAIfaceCfg Struct Reference</a>	413
21.87.1	Field Documentation	414
21.88	<a href="#">cryptoauthlib.iface.ATCAIfaceCfg Class Reference</a>	414
21.88.1	Detailed Description	415
21.88.2	Field Documentation	415
21.89	<a href="#">cryptoauthlib.iface.ATCAIfaceType Class Reference</a>	416
21.89.1	Detailed Description	416
21.90	<a href="#">cryptoauthlib.iface.ATCAKitType Class Reference</a>	417
21.90.1	Detailed Description	417
21.91	<a href="#">ATCAPacket Struct Reference</a>	417
21.92	<a href="#">cryptoauthlib.library.AtcaReference Class Reference</a>	418
21.92.1	Detailed Description	418
21.93	<a href="#">cryptoauthlib.library.AtcaStructure Class Reference</a>	418
21.93.1	Detailed Description	419
21.93.2	Member Function Documentation	419
21.94	<a href="#">atcaSWImaster Struct Reference</a>	419
21.94.1	Detailed Description	420
21.95	<a href="#">cryptoauthlib.library.AtcaUnion Class Reference</a>	420
21.95.1	Detailed Description	420
21.95.2	Member Function Documentation	420
21.96	<a href="#">atecc508a_config_s Struct Reference</a>	421
21.97	<a href="#">cryptoauthlib.device.Atecc508aConfig Class Reference</a>	422
21.97.1	Detailed Description	422
21.97.2	Field Documentation	422
21.98	<a href="#">atecc608_config_s Struct Reference</a>	423
21.99	<a href="#">cryptoauthlib.device.Atecc608Config Class Reference</a>	424
21.99.1	Detailed Description	424
21.99.2	Field Documentation	424
21.100	<a href="#">atsha204a_config_s Struct Reference</a>	425

21.101 <a href="#">cryptoauthlib.device.Atsha204aConfig Class Reference</a>	426
21.101.1 Detailed Description	426
21.101.2 Field Documentation	426
21.102 <a href="#">cryptoauthlib.exceptions.BadArgumentError Class Reference</a>	427
21.102.1 Detailed Description	427
21.103 <a href="#">cryptoauthlib.exceptions.BadCrcError Class Reference</a>	427
21.103.1 Detailed Description	427
21.104 <a href="#">cryptoauthlib.exceptions.BadOpcodeError Class Reference</a>	427
21.104.1 Detailed Description	428
21.105 <a href="#">setup.BinaryDistribution Class Reference</a>	428
21.106 <a href="#">cal_buffer_s Struct Reference</a>	428
21.106.1 Field Documentation	428
21.107 <a href="#">cryptoauthlib.atcacert.CertStatus Class Reference</a>	429
21.107.1 Detailed Description	429
21.108 <a href="#">cryptoauthlib.exceptions.CheckmacVerifyFailedError Class Reference</a>	430
21.108.1 Detailed Description	430
21.109 <a href="#">cryptoauthlib.device.ChipMode508 Class Reference</a>	430
21.109.1 Detailed Description	430
21.109.2 Field Documentation	430
21.110 <a href="#">cryptoauthlib.device.ChipMode608 Class Reference</a>	431
21.110.1 Detailed Description	431
21.110.2 Field Documentation	431
21.111 <a href="#">cryptoauthlib.device.ChipOptions Class Reference</a>	431
21.111.1 Detailed Description	432
21.111.2 Field Documentation	432
21.112 <a href="#">CK_AES_CBC_ENCRYPT_DATA_PARAMS Struct Reference</a>	432
21.113 <a href="#">CK_AES_CCM_PARAMS Struct Reference</a>	432
21.114 <a href="#">CK_AES_CTR_PARAMS Struct Reference</a>	432
21.115 <a href="#">CK_AES_GCM_PARAMS Struct Reference</a>	433
21.116 <a href="#">CK_ARIA_CBC_ENCRYPT_DATA_PARAMS Struct Reference</a>	433
21.117 <a href="#">CK_ATTRIBUTE Struct Reference</a>	433
21.118 <a href="#">CK_C_INITIALIZE_ARGS Struct Reference</a>	433
21.119 <a href="#">CK_CAMELLIA_CBC_ENCRYPT_DATA_PARAMS Struct Reference</a>	433
21.120 <a href="#">CK_CAMELLIA_CTR_PARAMS Struct Reference</a>	434
21.121 <a href="#">CK_CCM_PARAMS Struct Reference</a>	434
21.122 <a href="#">CK_CMS_SIG_PARAMS Struct Reference</a>	434
21.123 <a href="#">CK_DATE Struct Reference</a>	434
21.124 <a href="#">CK_DES_CBC_ENCRYPT_DATA_PARAMS Struct Reference</a>	434
21.125 <a href="#">CK_DSA_PARAMETER_GEN_PARAM Struct Reference</a>	435
21.126 <a href="#">CK_ECDH1_DERIVE_PARAMS Struct Reference</a>	435
21.127 <a href="#">CK_ECDH2_DERIVE_PARAMS Struct Reference</a>	435
21.128 <a href="#">CK_ECDH_AES_KEY_WRAP_PARAMS Struct Reference</a>	435

21.129 CK_ECMQV_DERIVE_PARAMS Struct Reference . . . . .	436
21.130 CK_FUNCTION_LIST Struct Reference . . . . .	436
21.131 CK_GCM_PARAMS Struct Reference . . . . .	436
21.132 CK_GOSTR3410_DERIVE_PARAMS Struct Reference . . . . .	436
21.133 CK_GOSTR3410_KEY_WRAP_PARAMS Struct Reference . . . . .	437
21.134 CK_INFO Struct Reference . . . . .	437
21.135 CK_KEA_DERIVE_PARAMS Struct Reference . . . . .	437
21.136 CK_KEY_DERIVATION_STRING_DATA Struct Reference . . . . .	437
21.137 CK_KEY_WRAP_SET_OAEP_PARAMS Struct Reference . . . . .	437
21.138 CK_KIP_PARAMS Struct Reference . . . . .	438
21.139 CK_MECHANISM Struct Reference . . . . .	438
21.140 CK_MECHANISM_INFO Struct Reference . . . . .	438
21.141 CK_OTP_PARAM Struct Reference . . . . .	438
21.142 CK_OTP_PARAMS Struct Reference . . . . .	438
21.143 CK_OTP_SIGNATURE_INFO Struct Reference . . . . .	439
21.144 CK_PBE_PARAMS Struct Reference . . . . .	439
21.145 CK_PKCS5_PBKD2_PARAMS Struct Reference . . . . .	439
21.146 CK_PKCS5_PBKD2_PARAMS2 Struct Reference . . . . .	439
21.147 CK_RC2_CBC_PARAMS Struct Reference . . . . .	440
21.148 CK_RC2_MAC_GENERAL_PARAMS Struct Reference . . . . .	440
21.149 CK_RC5_CBC_PARAMS Struct Reference . . . . .	440
21.150 CK_RC5_MAC_GENERAL_PARAMS Struct Reference . . . . .	440
21.151 CK_RC5_PARAMS Struct Reference . . . . .	440
21.152 CK_RSA_AES_KEY_WRAP_PARAMS Struct Reference . . . . .	440
21.153 CK_RSA_PKCS_OAEP_PARAMS Struct Reference . . . . .	441
21.154 CK_RSA_PKCS_PSS_PARAMS Struct Reference . . . . .	441
21.155 CK_SEED_CBC_ENCRYPT_DATA_PARAMS Struct Reference . . . . .	441
21.156 CK_SESSION_INFO Struct Reference . . . . .	441
21.157 CK_SKIPJACK_PRIVATE_WRAP_PARAMS Struct Reference . . . . .	441
21.158 CK_SKIPJACK_RELAYX_PARAMS Struct Reference . . . . .	442
21.159 CK_SLOT_INFO Struct Reference . . . . .	442
21.160 CK_SSL3_KEY_MAT_OUT Struct Reference . . . . .	442
21.161 CK_SSL3_KEY_MAT_PARAMS Struct Reference . . . . .	442
21.162 CK_SSL3_MASTER_KEY_DERIVE_PARAMS Struct Reference . . . . .	443
21.163 CK_SSL3_RANDOM_DATA Struct Reference . . . . .	443
21.164 CK_TLS12_KEY_MAT_PARAMS Struct Reference . . . . .	443
21.165 CK_TLS12_MASTER_KEY_DERIVE_PARAMS Struct Reference . . . . .	443
21.166 CK_TLS_KDF_PARAMS Struct Reference . . . . .	443
21.167 CK_TLS_MAC_PARAMS Struct Reference . . . . .	444
21.168 CK_TLS_PRF_PARAMS Struct Reference . . . . .	444
21.169 CK_TOKEN_INFO Struct Reference . . . . .	444
21.170 CK_VERSION Struct Reference . . . . .	444

21.171 CK_WTLS_KEY_MAT_OUT Struct Reference . . . . .	445
21.172 CK_WTLS_KEY_MAT_PARAMS Struct Reference . . . . .	445
21.173 CK_WTLS_MASTER_KEY_DERIVE_PARAMS Struct Reference . . . . .	445
21.174 CK_WTLS_PRF_PARAMS Struct Reference . . . . .	445
21.175 CK_WTLS_RANDOM_DATA Struct Reference . . . . .	445
21.176 CK_X9_42_DH1_DERIVE_PARAMS Struct Reference . . . . .	446
21.177 CK_X9_42_DH2_DERIVE_PARAMS Struct Reference . . . . .	446
21.178 CK_X9_42_MQV_DERIVE_PARAMS Struct Reference . . . . .	446
21.179 CL_HashContext Struct Reference . . . . .	446
21.180 cryptoauthlib.exceptions.CommunicationError Class Reference . . . . .	447
21.180.1 Detailed Description . . . . .	447
21.181 cryptoauthlib.exceptions.ConfigZoneLockedError Class Reference . . . . .	447
21.181.1 Detailed Description . . . . .	447
21.182 cryptoauthlib.device.Counter204 Class Reference . . . . .	447
21.182.1 Detailed Description . . . . .	448
21.182.2 Field Documentation . . . . .	448
21.183 cryptoauthlib.device.CountMatch Class Reference . . . . .	448
21.183.1 Detailed Description . . . . .	448
21.183.2 Field Documentation . . . . .	448
21.184 cryptoauthlib.exceptions.CrcError Class Reference . . . . .	449
21.184.1 Detailed Description . . . . .	449
21.185 setup.CryptoAuthCommandBuildExt Class Reference . . . . .	449
21.186 setup.CryptoAuthCommandInstall Class Reference . . . . .	449
21.187 cryptoauthlib.exceptions.CryptoError Class Reference . . . . .	450
21.187.1 Detailed Description . . . . .	450
21.188 cryptoauthlib.exceptions.DataZoneLockedError Class Reference . . . . .	450
21.188.1 Detailed Description . . . . .	451
21.189 device_execution_time_t Struct Reference . . . . .	451
21.189.1 Detailed Description . . . . .	451
21.190 devtype_names_t Struct Reference . . . . .	451
21.191 cryptoauthlib.exceptions.EccFaultError Class Reference . . . . .	451
21.191.1 Detailed Description . . . . .	451
21.192 cryptoauthlib.exceptions.ExecutionError Class Reference . . . . .	452
21.192.1 Detailed Description . . . . .	452
21.193 cryptoauthlib.exceptions.FunctionError Class Reference . . . . .	452
21.193.1 Detailed Description . . . . .	452
21.194 cryptoauthlib.exceptions.GenericError Class Reference . . . . .	452
21.194.1 Detailed Description . . . . .	453
21.195 cryptoauthlib.exceptions.HealthTestError Class Reference . . . . .	453
21.195.1 Detailed Description . . . . .	453
21.196 cryptoauthlib.atjwt.HwEcAlgorithm Class Reference . . . . .	453
21.196.1 Detailed Description . . . . .	453

21.196.2 Member Function Documentation . . . . .	454
21.197 cryptoauthlib.atjwt.HwHmacAlgorithm Class Reference . . . . .	454
21.197.1 Detailed Description . . . . .	454
21.197.2 Member Function Documentation . . . . .	454
21.198 i2c_sam0_instance Struct Reference . . . . .	455
21.199 i2c_sam_instance Struct Reference . . . . .	455
21.200 i2c_start_instance Struct Reference . . . . .	455
21.201 cryptoauthlib.device.I2cEnable Class Reference . . . . .	456
21.201.1 Detailed Description . . . . .	456
21.201.2 Field Documentation . . . . .	456
21.202 cryptoauthlib.exceptions.InvalidIdentifierError Class Reference . . . . .	456
21.202.1 Detailed Description . . . . .	456
21.203 cryptoauthlib.exceptions.InvalidSizeError Class Reference . . . . .	457
21.203.1 Detailed Description . . . . .	457
21.204 cryptoauthlib.device.KeyConfig Class Reference . . . . .	457
21.204.1 Detailed Description . . . . .	457
21.204.2 Field Documentation . . . . .	457
21.205 cryptoauthlib.exceptions.LibraryLoadError Class Reference . . . . .	458
21.205.1 Detailed Description . . . . .	458
21.206 cryptoauthlib.exceptions.LibraryMemoryError Class Reference . . . . .	458
21.206.1 Detailed Description . . . . .	458
21.207 cryptoauthlib.exceptions.LibraryNotInitialized Class Reference . . . . .	459
21.207.1 Detailed Description . . . . .	459
21.208 memory_parameters Struct Reference . . . . .	459
21.209 cryptoauthlib.exceptions.NoDevicesFoundError Class Reference . . . . .	459
21.209.1 Detailed Description . . . . .	459
21.210 cryptoauthlib.exceptions.NoResponseError Class Reference . . . . .	460
21.210.1 Detailed Description . . . . .	460
21.211 cryptoauthlib.exceptions.NoUseFlagError Class Reference . . . . .	460
21.211.1 Detailed Description . . . . .	460
21.212 cryptoauthlib.exceptions.ParityError Class Reference . . . . .	460
21.212.1 Detailed Description . . . . .	461
21.213 cryptoauthlib.exceptions.ParseError Class Reference . . . . .	461
21.213.1 Detailed Description . . . . .	461
21.214 pcks11_mech_table_e Struct Reference . . . . .	461
21.215 pcks11_attr_model_s Struct Reference . . . . .	461
21.216 pcks11_conf_filedata_s Struct Reference . . . . .	461
21.217 pcks11_dev_ctx Struct Reference . . . . .	462
21.217.1 Detailed Description . . . . .	462
21.218 pcks11_dev_res Struct Reference . . . . .	462
21.218.1 Detailed Description . . . . .	462
21.219 pcks11_dev_state Struct Reference . . . . .	462



21.219.1 Detailed Description . . . . .	462
21.219.2 Field Documentation . . . . .	462
21.220 pkcs11_ecc_key_info_s Struct Reference . . . . .	463
21.221 pkcs11_lib_ctx_s Struct Reference . . . . .	463
21.221.1 Detailed Description . . . . .	463
21.221.2 Field Documentation . . . . .	464
21.222 pkcs11_object_cache_s Struct Reference . . . . .	465
21.222.1 Field Documentation . . . . .	465
21.223 pkcs11_object_s Struct Reference . . . . .	465
21.223.1 Field Documentation . . . . .	466
21.224 pkcs11_session_ctx_s Struct Reference . . . . .	466
21.224.1 Detailed Description . . . . .	467
21.225 pkcs11_session_mech_ctx_s Struct Reference . . . . .	467
21.226 pkcs11_slot_ctx_s Struct Reference . . . . .	467
21.226.1 Detailed Description . . . . .	467
21.226.2 Field Documentation . . . . .	468
21.227 cryptoauthlib.atjwt.PyJWT Class Reference . . . . .	468
21.227.1 Detailed Description . . . . .	468
21.228 cryptoauthlib.exceptions.ReceiveError Class Reference . . . . .	468
21.228.1 Detailed Description . . . . .	468
21.229 cryptoauthlib.exceptions.ReceiveTimeoutError Class Reference . . . . .	469
21.229.1 Detailed Description . . . . .	469
21.230 cryptoauthlib.exceptions.ResyncWithWakeupError Class Reference . . . . .	469
21.230.1 Detailed Description . . . . .	469
21.231 secure_boot_config_bits Struct Reference . . . . .	469
21.232 secure_boot_parameters Struct Reference . . . . .	470
21.233 cryptoauthlib.device.SecureBoot Class Reference . . . . .	470
21.233.1 Detailed Description . . . . .	470
21.233.2 Field Documentation . . . . .	470
21.234 cryptoauthlib.device.SlotConfig Class Reference . . . . .	471
21.234.1 Detailed Description . . . . .	471
21.234.2 Field Documentation . . . . .	471
21.235 cryptoauthlib.status.Status Class Reference . . . . .	471
21.235.1 Detailed Description . . . . .	473
21.236 cryptoauthlib.exceptions.StatusUnknownError Class Reference . . . . .	473
21.236.1 Detailed Description . . . . .	473
21.237 sw_sha256_ctx Struct Reference . . . . .	473
21.238 cryptoauthlib.exceptions.TimeOutError Class Reference . . . . .	473
21.238.1 Detailed Description . . . . .	474
21.239 tng_cert_map_element Struct Reference . . . . .	474
21.240 cryptoauthlib.exceptions.TransmissionError Class Reference . . . . .	474
21.240.1 Detailed Description . . . . .	474

21.241	<a href="#">cryptoauthlib.exceptions.TransmissionTimeoutError Class Reference</a>	474
21.241.1	Detailed Description	474
21.242	<a href="#">cryptoauthlib.exceptions.UnimplementedError Class Reference</a>	475
21.242.1	Detailed Description	475
21.243	<a href="#">cryptoauthlib.exceptions.UnsupportedInterface Class Reference</a>	475
21.243.1	Detailed Description	475
21.244	<a href="#">cryptoauthlib.device.UseLock Class Reference</a>	475
21.244.1	Detailed Description	476
21.244.2	Field Documentation	476
21.245	<a href="#">cryptoauthlib.device.VolatileKeyPermission Class Reference</a>	476
21.245.1	Detailed Description	476
21.245.2	Field Documentation	476
21.246	<a href="#">cryptoauthlib.exceptions.WakeFailedError Class Reference</a>	477
21.246.1	Detailed Description	477
21.247	<a href="#">cryptoauthlib.device.X509Format Class Reference</a>	477
21.247.1	Detailed Description	477
21.247.2	Field Documentation	477
21.248	<a href="#">cryptoauthlib.exceptions.ZoneNotLockedError Class Reference</a>	478
21.248.1	Detailed Description	478
<b>22</b>	<b>File Documentation</b>	<b>479</b>
22.1	<a href="#">api_206a.c File Reference</a>	479
22.1.1	Detailed Description	480
22.1.2	Function Documentation	480
22.2	<a href="#">api_206a.h File Reference</a>	485
22.2.1	Detailed Description	486
22.2.2	Function Documentation	486
22.3	<a href="#">symmetric_authentication.c File Reference</a>	492
22.3.1	Detailed Description	492
22.3.2	Function Documentation	492
22.4	<a href="#">symmetric_authentication.h File Reference</a>	493
22.4.1	Detailed Description	493
22.4.2	Function Documentation	493
22.5	<a href="#">ascii_kit_host.c File Reference</a>	494
22.5.1	Detailed Description	494
22.5.2	Function Documentation	494
22.6	<a href="#">ascii_kit_host.h File Reference</a>	495
22.6.1	Detailed Description	496
22.6.2	Macro Definition Documentation	496
22.6.3	Typedef Documentation	497
22.6.4	Function Documentation	497
22.7	<a href="#">trust_pkcs11_config.c File Reference</a>	498

---

22.7.1 Detailed Description . . . . .	498
22.8 io_protection_key.h File Reference . . . . .	498
22.8.1 Detailed Description . . . . .	499
22.9 secure_boot.c File Reference . . . . .	499
22.9.1 Detailed Description . . . . .	499
22.9.2 Function Documentation . . . . .	499
22.10 secure_boot.h File Reference . . . . .	500
22.10.1 Detailed Description . . . . .	501
22.10.2 Function Documentation . . . . .	501
22.11 secure_boot_memory.h File Reference . . . . .	502
22.11.1 Detailed Description . . . . .	502
22.12 tflxtls_cert_def_4_device.c File Reference . . . . .	502
22.12.1 Detailed Description . . . . .	503
22.13 tflxtls_cert_def_4_device.h File Reference . . . . .	503
22.13.1 Detailed Description . . . . .	503
22.14 tng_atca.c File Reference . . . . .	503
22.14.1 Detailed Description . . . . .	504
22.15 tng_atca.h File Reference . . . . .	504
22.15.1 Detailed Description . . . . .	505
22.16 tng_atcacert_client.c File Reference . . . . .	505
22.16.1 Detailed Description . . . . .	505
22.16.2 Function Documentation . . . . .	506
22.17 tng_atcacert_client.h File Reference . . . . .	509
22.17.1 Detailed Description . . . . .	509
22.18 tng_root_cert.c File Reference . . . . .	510
22.18.1 Detailed Description . . . . .	510
22.19 tng_root_cert.h File Reference . . . . .	510
22.19.1 Detailed Description . . . . .	510
22.20 tnglora_cert_def_1_signer.c File Reference . . . . .	510
22.20.1 Detailed Description . . . . .	511
22.21 tnglora_cert_def_1_signer.h File Reference . . . . .	511
22.21.1 Detailed Description . . . . .	511
22.22 tnglora_cert_def_2_device.c File Reference . . . . .	511
22.22.1 Detailed Description . . . . .	512
22.23 tnglora_cert_def_2_device.h File Reference . . . . .	512
22.23.1 Detailed Description . . . . .	512
22.24 tnglora_cert_def_4_device.c File Reference . . . . .	512
22.24.1 Detailed Description . . . . .	513
22.25 tnglora_cert_def_4_device.h File Reference . . . . .	513
22.25.1 Detailed Description . . . . .	513
22.26 tngtls_cert_def_1_signer.c File Reference . . . . .	513
22.26.1 Detailed Description . . . . .	513

22.26.2 Variable Documentation . . . . .	514
22.27 tngtls_cert_def_1_signer.h File Reference . . . . .	514
22.27.1 Detailed Description . . . . .	514
22.28 tngtls_cert_def_2_device.c File Reference . . . . .	514
22.28.1 Detailed Description . . . . .	515
22.29 tngtls_cert_def_2_device.h File Reference . . . . .	515
22.29.1 Detailed Description . . . . .	515
22.30 tngtls_cert_def_3_device.c File Reference . . . . .	515
22.30.1 Detailed Description . . . . .	516
22.31 tngtls_cert_def_3_device.h File Reference . . . . .	516
22.31.1 Detailed Description . . . . .	516
22.32 wpc_apis.c File Reference . . . . .	516
22.32.1 Detailed Description . . . . .	517
22.33 wpc_apis.h File Reference . . . . .	517
22.33.1 Detailed Description . . . . .	518
22.34 wpccert_client.c File Reference . . . . .	518
22.34.1 Detailed Description . . . . .	518
22.34.2 Function Documentation . . . . .	518
22.35 wpccert_client.h File Reference . . . . .	519
22.35.1 Detailed Description . . . . .	519
22.35.2 Function Documentation . . . . .	519
22.36 atca_basic.c File Reference . . . . .	520
22.36.1 Detailed Description . . . . .	528
22.37 atca_basic.h File Reference . . . . .	528
22.37.1 Detailed Description . . . . .	536
22.38 atca_cfgs.c File Reference . . . . .	537
22.38.1 Detailed Description . . . . .	537
22.39 atca_cfgs.h File Reference . . . . .	537
22.39.1 Detailed Description . . . . .	537
22.40 atca_compiler.h File Reference . . . . .	537
22.40.1 Detailed Description . . . . .	538
22.40.2 Macro Definition Documentation . . . . .	538
22.41 atca_config_check.h File Reference . . . . .	538
22.41.1 Detailed Description . . . . .	539
22.41.2 Macro Definition Documentation . . . . .	540
22.42 atca_debug.c File Reference . . . . .	542
22.42.1 Detailed Description . . . . .	542
22.43 atca_device.c File Reference . . . . .	542
22.43.1 Detailed Description . . . . .	543
22.44 atca_device.h File Reference . . . . .	543
22.44.1 Detailed Description . . . . .	544
22.45 atca_devtypes.h File Reference . . . . .	544

22.45.1 Detailed Description . . . . .	545
22.46 atca_helpers.c File Reference . . . . .	545
22.46.1 Detailed Description . . . . .	546
22.46.2 Function Documentation . . . . .	546
22.47 atca_helpers.h File Reference . . . . .	553
22.47.1 Detailed Description . . . . .	555
22.48 atca_iface.c File Reference . . . . .	555
22.48.1 Detailed Description . . . . .	556
22.49 atca_iface.h File Reference . . . . .	556
22.49.1 Detailed Description . . . . .	559
22.49.2 Variable Documentation . . . . .	559
22.50 atca_platform.h File Reference . . . . .	560
22.50.1 Detailed Description . . . . .	560
22.51 atca_status.h File Reference . . . . .	560
22.51.1 Detailed Description . . . . .	561
22.51.2 Macro Definition Documentation . . . . .	562
22.52 atca_utils_sizes.c File Reference . . . . .	566
22.52.1 Detailed Description . . . . .	567
22.53 atca_version.h File Reference . . . . .	568
22.53.1 Detailed Description . . . . .	568
22.54 atcacert.h File Reference . . . . .	568
22.54.1 Detailed Description . . . . .	569
22.55 atcacert_check_config.h File Reference . . . . .	569
22.55.1 Detailed Description . . . . .	569
22.56 atcacert_client.c File Reference . . . . .	569
22.56.1 Detailed Description . . . . .	570
22.57 atcacert_client.h File Reference . . . . .	570
22.57.1 Detailed Description . . . . .	571
22.58 atcacert_date.c File Reference . . . . .	571
22.58.1 Detailed Description . . . . .	572
22.59 atcacert_date.h File Reference . . . . .	572
22.59.1 Detailed Description . . . . .	574
22.60 atcacert_def.c File Reference . . . . .	574
22.60.1 Detailed Description . . . . .	575
22.61 atcacert_def.h File Reference . . . . .	575
22.61.1 Detailed Description . . . . .	577
22.62 atcacert_der.c File Reference . . . . .	577
22.62.1 Detailed Description . . . . .	578
22.63 atcacert_der.h File Reference . . . . .	578
22.63.1 Detailed Description . . . . .	578
22.64 atcacert_host_hw.c File Reference . . . . .	579
22.64.1 Detailed Description . . . . .	579

---

22.65 atcacert_host_hw.h File Reference . . . . .	579
22.65.1 Detailed Description . . . . .	579
22.66 atcacert_host_sw.c File Reference . . . . .	580
22.66.1 Detailed Description . . . . .	580
22.67 atcacert_host_sw.h File Reference . . . . .	580
22.67.1 Detailed Description . . . . .	580
22.68 atcacert_pem.c File Reference . . . . .	581
22.68.1 Detailed Description . . . . .	581
22.69 atcacert_pem.h File Reference . . . . .	581
22.69.1 Detailed Description . . . . .	582
22.69.2 Function Documentation . . . . .	582
22.70 cal_buffer.c File Reference . . . . .	585
22.70.1 Detailed Description . . . . .	585
22.70.2 Function Documentation . . . . .	586
22.71 cal_buffer.h File Reference . . . . .	587
22.71.1 Detailed Description . . . . .	588
22.71.2 Function Documentation . . . . .	588
22.72 cal_internal.h File Reference . . . . .	590
22.72.1 Detailed Description . . . . .	590
22.73 calib_aes.c File Reference . . . . .	590
22.73.1 Detailed Description . . . . .	590
22.74 calib_aes_gcm.c File Reference . . . . .	591
22.74.1 Detailed Description . . . . .	591
22.75 calib_aes_gcm.h File Reference . . . . .	591
22.75.1 Detailed Description . . . . .	591
22.76 calib_basic.c File Reference . . . . .	591
22.76.1 Detailed Description . . . . .	592
22.77 calib_checkmac.c File Reference . . . . .	592
22.77.1 Detailed Description . . . . .	592
22.78 calib_command.c File Reference . . . . .	593
22.78.1 Detailed Description . . . . .	593
22.78.2 Function Documentation . . . . .	593
22.79 calib_command.h File Reference . . . . .	596
22.79.1 Detailed Description . . . . .	614
22.79.2 Function Documentation . . . . .	614
22.80 calib_config_check.h File Reference . . . . .	617
22.80.1 Detailed Description . . . . .	619
22.80.2 Macro Definition Documentation . . . . .	619
22.81 calib_counter.c File Reference . . . . .	622
22.81.1 Detailed Description . . . . .	622
22.82 calib_delete.c File Reference . . . . .	622
22.82.1 Detailed Description . . . . .	622

22.83 calib_derivekey.c File Reference . . . . .	623
22.83.1 Detailed Description . . . . .	623
22.84 calib_device.h File Reference . . . . .	623
22.84.1 Detailed Description . . . . .	626
22.85 calib_ecdh.c File Reference . . . . .	626
22.85.1 Detailed Description . . . . .	627
22.86 calib_execution.c File Reference . . . . .	627
22.86.1 Detailed Description . . . . .	627
22.86.2 Function Documentation . . . . .	627
22.87 calib_execution.h File Reference . . . . .	628
22.87.1 Detailed Description . . . . .	629
22.87.2 Function Documentation . . . . .	629
22.88 calib_gendig.c File Reference . . . . .	630
22.88.1 Detailed Description . . . . .	630
22.89 calib_genkey.c File Reference . . . . .	631
22.89.1 Detailed Description . . . . .	631
22.90 calib_helpers.c File Reference . . . . .	631
22.90.1 Detailed Description . . . . .	631
22.91 calib_hmac.c File Reference . . . . .	632
22.91.1 Detailed Description . . . . .	632
22.92 calib_info.c File Reference . . . . .	632
22.92.1 Detailed Description . . . . .	633
22.93 calib_kdf.c File Reference . . . . .	633
22.93.1 Detailed Description . . . . .	633
22.94 calib_lock.c File Reference . . . . .	633
22.94.1 Detailed Description . . . . .	634
22.95 calib_mac.c File Reference . . . . .	634
22.95.1 Detailed Description . . . . .	634
22.96 calib_nonce.c File Reference . . . . .	634
22.96.1 Detailed Description . . . . .	635
22.97 calib_privwrite.c File Reference . . . . .	635
22.97.1 Detailed Description . . . . .	635
22.98 calib_random.c File Reference . . . . .	635
22.98.1 Detailed Description . . . . .	636
22.99 calib_read.c File Reference . . . . .	636
22.99.1 Detailed Description . . . . .	636
22.100 calib_secureboot.c File Reference . . . . .	636
22.100.1 Detailed Description . . . . .	637
22.101 calib_selftest.c File Reference . . . . .	637
22.101.1 Detailed Description . . . . .	637
22.102 calib_sha.c File Reference . . . . .	637
22.102.1 Detailed Description . . . . .	638

22.103 calib_sign.c File Reference . . . . .	638
22.103.1 Detailed Description . . . . .	638
22.104 calib_updateextra.c File Reference . . . . .	638
22.104.1 Detailed Description . . . . .	639
22.105 calib_verify.c File Reference . . . . .	639
22.105.1 Detailed Description . . . . .	639
22.106 calib_write.c File Reference . . . . .	639
22.106.1 Detailed Description . . . . .	640
22.107 atca_crypto_hw_aes.h File Reference . . . . .	640
22.107.1 Detailed Description . . . . .	640
22.108 atca_crypto_hw_aes_cbc.c File Reference . . . . .	640
22.108.1 Detailed Description . . . . .	641
22.109 atca_crypto_hw_aes_cbcmac.c File Reference . . . . .	641
22.109.1 Detailed Description . . . . .	641
22.110 atca_crypto_hw_aes_ccm.c File Reference . . . . .	641
22.110.1 Detailed Description . . . . .	642
22.111 atca_crypto_hw_aes_cmac.c File Reference . . . . .	642
22.111.1 Detailed Description . . . . .	642
22.112 atca_crypto_hw_aes_ctr.c File Reference . . . . .	642
22.112.1 Detailed Description . . . . .	643
22.113 atca_crypto_pad.c File Reference . . . . .	643
22.113.1 Detailed Description . . . . .	643
22.114 atca_crypto_pbkdf2.c File Reference . . . . .	643
22.114.1 Detailed Description . . . . .	643
22.115 atca_crypto_sw.h File Reference . . . . .	644
22.115.1 Detailed Description . . . . .	644
22.116 atca_crypto_sw_aes_gcm.c File Reference . . . . .	644
22.116.1 Detailed Description . . . . .	644
22.117 atca_crypto_sw_sha1.c File Reference . . . . .	644
22.117.1 Detailed Description . . . . .	645
22.118 atca_crypto_sw_sha1.h File Reference . . . . .	645
22.118.1 Detailed Description . . . . .	645
22.119 atca_crypto_sw_sha2.c File Reference . . . . .	645
22.119.1 Detailed Description . . . . .	645
22.120 atca_crypto_sw_sha2.h File Reference . . . . .	646
22.120.1 Detailed Description . . . . .	646
22.121 crypto_hw_config_check.h File Reference . . . . .	646
22.121.1 Detailed Description . . . . .	647
22.121.2 Macro Definition Documentation . . . . .	647
22.122 crypto_sw_config_check.h File Reference . . . . .	648
22.122.1 Detailed Description . . . . .	649
22.122.2 Macro Definition Documentation . . . . .	649



22.123 sha1_routines.c File Reference . . . . .	651
22.123.1 Detailed Description . . . . .	651
22.124 sha1_routines.h File Reference . . . . .	652
22.124.1 Detailed Description . . . . .	652
22.125 sha2_routines.c File Reference . . . . .	652
22.125.1 Detailed Description . . . . .	653
22.126 sha2_routines.h File Reference . . . . .	653
22.126.1 Detailed Description . . . . .	653
22.127 cryptoauthlib.h File Reference . . . . .	654
22.127.1 Detailed Description . . . . .	655
22.127.2 Macro Definition Documentation . . . . .	655
22.128 atca_hal.c File Reference . . . . .	656
22.128.1 Detailed Description . . . . .	656
22.129 atca_hal.h File Reference . . . . .	657
22.129.1 Detailed Description . . . . .	658
22.130 hal_all_platforms_kit_hidapi.c File Reference . . . . .	658
22.130.1 Detailed Description . . . . .	659
22.131 hal_freertos.c File Reference . . . . .	659
22.131.1 Detailed Description . . . . .	660
22.132 hal_gpio_harmony.c File Reference . . . . .	660
22.132.1 Detailed Description . . . . .	660
22.132.2 Function Documentation . . . . .	660
22.133 hal_i2c_harmony.c File Reference . . . . .	662
22.133.1 Detailed Description . . . . .	663
22.134 hal_i2c_start.c File Reference . . . . .	663
22.134.1 Detailed Description . . . . .	664
22.135 hal_i2c_start.h File Reference . . . . .	664
22.135.1 Detailed Description . . . . .	665
22.136 hal_kit_bridge.c File Reference . . . . .	665
22.136.1 Detailed Description . . . . .	666
22.137 hal_kit_bridge.h File Reference . . . . .	666
22.137.1 Detailed Description . . . . .	666
22.138 hal_linux.c File Reference . . . . .	667
22.138.1 Detailed Description . . . . .	667
22.139 hal_linux_i2c_userspace.c File Reference . . . . .	667
22.139.1 Detailed Description . . . . .	668
22.140 hal_linux_uart_userspace.c File Reference . . . . .	668
22.140.1 Detailed Description . . . . .	669
22.140.2 Function Documentation . . . . .	669
22.141 hal_sam0_i2c_asf.c File Reference . . . . .	672
22.141.1 Detailed Description . . . . .	672
22.142 hal_sam0_i2c_asf.h File Reference . . . . .	673

22.142.1 Detailed Description . . . . .	673
22.143 hal_sam_i2c_asf.c File Reference . . . . .	673
22.143.1 Detailed Description . . . . .	674
22.144 hal_sam_i2c_asf.h File Reference . . . . .	674
22.144.1 Detailed Description . . . . .	675
22.145 hal_sam_timer_asf.c File Reference . . . . .	675
22.145.1 Detailed Description . . . . .	675
22.146 hal_spi_harmony.c File Reference . . . . .	676
22.146.1 Detailed Description . . . . .	676
22.147 hal_swi_gpio.c File Reference . . . . .	677
22.147.1 Detailed Description . . . . .	677
22.147.2 Function Documentation . . . . .	677
22.148 hal_swi_gpio.h File Reference . . . . .	680
22.148.1 Detailed Description . . . . .	681
22.148.2 Macro Definition Documentation . . . . .	682
22.149 hal_swi_uart.c File Reference . . . . .	682
22.149.1 Detailed Description . . . . .	683
22.150 hal_timer_start.c File Reference . . . . .	683
22.150.1 Detailed Description . . . . .	684
22.151 hal_uart_harmony.c File Reference . . . . .	684
22.151.1 Detailed Description . . . . .	684
22.151.2 Function Documentation . . . . .	685
22.151.3 Variable Documentation . . . . .	687
22.152 hal_uc3_i2c_asf.c File Reference . . . . .	688
22.152.1 Detailed Description . . . . .	689
22.153 hal_uc3_i2c_asf.h File Reference . . . . .	689
22.153.1 Detailed Description . . . . .	689
22.154 hal_uc3_timer_asf.c File Reference . . . . .	690
22.154.1 Detailed Description . . . . .	690
22.155 hal_windows.c File Reference . . . . .	690
22.155.1 Detailed Description . . . . .	691
22.156 hal_windows_kit_uart.c File Reference . . . . .	691
22.156.1 Detailed Description . . . . .	692
22.156.2 Function Documentation . . . . .	692
22.157 kit_protocol.c File Reference . . . . .	695
22.157.1 Detailed Description . . . . .	696
22.158 kit_protocol.h File Reference . . . . .	696
22.158.1 Detailed Description . . . . .	697
22.159 swi_uart_samd21_asf.c File Reference . . . . .	697
22.159.1 Detailed Description . . . . .	697
22.160 swi_uart_samd21_asf.h File Reference . . . . .	698
22.160.1 Detailed Description . . . . .	699

22.161 swi_uart_start.c File Reference . . . . .	699
22.161.1 Detailed Description . . . . .	699
22.162 swi_uart_start.h File Reference . . . . .	700
22.162.1 Detailed Description . . . . .	700
22.163 atca_host.c File Reference . . . . .	701
22.163.1 Detailed Description . . . . .	701
22.164 atca_host.h File Reference . . . . .	701
22.164.1 Detailed Description . . . . .	704
22.165 atca_host_config_check.h File Reference . . . . .	704
22.165.1 Detailed Description . . . . .	705
22.165.2 Macro Definition Documentation . . . . .	705
22.166 atca_jwt.c File Reference . . . . .	710
22.166.1 Detailed Description . . . . .	711
22.167 atca_jwt.h File Reference . . . . .	711
22.167.1 Detailed Description . . . . .	711
22.168 atca_mbedtls_interface.h File Reference . . . . .	711
22.168.1 Detailed Description . . . . .	712
22.168.2 Macro Definition Documentation . . . . .	712
22.169 atca_mbedtls_wrap.c File Reference . . . . .	713
22.169.1 Detailed Description . . . . .	715
22.169.2 Function Documentation . . . . .	715
22.169.3 Variable Documentation . . . . .	726
22.170 atca_openssl_interface.c File Reference . . . . .	727
22.170.1 Detailed Description . . . . .	729
22.170.2 Function Documentation . . . . .	729
22.171 atca_openssl_interface.h File Reference . . . . .	740
22.171.1 Detailed Description . . . . .	741
22.171.2 Macro Definition Documentation . . . . .	741
22.172 pkcs11_attrb.c File Reference . . . . .	742
22.172.1 Detailed Description . . . . .	743
22.173 pkcs11_attrb.h File Reference . . . . .	743
22.173.1 Detailed Description . . . . .	743
22.173.2 Typedef Documentation . . . . .	744
22.174 pkcs11_cert.c File Reference . . . . .	744
22.174.1 Detailed Description . . . . .	745
22.175 pkcs11_cert.h File Reference . . . . .	745
22.175.1 Detailed Description . . . . .	745
22.176 pkcs11_config.c File Reference . . . . .	746
22.176.1 Detailed Description . . . . .	747
22.177 pkcs11_debug.c File Reference . . . . .	747
22.177.1 Detailed Description . . . . .	747
22.178 pkcs11_debug.h File Reference . . . . .	747

---

22.178.1 Detailed Description . . . . .	747
22.179 pkcs11_digest.h File Reference . . . . .	748
22.179.1 Detailed Description . . . . .	748
22.180 pkcs11_encrypt.c File Reference . . . . .	748
22.180.1 Detailed Description . . . . .	749
22.181 pkcs11_encrypt.h File Reference . . . . .	749
22.181.1 Detailed Description . . . . .	750
22.182 pkcs11_find.c File Reference . . . . .	750
22.182.1 Detailed Description . . . . .	750
22.183 pkcs11_find.h File Reference . . . . .	750
22.183.1 Detailed Description . . . . .	751
22.184 pkcs11_info.c File Reference . . . . .	751
22.184.1 Detailed Description . . . . .	751
22.185 pkcs11_info.h File Reference . . . . .	752
22.185.1 Detailed Description . . . . .	752
22.186 pkcs11_init.c File Reference . . . . .	752
22.186.1 Detailed Description . . . . .	753
22.187 pkcs11_init.h File Reference . . . . .	753
22.187.1 Detailed Description . . . . .	754
22.187.2 Typedef Documentation . . . . .	754
22.188 pkcs11_key.c File Reference . . . . .	754
22.188.1 Detailed Description . . . . .	755
22.189 pkcs11_key.h File Reference . . . . .	756
22.189.1 Detailed Description . . . . .	757
22.190 pkcs11_main.c File Reference . . . . .	757
22.190.1 Detailed Description . . . . .	761
22.191 pkcs11_mech.c File Reference . . . . .	762
22.191.1 Detailed Description . . . . .	762
22.192 pkcs11_mech.h File Reference . . . . .	762
22.192.1 Detailed Description . . . . .	763
22.193 pkcs11_object.c File Reference . . . . .	763
22.193.1 Detailed Description . . . . .	764
22.194 pkcs11_object.h File Reference . . . . .	764
22.194.1 Detailed Description . . . . .	766
22.195 pkcs11_os.c File Reference . . . . .	766
22.195.1 Detailed Description . . . . .	766
22.196 pkcs11_os.h File Reference . . . . .	766
22.196.1 Detailed Description . . . . .	767
22.197 pkcs11_session.c File Reference . . . . .	767
22.197.1 Detailed Description . . . . .	768
22.198 pkcs11_session.h File Reference . . . . .	768
22.198.1 Detailed Description . . . . .	769

---

22.198.2 Typedef Documentation . . . . .	769
22.199 pkcs11_signature.c File Reference . . . . .	769
22.199.1 Detailed Description . . . . .	770
22.200 pkcs11_signature.h File Reference . . . . .	770
22.200.1 Detailed Description . . . . .	771
22.201 pkcs11_slot.c File Reference . . . . .	771
22.201.1 Detailed Description . . . . .	772
22.202 pkcs11_slot.h File Reference . . . . .	772
22.202.1 Detailed Description . . . . .	773
22.202.2 Typedef Documentation . . . . .	773
22.203 pkcs11_token.c File Reference . . . . .	773
22.203.1 Detailed Description . . . . .	774
22.204 pkcs11_token.h File Reference . . . . .	774
22.204.1 Detailed Description . . . . .	775
22.205 pkcs11_util.c File Reference . . . . .	775
22.205.1 Detailed Description . . . . .	775
22.206 pkcs11_util.h File Reference . . . . .	776
22.206.1 Detailed Description . . . . .	776
22.207 atca_wolfssl_interface.c File Reference . . . . .	776
22.207.1 Detailed Description . . . . .	776
22.208 atca_wolfssl_interface.h File Reference . . . . .	776
22.208.1 Detailed Description . . . . .	777
22.209 atca_wolfssl_internal.h File Reference . . . . .	777
22.209.1 Detailed Description . . . . .	777
<b>Index</b>	<b>779</b>

## Chapter 1

# CryptoAuthLib - Microchip CryptoAuthentication Library

### 1.1 Introduction

This library implements the APIs required to communicate with Microchip Security device. The family of devices supported currently are:

CryptoAuth	CryptoAuth2
ATECC608B	ECC204
ATECC608A	ECC206
ATECC508A	SHA104
ATECC108A	SHA105
ATSHA204A	SHA106
ATSHA206A	RNG90

The best place to start is with the [Microchip Trust Platform](#)

Online API documentation is at <https://microchiptech.github.io/cryptoauthlib/>

Latest software and examples can be found at:

- <https://www.microchip.com/design-centers/security-ics/trust-platform>
- <http://www.microchip.com/SWLibraryWeb/product.aspx?product=CryptoAuthLib>

Prerequisite hardware to run CryptoAuthLib examples:

- [CryptoAuth Trust Platform Development Kit](#)

Alternatively a Microchip MCU and Adapter Board:

- [ATSAMR21 Xplained Pro](#) or [ATSAMD21 Xplained Pro](#)

- [CryptoAuthentication SOIC Socket Board](#) to accept SOIC parts
- [ATECC608B mikroBUS evaluation board](#)
- [ECC204 mikroBUS evaluation board](#)
- [SHA104/SHA105 mikroBUS evaluation board](#)
- [TA010 mikroBUS evaluation board](#)

For most development, using socketed top-boards is preferable until your configuration is well tested, then you can commit it to a CryptoAuth Xplained Pro Extension, for example. Keep in mind that once you lock a device, it will not be changeable.

## 1.2 Examples

- Install the [Trust Platform Design Suite](#) to access Use Case examples for the different Security Solutions (ATECC608, SHA104/105, ECC204, TA010, TA100...)

## 1.3 Configuration

In order to properly configured the library there must be a header file in your project named `atca_config.h` at minimum this needs to contain defines for the hal and device types being used. Most integrations have an configuration mechanism for generating this file. See the [atca\\_config.h.in](#) template which is configured by CMake for Linux, MacOS, & Windows projects.

An example of the configuration:

```
/* Cryptoauthlib Configuration File */
#ifndef ATCA_CONFIG_H
#define ATCA_CONFIG_H
/* Include HALS */
#define ATCA_HAL_I2C
/* Included device support */
#define ATCA_ATECC608_SUPPORT
/* \brief How long to wait after an initial wake failure for the POST to
 * complete.
 * If Power-on self test (POST) is enabled, the self test will run on waking
 * from sleep or during power-on, which delays the wake reply.
 */
#ifndef ATCA_POST_DELAY_MSEC
#define ATCA_POST_DELAY_MSEC 25
#endif
#endif // ATCA_CONFIG_H
```

There are two major compiler defines that affect the operation of the library.

- `ATCA_NO_POLL` can be used to revert to a non-polling mechanism for device responses. Normally responses are polled for after sending a command, giving quicker response times. However, if `ATCA_NO_POLL` is defined, then the library will simply delay the max execution time of a command before reading the response.
- `ATCA_NO_HEAP` can be used to remove the use of malloc/free from the main library. This can be helpful for smaller MCUs that don't have a heap implemented. If just using the basic API, then there shouldn't be any code changes required. The lower-level API will no longer use the new/delete functions and the init/release functions should be used directly.

Some specific options are available in the fully documented configuration files `lib/calib/calib_config.h`, `atca_configuration.h`, `lib/crypto/crypto_config.h`, `lib/host/atca_host_config.h` which is also the place where features can be selected. We provide some configurations focused on specific use cases and the checks are enabled by default.

## 1.4 Release notes

See [Release Notes](#)

## 1.5 Host Device Support

CryptoAuthLib will run on a variety of platforms from small micro-controllers to desktop host systems. See [hal readme](#)

Porting requires a time delay function of millisecond resolution (`hal_delay_ms`) which can be implemented via loop, timer, or rtos sleep/wait and a communication interface.

## 1.6 CryptoAuthLib Architecture

Cryptoauthlib API documentation is at <https://microchiptech.github.io/cryptoauthlib/>

The library is structured to support portability to:

- multiple hardware/microcontroller platforms
- multiple environments including bare-metal, RTOS and Windows/Linux/macOS
- multiple chip communication protocols (I2C, SPI, and SWI)

All platform dependencies are contained within the HAL (hardware abstraction layer).

## 1.7 Directory Structure

```
lib - primary library source code
lib/atcacert - certificate data and i/o methods
lib/calib - the Basic Cryptoauth API
lib/crypto - Software crypto implementations external crypto libraries support (primarily SHA1 and SHA256)
lib/hal - hardware abstraction layer code for supporting specific platforms
lib/host - support functions for common host-side calculations
lib/jwt - json web token functions
test - Integration test and examples. See test/cmd-processor.c for main() implementation.
For production code, test directories should be excluded by not compiling it
into a project, so it is up to the developer to include or not as needed. Test
code adds significant bulk to an application - it's not intended to be included
in production code.
```

## 1.8 Tests

There is a set of integration tests found in the test directory which will at least partially demonstrate the use of the objects. Some tests may depend upon a certain device being configured in a certain way and may not work for all devices or specific configurations of the device. See test readme



## 1.9 Using CryptoAuthLib (Microchip CryptoAuth Library)

The best place to start is with the [Microchip Trust Platform](#)

Also application examples are included as part of the Harmony 3 framework and can be copied from the Harmony Content Manager or found with the Harmony 3 Framework [Cryptoauthlib\\_apps](#)

### 1.9.1 Incorporating CryptoAuthLib in a Linux project using USB HID devices

The Linux HID HAL files use the Linux udev development software package.

To install the udev development package under Ubuntu Linux, please type the following command at the terminal window:

```
sudo apt-get install libudev-dev
```

This adds the udev development development software package to the Ubuntu Linux installation.

The Linux HID HAL files also require a udev rule to be added to change the permissions of the USB HID Devices. Please add a new udev rule for the Microchip CryptoAuth USB devices.

```
cd /etc/udev/rules.d
sudo touch mchp-cryptoauth.rules
```

Edit the mchp-cryptoauth.rules file and add the following line to the file:

```
SUBSYSTEM=="hidraw", ATTRS{idVendor}=="03eb", ATTRS{idProduct}=="2312", MODE="0666"
```

## Chapter 2

# License

Replace mbedTLS ECDH Functions with hardware acceleration & hardware key security.

mbedTLS Interface Functions that enable mbedtIs objects to use cryptoauthlib functions

Replace mbedTLS ECDSA Functions with hardware acceleration & hardware key security.

Subject to your compliance with these terms, you may use Microchip software and any derivatives exclusively with Microchip products. It is your responsibility to comply with third party license terms applicable to your use of third party software (including open source software) that may accompany Microchip software.

THIS SOFTWARE IS SUPPLIED BY MICROCHIP "AS IS". NO WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, APPLY TO THIS SOFTWARE, INCLUDING ANY IMPLIED WARRANTIES OF NON-↵ INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL LOSS, DAMAGE, COST OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE SOFTWARE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THIS SOFTWARE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THIS SOFTWARE.

(c) 2018 Microchip Technology Inc. and its subsidiaries. You may use this software and any derivatives exclusively with Microchip products.

THIS SOFTWARE IS SUPPLIED BY MICROCHIP "AS IS". NO WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, APPLY TO THIS SOFTWARE, INCLUDING ANY IMPLIED WARRANTIES OF NON-↵ INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR ITS INTERACTION WITH MICROCHIP PRODUCTS, COMBINATION WITH ANY OTHER PRODUCTS, OR USE IN ANY APPLICATION.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL LOSS, DAMAGE, COST OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE SOFTWARE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIPS TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THIS SOFTWARE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THIS SOFTWARE.

MICROCHIP PROVIDES THIS SOFTWARE CONDITIONALLY UPON YOUR ACCEPTANCE OF THESE TERMS.

**Copyright**

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

Subject to your compliance with these terms, you may use Microchip software and any derivatives exclusively with Microchip products. It is your responsibility to comply with third party license terms applicable to your use of third party software (including open source software) that may accompany Microchip software.

THIS SOFTWARE IS SUPPLIED BY MICROCHIP "AS IS". NO WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, APPLY TO THIS SOFTWARE, INCLUDING ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL LOSS, DAMAGE, COST OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE SOFTWARE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THIS SOFTWARE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THIS SOFTWARE.

## Chapter 3

# IP Protection with Symmetric Authentication

n

The IP protection can be easily integrated to the existing projects. The user project should include [symmetric\\_authentication.c](#) & [symmetric\\_authentication.h](#) files which contains the api

- [symmetric\\_authenticate\(\)](#) - For Performing the authentication between host & device.

### 3.1 User Considerations

- The user should take care on how the master key should be stored on the MCU side.
- The api's in the file doesn't do the provisioning of the chip and user should take care of the provisioning.

With the provisioned cryptoauthentication device and after doing the cryptoauthlib initialisation, user should only be calling the function [symmetric\\_authenticate\(\)](#) with its necessary parameters for the authentication. The returned authentication status should be used in the application.

### 3.2 Examples

For more information about IP protection and its example project refer [Microchip github](#)



## Chapter 4

# PKCS11 Application Information

n

### 4.1 Setting up cryptoauthlib as a PKCS11 Provider for your system (LINUX)

These instructions are for building, installing and configuring cryptoauthlib as a pkcs11 provider. These instructions are for commonly available Linux systems with package managers.

#### 4.1.1 Update libp11 on the system. The version should be at minimum 0.4.10

- Install the build dependencies for the system:  

```
# Debian like systems
$ sudo apt-get build-dep libengine-pkcs11-openssl1.1
# RPM based systems
$ yum-builddep engine-pkcs11
```
- Change to a sane directory  

```
cd ~
```
- Get the latest version of libp11  

```
$ git clone https://github.com/OpenSC/libp11.git
```
- Rerun the build configuration tools:  

```
$ cd libp11
$ ./bootstrap
$ ./configure
```
- Build the library:  

```
$ make
```
- Install the library:  

```
$ sudo make install
```

## 4.1.2 Build and Install cryptauthlib with PKCS11 support

- Install the build dependencies for the system:
 

```
# Debian like systems
$ sudo apt-get install cmake libudev-dev
# RPM based systems
$ yum install cmake
$ yum install libudev-devel
```
- Change to a sane directory
 

```
cd ~
```
- Get the latest version of cryptauthlib with PKCS11 support
 

```
$ git clone https://github.com/MicrochipTech/cryptauthlib
```
- Rerun the build configuration tools:
 

```
$ cd cryptauthlib
$ cmake -DATCA_PKCS11=ON .
```
- Build the library:
 

```
$ make
```
- Install the library:
 

```
$ sudo make install
```

## 4.1.3 Configuring the cryptauthlib PKCS11 library

By default the following files will be created.

- `/etc/cryptauthlib/cryptauthlib.conf`

```
# Cryptauthlib Configuration File
filestore = /var/lib/cryptauthlib
```
- `/var/lib/cryptauthlib/slot.conf.tmpl`

```
# Reserved Configuration for a device
# The objects in this file will be created and marked as undeletable
# These are processed in order. Configuration parameters must be comma
# delimited and may not contain spaces
interface = i2c,0xB0
freeslots = 1,2,3
# Slot 0 is the primary private key
object = private,device,0
# Slot 10 is the certificate data for the device's public key
#object = certificate,device,10
# Slot 12 is the intermediate/signer certificate data
#object = certificate,signer,12
# Slot 15 is a public key
object = public,root,15
```

### 4.1.3.1 cryptauthlib.conf

This file provides the basic configuration information for the library. The only variable is "filestore" which is where cryptauthlib will find device specific configuration and where it will store object files from pkcs11 operations.

### 4.1.3.2 slot.conf.tmpl

This is a template for device configuration files that cryptauthlib will use to map devices and their resources into pkcs11 tokens and objects.

A device file must be named `<pkcs11_slot_number>.conf`

For a single device:

```
$ cd /var/lib/cryptauthlib
$ cp slot.conf.tmpl 0.conf
```

Then edit 0.conf to match the device configuration being used.

## 4.1 Setting up cryptoauthlib as a PKCS11 Provider for your system (LINUX)

---

**4.1.3.2.1 interface** Allows values: 'hid', 'i2c' If using i2c specify the address in hex for the device. This is in the device format (upper 7 bits define the address) so will not appear the same as the i2cdetect address (lower 7 bits)

**4.1.3.2.2 freeslots** This is a list of slots that may be used by the library when a pkcs11 operation that creates new objects is used. When the library is initialized it will scan for files of the form <pkcs11\_slot\_num>.<device\_↵ slot\_num>.conf which defines the object using that device resource.

### 4.1.4 Using p11-kit-proxy

This is an optional step but is very helpful for using multiple pkcs11 libraries in a system. Detailed setup can be found at [p11-glue](#)

```
# Debian like systems
$ sudo apt-get install p11-kit
# RPM based systems
$ yum install p11-kit
```

- Create or edit the global configuration file /etc/pkcs11/pkcs11.conf. The directory /etc/pkcs11 may require creation first.

```
# This setting controls whether to load user configuration from the
# ~/.config/pkcs11 directory. Possible values:
#   none: No user configuration
#   merge: Merge the user config over the system configuration (default)
#   only: Only user configuration, ignore system configuration
user-config: merge
```

- Create a module configuration file.

- User module name (only available for a single user): ~/.config/pkcs11/modules/cryptoauthlib.↵ module
- Global module name (available to the whole system): /usr/share/p11-kit/modules/cryptoauthlib.modu↵

```
module: /usr/lib/libcryptoauth.so
critical: yes
trust-policy: yes
managed: yes
log-calls: no
```

For more details on the configuration files see the [configuration documentation](#).

### 4.1.5 Without using p11-kit-proxy

OpenSSL (via the libp11 project above) and p11tool support p11-kit-proxy natively so do not require additional set up if it is being used. If p11-kit-proxy is not being used then OpenSSL will have to be manually configured to use libp11 and cryptoauthlib

This requires editing the default openssl.cnf file. To locate the file being used by the system run the following command:

```
$ openssl version -a | grep OPENSSLDIR:
OPENSSLDIR: "/usr/lib/ssl"
```

This gives the default path where openssl is compiled to find the openssl.cnf file

In this case the file to edit will be /usr/lib/ssl/openssl.cnf

This line must be placed at the top, before any sections are defined:

```
openssl_conf = openssl_init
```

This should be added to the bottom of the file:

```
[openssl_init]
engines=engine_section
[engine_section]
pkcs11 = pkcs11_section
[pkcs11_section]
engine_id = pkcs11
# Wherever the engine installed by libp11 is. For example it could be:
# /usr/lib/arm-linux-gnueabi/hf/engines-1.1/libpkcs11.so
dynamic_path = /usr/lib/ssl/engines/libpkcs11.so
MODULE_PATH = /usr/lib/libcryptoauth.so
init = 0
```



## 4.1.6 Testing

To use p11tool it has to be installed:

```
# Debian like systems
$ sudo apt-get install gnutls-bin
# RPM based systems
$ yum install gnutls-utils
```

**Note:** If not using p11-kit-proxy then the provider has to be specified in p11tool calls:

```
$ p11tool --provider=/usr/lib/libcryptoauth.so
```

- Get the public key for a private key (as defined by the 0.conf file cited above):

```
$ p11tool --export-pubkey "pkcs11:token=0123EE;object=device;type=private"
warning: --login was not specified and it may be required for this operation.
warning: no --outfile was specified and the public key will be printed on screen.
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE9wzUq1EUAoNrG01rXYjNd35mxKuA
Ojw/k1IrNEBciSLL0TLjs/gvFS7N8AFXDK18vpxxu6yKzF2LRd7RY8yEFw==
-----END PUBLIC KEY-----
```

- Get the public key and decode it using OpenSSL

```
$ p11tool --export-pubkey "pkcs11:token=0123EE;object=device;type=private" | openssl pkey -pubin -text
-noout
warning: --login was not specified and it may be required for this operation.
warning: no --outfile was specified and the public key will be printed on screen.
Public-Key: (256 bit)
pub:
    04:f7:0c:d4:ab:51:14:02:83:6b:1b:4d:6b:5d:88:
    cd:77:7e:66:c4:ab:80:3a:3c:3f:92:52:2b:34:40:
    5c:89:22:cb:39:32:e3:b3:f8:2f:15:2e:cd:f0:01:
    57:0c:ad:7c:be:9c:71:bb:ac:a4:cc:5d:8b:45:de:
    dl:63:cc:84:17
ASN1 OID: prime256v1
NIST CURVE: P-256
```

- Create a CSR for the private key

```
$ openssl req -engine pkcs11 -key "pkcs11:token=0123EE;object=device;type=private" -keyform engine
-new -out new_device.csr -subj "/CN=NEW CSR EXAMPLE"
engine "pkcs11" set.
$ cat new_device.csr
-----BEGIN CERTIFICATE REQUEST-----
MIHVMHwCAQAwGjEYMBYGA1UEAwPTkVXIEN0U1BFWEFNUExFMFkwEwYHKoZIzj0C
AQYIKoZIzj0DAQcDQgAE9wzUq1EUAoNrG01rXYjNd35mxKuAOjw/k1IrNEBciSLL
OTLjs/gvFS7N8AFXDK18vpxxu6yKzF2LRd7RY8yEF6AAMAoGCCqGSM49BAMCA0kA
MEYCIQDUPElFpCOWtZxYJDYXPdl2UhpReVn6kK2LKCCX6byM8QIhAIfqfnggtcCi
W21xLAzabr8A4mHyfIIQ1oFYBg8QO9jZ
-----END CERTIFICATE REQUEST-----
```

- Verify the newly created csr

```
$ openssl req -in new_device.csr -verify -text -noout
verify OK
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: CN = NEW CSR EXAMPLE
  Subject Public Key Info:
    Public Key Algorithm: id-ecPublicKey
    Public-Key: (256 bit)
    pub:
        04:f7:0c:d4:ab:51:14:02:83:6b:1b:4d:6b:5d:88:
        cd:77:7e:66:c4:ab:80:3a:3c:3f:92:52:2b:34:40:
        5c:89:22:cb:39:32:e3:b3:f8:2f:15:2e:cd:f0:01:
        57:0c:ad:7c:be:9c:71:bb:ac:a4:cc:5d:8b:45:de:
        dl:63:cc:84:17
    ASN1 OID: prime256v1
    NIST CURVE: P-256
  Attributes:
    a0:00
  Signature Algorithm: ecdsa-with-SHA256
    30:46:02:21:00:d4:3d:e2:df:3d:c3:b0:b5:9c:58:24:36:17:
    3d:d9:76:52:1a:51:79:59:fa:90:ad:a5:28:20:97:e9:bc:8c:
    f1:02:21:00:87:ea:7e:78:20:b5:c0:a2:5b:6d:71:2c:0c:da:
    6e:bf:00:e2:61:f2:7c:82:10:d6:87:d8:06:0f:10:3b:d8:d9
```

## Chapter 5

# Application Support

This directory is for application specific implementation of various use cases.

Methods in this directory provide a simple API to perform potentially complex combinations of calls to the main library or API.

[app\\_info\\_ip\\_prot](#)

[app\\_info\\_pkcs11](#)

[app\\_info\\_secure\\_boot](#)



## Chapter 6

# Secure boot using ATECC608

8

The SecureBoot command is a new feature on the [ATECC608A](#) device compared to earlier CryptoAuthentication devices from Microchip. This feature helps the MCU to identify fraudulent code installed on it. When this feature is implemented, the MCU can send a firmware digest and signature to the ATECC608. The ATECC608 validates this information (ECDSA verify) and responds to host with a yes or no answer.

The ATECC608 provides options to reduce the firmware verification time by storing the signature or digest after a good full verification (FullStore mode of the SecureBoot command).

- When the ATECC608 stores the digest (SecureBootMode is FullDig), the host only needs to send the firmware digest, which is compared to the stored copy. This skips the comparatively lengthy ECDSA verify, speeding up the secure boot process.
- When the ATECC608 stores the signature (SecureBootMode is FullSig), the host only needs to send the firmware digest, which is verified against the stored signature using ECDSA. This saves time by not needing to send the signature in the command over the bus.

The ATECC608 also provides wire protection features for the SecureBoot command, which can be used to encrypt the digest being sent from the host to the ATECC608 and add a MAC to the verify result coming back to the host so it can't be forced to a success state. This feature makes use of a shared secret between the host and ATECC608, called the IO protection key.

The secure boot feature can be easily integrated to an existing project. The project should include the following files from the secure\_boot folder:

- [secure\\_boot.c](#)
- [secure\\_boot.h](#)
- [secure\\_boot\\_memory.h](#)
- [io\\_protection\\_key.h](#)

The project should also implement the following platform-specific APIs:

- `secure_boot_init_memory()`
- `secure_boot_read_memory()`

- `secure_boot_deinit_memory()`
- `secure_boot_mark_full_copy_completion()`
- `secure_boot_check_full_copy_completion()`
- `io_protection_get_key()`
- `io_protection_set_key()`

The project can set the secure boot configuration with the following defines:

- `SECURE_BOOT_CONFIGURATION`
- `SECURE_BOOT_DIGEST_ENCRYPT_ENABLED`
- `SECURE_BOOT_UPGRADE_SUPPORT`

The secure boot process is performed by initializing CryptoAuthLib and calling the [secure\\_boot\\_process\(\)](#) function.

## 6.1 Implementation Considerations

- Need to perform SHA256 calculations on the host. CryptoAuthLib provides a software implementation in [lib/crypto/atca\\_crypto\\_sw\\_sha2.c](#)
- When using the wire protection features:
  - The host needs to be able to generate a nonce (number used once). This is the NumIn parameter to the Nonce command that is sent before the SecureBoot command. The ATECC608 can not be used to generate NumIn, but it should come from a good random or non-repeating source in the host.
  - If the host has any protected internal memory, it should be used to store its copy of the IO protection key.
- Secure boot depends on proper protections of the boot loader code in the host. If the code can be easily changed, then the secure boot process can be easily skipped. Boot loader should ideally be stored in an immutable (unchangeable) location like a boot ROM or write-protected flash.
- Note that these APIs don't provision the ATECC608. They assume the ATECC608 has already been configured and provisioned with the necessary keys for secure boot.

## 6.2 Examples

For more information about secure boot, please see the example implementation project and documentation at: [https://github.com/MicrochipTech/cryptoauth\\_usecase\\_secureboot](https://github.com/MicrochipTech/cryptoauth_usecase_secureboot)

## Chapter 7

# Contribution Guidelines

While this is an open source project there are a few considerations that make it somewhat unique in how it is managed. The first issue is that the development workflow is a hybrid between internal development and CI/CD systems and external develop and associated CI/CD systems.

- This project contains a mixture of licenses depending on the section. The vast majority is under a Microchip proprietary license that is restrictive.
- Contributors must be aware of the specific license they are working under and must be aware that by submitting the patch that they agree to the terms of the license covering the target file.
- Sources contained in the `third_party` path are covered by true open source licenses and as such are not bound by Microchip's license restrictions.
- Third party contributions for HALs must be licensed under MIT, BSD (3 clause), or Apache 2.0 license and are placed in `third_party/hal/<platform>`
- Pull requests (PR) must attest to reviewing of these rules, that licensing terms have been reviewed, the submitter has approval to submit the changes under the target license terms.



## **Chapter 8**

### **openssl directory - Purpose**

This directory contains the interfacing and wrapper functions to integrate openssl as the software crypto library.





## Chapter 9

# Python CryptoAuthLib module

### 9.1 Introduction

This module provides a thin python ctypes layer to evaluate the cryptauthlib interface to Microchip Crypto↔ Authentication devices.

#### 9.1.1 Code Examples

Code examples for python are available on github as part of [CryptoAuthTools](#) under the [python/examples](#) directory

### 9.2 Installation

#### 9.2.1 CryptoAuthLib python module can be installed through Python's pip tool:

```
pip install cryptauthlib
```

#### 9.2.2 To upgrade your installation when new releases are made:

```
pip install -U cryptauthlib
```

#### 9.2.3 If you ever need to remove your installation:

```
pip uninstall cryptauthlib
```

### 9.3 What does python CryptoAuthLib package do?

CryptoAuthLib module gives access to most functions available as part of standard cryptauthlib (which is written in 'C'). These python functions for the most part are very similar to 'C' functions. The module in short acts as a wrapper over the 'C' cryptauth library functions.

Microchip cryptauthlib product page: [Link](#)

## 9.4 Supported hardware

- AT88CK101
- CryptoAuthentication SOIC XPRO Starter Kit (DM320109)

## 9.5 Supported devices

The family of devices supported currently are:

- ATSHA204A
- ATECC108A
- ATECC508A
- ATECC608A

## 9.6 Using cryptoauthlib python module

The following is a 'C' code made using cryptoauthlib 'C' library.

```
#include "cryptoauthlib.h"
void main()
{
    ATCA_STATUS status;
    uint8_t revision[4];
    uint8_t randomnum[32];
    status = atcab_init(cfg_ateccx08a_kitcdc_default);
    if (status != ATCA_SUCCESS)
    {
        printf("Error");
        exit();
    }
    status = atcab_info(revision);
    if (status != ATCA_SUCCESS)
    {
        printf("Error");
        exit();
    }
    status = atcab_random(randomnum);
    if (status != ATCA_SUCCESS)
    {
        printf("Error");
        exit();
    }
}
```

The same code in python would be:

```
from cryptoauthlib import *
ATCA_SUCCESS = 0x00
revision = bytearray(4)
randomnum = bytearray(32)
# Locate and load the compiled library
load_cryptoauthlib()
assert ATCA_SUCCESS == atcab_init(cfg_ateccx08a_kithid_default())
assert ATCA_SUCCESS == atcab_info(revision)
print("".join(['%02X ' % x for x in revision]))
assert ATCA_SUCCESS == atcab_random(randomnum)
print("".join(['%02X ' % x for x in randomnum]))
```

In the above python code, "import cryptoauthlib" imports the python module. load\_cryptoauthlib() function loads the compiled library. The load\_cryptoauthlib() is a function that you will not see in the 'C' library, this is a python specific utility function and is required for python scripts to locate and load the compiled library.

## 9.7 In Summary

### 9.7.1 Step I: Import the module

```
from cryptoauthlib import *
```

### 9.7.2 Step II: Initilize the module

```
load_cryptoauthlib()  
assert ATCA_SUCCESS == atcab_init(cfg_ateccx08a_kithid_default())
```

### 9.7.3 Step III: Use Cryptoauthlib APIs

Call library APIs of your choice

## 9.8 Code portability

Microchip's CryptoAuthentication products can now be evaluated with the power and flexibility of python. Once the evaluation stage is done the python code can be ported to 'C' code.

As seen above the python API maintains a 1 to 1 equivalence to the 'C' API in order to easy the transition between the two.

## 9.9 Cryptoauthlib module API documentation

### 9.9.1 help() command

All of the python function's documentation can be viewed through python's built in help() function.

For example, to get the documentation of [atcab\\_info\(\)](#) function:

```
>> help(cryptoauthlib.atcab_info)  
Help on function atcab_info in module cryptoauthlib.atcab:  
atcab_info(revision)  
Used to get the device revision number. (DevRev)  
Args:  
    revision          4-byte bytearray receiving the revision number  
                      from the device. (Expects bytearray)  
Returns:  
    Status code
```

### 9.9.2 dir() command

The dir command without arguments, return the list of names in the current local scope. With an argument, attempt to return a list of valid attributes for that object. For example `dir(cryptoauthlib)` will return all the methods available in the cryptoauthlib module.

## 9.10 Code Examples

Code examples for python are available on github as part of [CryptoAuthTools](#) under the python/examples directory

## 9.11 Tests

Module tests can be located in the [python/tests](#) of the main cryptoauthlib repository. The [README.md](#) has details for how to run the tests. The module tests are not comprehensive for the entire functionality of cryptoauthlib but rather are meant to test the python module code only against the library to ensure the interfaces are correct and ctypes structures match the platform.

## 9.12 Release notes

See Release Notes

## Chapter 10

# Python CryptoAuthLib Module Testing

### 10.1 Introduction

These tests are designed to only test the python interface to the library and are not designed to test the library itself which is covered by the main cryptoauthlib tests

#### 10.1.1 Running

The best way to run the test suite is to use `tox` which can be easily installed with pip:

```
$ pip install tox
```

From the python folder:

```
~/cryptoauthlib/python $ tox
```

It is possible to directly run tests but requires more setup

1) Install pytest

```
$ pip install pytest
```

2) Modify the PYTHONPATH environment variable

Windows:

```
cryptoauthlib/python> set PYTHONPATH=<path_to>/cryptoauthlib/python
```

Linux:

```
$ export PYTHONPATH=${PYTHONPATH}:<path_to>/cryptoauthlib/python
```

3) Run the tests

```
$ pytest -vv
```

#### 10.1.2 Test options

There are additional options that can be invoked with the tests that define what tests will be run

1) `--with-lib` will attempt to run tests against the compiled c library. These tests are good for detecting possible platform incompatibilities between the C compiler and the expectations of python

2) `--with-device` will attempt to invoke some tests with a real attached device These tests are restricted to only the minimum required to verify the python to library connectivity and are only meant to detect situations can not be determined from the library tests alone.



# Chapter 11

## Microchip Cryptoauthlib Release Notes

### 11.1 Release v3.7.5 (06/26/2024)

#### 11.1.1 New Features

- In PKCS11 module, added ECCP384,ECCP521,ECCP224 elliptic curves support for ECC key operations, in addition to the existing ECCP256 support
- Enhanced certificate related tests to include coverage for ECC204 and TA010 devices
- Added a new ATCA\_HEAP internal macro check in place of ATCA\_NO\_HEAP for dynamic memory usages
- Added an additional test to validate AES-CBC encrypt/decrypt APIs using CAVP's AES multiblock message test (MMT) sample vectors
- See [talib/CHANGES.md] for details on talib module changes

#### 11.1.2 Fixes

- Fixed atcacert\_get\_comp\_cert() API to support certificates with expiry dates beyond year 2031
- Fixed [atcacert\\_read\\_cert\(\)](#) API to consider serial number as source while processing extracted certificates
- Fixed [atcacert\\_write\\_cert\(\)](#) API to support X509 certificates with an odd byte length, without any additional padding
- Fixed calib\_execute\_send() to consider correct data buffer when ATCA\_HAL\_LEGACY\_API is used
- PKCS11 layer fixes/updates
  - Fixed certificate chain/key export failures in ECC608 Trust devices
  - Fixed memory leak during C\_Finalize API call usage in a multi-slot configuration

#### 11.1.3 API Changes

- Added atcacert\_generate\_sn() API in atcacert module to generate certificate serial number from a valid serial number source



## 11.2 Release v3.7.4 (03/08/2024)

### 11.2.1 New Features

- Updated wolfSSL interface `atcac` wrapper APIs usage for AES GCM encrypt/decrypt similar to MbedTLS and openssl library wrapper APIs
- Added package.yml file to support MPLAB Harmony metadata package format

### 11.2.2 Fixes

- Fixed `calib_wakeup_i2c` API to follow specified i2c wakeup sequence for ECC608 devices
- PKCS11 layer fixes/updates
  - Lock usage optimization in `pkcs11_find_continue` API
  - `pkcs11_digest` API updates for SHA context memory allocation
  - `pkcs11_token_set_pin` API updates to write data based on generated GCM key size
- Fixed `atcacert_get_comp_cert` API to remove a redundant `atcacert_date_enc_compcert` call
- Resolved build warnings/issues in Windows, Linux and 8-bit (XC8) platforms
- wolfSSL's `atcac_pk_init_pem` wrapper API updates to use `wc_PEM` to DER functions
- Fixed broken links in README.md files

## 11.3 Release v3.7.3 (01/31/2024)

### 11.3.1 New Features

- In PKCS11 module, added cache support to store `Key id` attribute of key type objects into stack memory and use it for subsequent accesses

### 11.3.2 Fixes

- Fixed `calib_sha_hmac_finish` api to set mode value correctly for ECC204, TA010 and ECC608 devices
- Fixed memory leak in MbedTLS configuration
- Fixed build errors when a project is generated with PKCS11 Component enabled in MPLAB Harmony Configurator (MHC)

## 11.4 Release v3.7.2 (01/19/2024)

### 11.4.1 New Features

- See [talib/CHANGES.md] for details on talib module changes

### 11.4.2 Fixes

- Updated PKCS11 token info to list TA101 device details
- Fixed compilation errors when ECC508 device is enabled
- See [talib/CHANGES.md] for details on talib module fixes

### 11.4.3 API Changes

- Added sign and verify API in talib module to support 1024 bytes ED25519 mode

## 11.5 Release v3.7.1 (12/15/2023)

### 11.5.1 New Features

- PKCS11 module enhancements for x509 public key certificates
  - Added more certificate attributes to x509 public key certificates. These attributes include certificate start date, certificate end date, subject, subject key, DER encoded certificate issuer name, DER encoded certificate serial number and hash of the issuer public key.
  - Added cache support to store these certificates into stack memory and utilize it for parsing the above specified certificate attributes.
- See [talib/CHANGES.md] for details on talib module changes

### 11.5.2 Fixes

- Updated atcab\_read\_config\_zone to support SHA106
- For Linux platforms, i2c baud rate is always set to 100 khz as the default configuration
- Resolved build errors when ATCA\_USE\_SHARED\_MUTEX is disabled
- Resolved build error with ATCA\_JWT\_EN

### 11.5.3 API Changes

- Added atcacert\_get\_subject api to get the subject name from public x509 certificates
- Added atcacert\_get\_issuer api to get the issuer name from public x509 certificates
- Updated the [atcacert\\_def\\_s](#) structure to include x509 full certificates support

## 11.6 Release v3.7.0 (09/08/2023)

### 11.6.1 New Features

- Added unified buffer implementation to enable multipart buffer use with APIs that support them.
- See [talib/CHANGES.md] for details on talib module changes

### 11.6.2 Fixes

- Made `atcac` structures referencing third party libraries opaque to the user so installed header files are usable by applications without also including the third party headers.

### 11.6.3 API Changes

- The software crypto structures are generally no longer typedef'd so they must be declared with the `struct` keyword. New typedefs were added by appending the suffix `_t` which allows for the same mechanism for declaring these structure in code if building a standalone application (such as in embedded projects). If dynamically linking with the library and using a third party crypto library one will need to use the `_new` & `_free` APIs to allocate these structures for use with the `atcac` interfaces.

## 11.7 Release v3.6.1 (07/14/2023)

### 11.7.1 New Features

- Added support for PIC18 memory model with a `MAX_PACKET_SIZE` setting.
- PKCS11 Improvement to support context reservation automatically for operations that span multiple `pkcs11` calls such as login/logout, encrypt/decrypt, etc. This prevents concurrent processes from interrupting init-update-finish operations in PKCS11
- Added support for data element transfers between trust anchor devices

### 11.7.2 Fixes

- PKCS11: resolved issues with configuration directory parsing to ensure configurations parse in the correct order and any extraneous files get properly rejected.
- PKCS11: improved public key loading logic for trust anchor handles to use the most appropriate mechanism based on handle configuration.
- Fixed minimal kit host implementation in support bridging to SPI by using select and deselect control commands

## 11.8 Release v3.6.0 (04/04/2023)

### 11.8.1 New Features

- Compliance certified to CERT-C Level 2 & MISRA 2012. Compliance reports can be requested from your FAE or account manager
- Added `talib_handle` helper functions to determine if a handle access type is allowed in the given auth session

### 11.8.2 Fixes

- pkcs11 public key for private keys requiring the token to be logged in will make a best effort to return a value by detecting various storage methods.
- pkcs11 encrypt/decrypt update calls return the maximum possible bytes per the selected algorithm.
- pkcs7 would return the wrong padding for `length % 16 == 0`
- hmac counter kdf method will default to digest length specified in bits

### 11.8.3 API Changes

- ATCA\_STATUS enum is now an integer and all APIs return type ATCA\_STATUS
- atcacert API return type is now ATCA\_STATUS rather than `int`
- atcac\_sw\_sha... API return type is now ATCA\_STATUS rather than `int`
- `_atcab_exit` has been removed (includes `_calib_exit` and `_talib_exit`)
- `_gDevice` has been renamed to `g_atcab_device_ptr` (one should be using `atcab_get_device()`)

## 11.9 Release v3.5.1 (03/26/2023)

### 11.9.1 New Features

- Add support for SHA104, SHA105, & SHA106

## 11.10 Release v3.5.0 (03/14/2023)

### 11.10.1 New Features

- Add support for ECC204, TA010 and framework for future devices

## 11.11 Release v3.4.3 (12/23/2022)

### 11.11.1 New Features

- Add key load mode flags for FCE config command

### 11.11.2 Fixes

- WPC certificate reconstruction buffer length was too short
- ECC204 block Read/Write did not write remaining bytes if the provided buffer was not padded to a 32 byte boundary
- TA100 lock CRC was being passed with the native endianness.
- ECC204 nonce command was missing the mode bit to emit a random number when called with the intention of producing random bytes

## 11.12 Release v3.4.2 (12/04/2022)

### 11.12.1 Fixes

- PKCS11: Correct init/deinit failures from initialization mutex options. These would manifest as a segmentation fault on deinit, unterminated authorization sessions, or library already initialized return codes based on the configuration and initialization data.
- PKCS11: Added configuration option to always terminate authorization sessions on library initialization to work around applications that may fail to call `C_CloseSession` or `C_Finalize` before exiting.
- PKCS11: Fix failures in `C_DigestInit` resulting from failing to check the session state before checking the requested digest mechanism type.
- PKCS11: Modify how the library returns public key information based on access levels of the private key (generate from the private key if allowed, read from a linked public key, and finally return data unavailable). For the vast majority of situations this prevents openssl & libp11 from crashing with segmentation faults if the user fails to provide a pkcs11 URI with pin value specified. These segmentation faults were confirmed to also exist with other PKCS11 libraries - the fundamental problem should be taken up with the maintainers of openssl, libp11, and pkcs11-provider (experimental OpenSSL 3.0 PKCS11 support).
- Modified CBC update/finish APIs (added as an experimental API in v3.4.0) to match standard expectations of how the APIs would function. Updated algorithm tests to reflect this usage.
- PKCS11: Updated encrypt/decrypt in cbc/cbcpad modes to use the updated algorithm implementations
- talib full element read & write functions now account for the maximum packet size based on session state.

## 11.13 Release v3.4.1 (11/11/2022)

### 11.13.1 Fixes

- `test_atcacert_build_start_signer` modified to verify the structure fields since the structure is no longer packed
- Python `ctypes_to_bytes` routine to work for all python versions
- Pkcs11 signature rules to match section 5.2 of the specification
- Compilation error when PKCS11 monotonic counter is enabled
- Compilation error when no HALs are specified during configuration
- Align ECC204 and cryptoauth counter APIs

## 11.14 Release v3.4.0 (10/27/2022)

### 11.14.1 New Features

- Added framework for fine grain library configuration including configuration check header files `<api>_↔ config_check.h` see [lib/atca\\_config\\_check.h](#) for the top level header
- Added WPC application files with reference message generation/parsing and library configuration file to optimize to the smallest footprint
- TA100 read/write apis updated to segment incoming buffer into partial read/write operations if it exceeds the maximum supported packet size
- Added PKCS7 padding algorithm for use with AES-CBC
- Expose PKCS11 configuration options to CMake configuration

### 11.14.2 Fixes

- Improve ECC204 apis to match cryptoauthlib apis and abstract the device differences
- Support for strict C99 compliance and clean up warnings from -Wall and pedantic levels
- Add rsa2048 key size support to talib\_rsaenc command
- Fix for ta100 devupdate to set the proper auth session exit flags so the library will properly reconnect when the ta100 reboots
- Fix ECC608 verify failure when ReqRandom bit is set for a stored public key by using tempkey in this situation rather than the message digest buffer. See the ECC608 datasheet for more details of this special condition
- Improve ta100 auth session handling of long messages by reporting the message size exceeds the wrapped message limit earlier in the packet creation process
- Fixes and Improvements for PKCS11 interface based on compliance testing

## 11.15 Release v3.3.3 (10/06/2021)

### 11.15.1 New features

- Added Zephyr support and zephyr driver api HALs for I2C & SPI. Adding cryptoauthlib to a zephyr project CMakeLists.txt is now possible - use subdirectory(cryptoauthlib/lib). One can also include the repo in the west manifest
- Added SWI device support for linux platforms using hardware uarts
- Added contributing guidelines and PR process documentation
- SWI bitbang driver for harmony - supports Atmel SWI and ECC204 protocols

### 11.15.2 Fixes

- Wolfssl build errors when generating MHC projects containing wolfssl
- Removed zero length aad limitation in CCM implementation
- Changed ECC204 zone identifiers and slot types to align with cryptoauthlib standard forms
- XC8/XC16 build warnings
- Several pkcs11 fixes - token\_init deadlock, null num\_in for private key writes, fsecret key length parsing, object\_create failing, etc
- Null pointer access violation in atcab\_release when using a native hal and double free in openssl implementation of atcac\_pk\_verify

## 11.16 Release v3.3.2 (06/20/2021)

### 11.16.1 New features

- All memory allocations now go through the hal\_platform definitions. In harmony these are the OSAL\_fuctions which work with any of the supported RTOS'.
- Enable multiple interfaces in the Harmony 3 test project through the user interface.
- Kit protocol over UART has been added. This can be paired with the included hosting application
- Simple kit protocol hosting application has been added. It is available in app/kit\_host and through Harmony 3. This is a preview release of the application.

## 11.16.2 Fixes

- Enable ATSHA206A api in the python extension
- Made the linux i2c configuration default to 100khz so they should work again without having to make modifications to the baud rate field.
- Fix pkcs11 static configuration option when used with the trust platform configuration file
- Fix PKCS11 ec\_point return value when pValue is null (libp11 checks the size in this manner before requesting it for real).
- Fix warnings generated by missing end of file newlines.
- Removed legacy (empty) START header references.

## 11.17 Release v3.3.1 (04/23/2021)

### 11.17.1 New features

- Core support for kit protocol over serial ports (i.e. tty/COM ports)
- PKCS11 support for TA100 auth sessions

### 11.17.2 Fixes

- Fix mbedtls integration combinations that would produce unexpected behavior. All variations of sign/verify \_ALT now work as expected given a configured key (for example if a key is configured as a stored public and VERIFY\_ALT is enabled then library will perform a stored key verify rather than an external public key load and verify)
- Added mbedtls integration tests to confirm that integrations are working on a target platform as expected. These generally bootstrap using NIST example vectors before using the validated functions/algorithms to test the remaining integration.
- Clean up warnings when run with very strict settings (-Wall -Wextra -pedantic -Werror)
- Fix false wake errors when baud rate switching for I2C
- Fix for I2C errors that could be created on the bus when there are devices on the bus that support general calls - this fix should also correct linux zero length kernel messages when enabled.
- Fix ESP32 HAL to work with the updated HAL structure.

## 11.18 Release v3.3.0 (01/22/2021)

### 11.18.1 API Updates

- HAL API has been significantly revised to improve portability. This update simplifies the requirements of each HAL to only the physical transport mechanisms. Please see the hal porting and library upgrading notes: <https://github.com/MicrochipTech/cryptoauthlib/wiki/Upgrading-to-v3.3>
- Internal structures have been updated by removing obsolete elements and combining mandatory fields. This saves significant memory in both program and data regions.
- Inclusive language update: all remaining legacy language elements have been updated. Where this impacts the external API there is the option ATCA\_ENABLE\_DEPRECATED to use the previous names.

### 11.18.2 New features

- ECC204 support has been added with one wire HAL support.
- ECC204, SHA206, one wire and single wire (uart and gpio) hals have been added to the Harmony 3 configurator.
- PKCS11 support for symmetric (AES & HMAC) keys has been added and enabled for additional mechanisms such as HMAC signing and AES encrypt/decrypt

### 11.18.3 Fixes

- pkcs11\_token\_init had several conditions that were corrected
- fix to detect differences in i2c clock rate specifications between flexcom and sercom configurators in Harmony 3 and the emit the correct value for the cryptoauthlib interface config structure.

## 11.19 Release v3.2.5 (11/30/2020)

### 11.19.1 New features

- TA100 ShareKey API to drive the sharekey process (requires NDA, consult with your FAE or submit a request through your myMicrochip account)
- Additional software crypto library interface functions for asymmetric cryptography (sign, verify, ecdh, etc)
- XC8 & XC16 compiler support
- AES CCM & CBC-MAC upper layer API using AES-ECB primitives

### 11.19.2 Fixes

- TA100 AES-GCM auth session tx packet length when command data is included
- PKCS11 Pin length check rejecting valid pin lengths
- aes-gcm nist vector test failed with mbedtls crypto backend due to aad update not being executed when aad length was zero

## 11.20 Release v3.2.4 (10/17/2020)

### 11.20.1 New features

- Additional TA100 command support (requires NDA, consult with your FAE or submit a request through your myMicrochip account)
- Library build and install on linux now also installs the headers that were used to build the library including all configuration files like atca\_config.h - customer applications building against the library will need to add the include/cryptoauthlib to their include search paths



## 11.20.2 Fixes

- Fixed errors produced when -fno-common was used during build of the library by resolving the variable declaration and exporting macros (tested with static/dynamic linkage on linux & windows platforms)
- Added a timeout during i2c plib commands in the Harmony3 hals to prevent system lockups from failed peripheral transfers that don't return errors.

## 11.21 Release v3.2.3 (09/12/2020)

### 11.21.1 New features

- Additional TA100 command support (requires NDA, consult with your FAE or submit a request through your myMicrochip account)

### 11.21.2 Fixes

- Security patch for USB HALs. Removed deprecated HALs and removed enumeration from the hidapi HAL.
- Fix device matching logic to support older kits when using "auto detect" settings in the interface configuration
- Fix SPI HAL generation errors for SAMG55 & SAM71 (flexcom) devices
- Added a timeout for Harmony I2C calls to prevent infinite loops on peripheral failures. If a loop exists inside the peripheral library then it may still cause processor spins until a watchdog reset.

## 11.22 Release v3.2.2 (07/28/2020)

### 11.22.1 New Features

- ATECC608B support added

### 11.22.2 Fixes

- Consistent null pointer checks between calib & talib apis. Tracing enabled for most all status changes
- Fix for pkcs11 ecdh with the legacy slot write mode and encrypted read to pull the read key id from the correct slot (private key slot | 0x01)
- call the proper api from atcab\_init\_ext so it works with device structures that are not the global instance

## 11.23 Release v3.2.1 (06/29/2020)

### 11.23.1 Fixes

- PKCS11 configuration option to set token label to the device serial number
- Fix OSX CLANG macro error
- Add missing c++ wrapper macros to calib\_basic.h
- Ensure atcab\_init\_ext calls atcab\_release\_ext rather than atcab\_release

## 11.24 Release v3.2.0 (06/10/2020)

### 11.24.1 New features

- TA100 device support (requires NDA, consult with your FAE or submit a request through your myMicrochip account)
- Extension of the existing API to support device context retention to allow multiple independent contexts to be maintained. The application still needs to ensure concurrency protections are used in the application to guard bus communication.
- PKCS11 support has been moved into the main library and will be maintained together.
- TNG/TFLEX support has been added to PKCS11 so enabling a TNG part in pkcs11 can be done by specifying the part number: `device = ATECC608A-TNGTLS`
- Several cryptographic library integrations have been added to enable additional host/mcu side functionality. This includes replacing cryptoauthlib software implementations of sha1 & sha256 with your preferred library. For example using WolfSSL in Harmony 3 will also enable hardware acceleration of those cryptographic functions. Cryptographic libraries enabled: WolfSSL, mbedTLS, & OpenSSL
- Changes to atcacert ("compressed" certificate processing) to enable exact certificate size retrieval which will help with some use cases that had issues with the max possible size answers.
- Consolidation of HALs into device families rather than exact processor model This should reduce the amount of effort required to port the library to a specific platform if the framework is one that is already known.

### 11.24.2 Known issues

- Power modes/states for the TA100 are not automatically controlled by the library so the application has to manually change the power state when lower power modes are required. A command such as the info command will wake the TA100 from sleep but will produce an error. Try another command after the specified time to ensure communication is restored. This behavior is detailed in the datasheet.
- Several TA100 commands and features are planned for the next released of the library such as import/export, transfer, and devupdate.

## 11.25 Release v3.1.1 (03/06/2020)

- Update Trust Flex certificates. Add compile time options to reduce code space by selectively including the trust certificates that are required
- Python updates: add sha206 apis. Fix atcab\_kdf parameters
- Fix compiler warnings in test application files and sha206 api

## 11.26 Release v3.1.0 (02/05/2020)

- The library is now semantic versioned along with the legacy date versioning. Python will continue to be released with the date version. Version APIs have been updated.
- Configuration is done via a configuration file `atca_config.h` rather than global compiler options. You have to add this file to your project to support this version of the library.
- Harmony 3 support has been added. Update harmony configurator (and content loader) or manually clone cryptoauthlib into your harmony directory.
- Additional Compiler support has been added for IAR-ARM and ARMCC

## 11.27 Release 11/22/2019

- Patches for CVE-2019-16128 & CVE-2019-16129: Ensure reported packet length is valid for the packet being processed.
- Improvement to encrypted read operations to allow supply of a host nonce (prevent replay of a read sequence to the host). Default API is changed but can be reverted by setting the option `ATCA_USE_CONSTANT_HOST_NONCE`
- Added Azure compatible TNGTLS and TNGLORA certificates. Use the TNG client API to retrieve the proper certificate based on the device.
- Misc Python updates (updated APIs for encrypted reads to match the C-API change) `atcacert_cert_element_t` now initializes properly

## 11.28 Release 08/30/2019

- Added big-endian architecture support
- Fixes to `atcah_gen_dig()` and `atcah_nonce()`

## 11.29 Release 05/17/2019

- Added support for TNG devices (cert transforms, new API)
- `atcab_write_pub_key()` now works when the data zone is unlocked

## 11.30 Release 03/04/2019

- mbed TLS wrapper added
- Minor bug fixes

## 11.31 Release 01/25/2019

- Python JWT support
- Python configuration structures added
- Restructure of secure boot app

## 11.32 Release 01/04/2019

- Added GCM functions
- Split AES modes into separate files
- Bug fix in SWI START driver

## 11.33 Release 10/25/2018

- Added basic certificate functions to the python wrapper.
- Added Espressif ESP32 I2C driver.
- Made generic Atmel START drivers to support most MCUs in START.
- Added AES-CTR mode functions.
- Python wrapper functions now return single values with AtcaReference.
- Added mutex support to HAL and better support for freeRTOS.

## 11.34 Release 08/17/2018

- Better support for multiple kit protocol devices

## 11.35 Release 07/25/2018

- Clean up python wrapper

## 11.36 Release 07/18/2018

- Added ATCA\_NO\_HEAP define to remove use of malloc/free.
- Moved PEM functions to their own file in atcacert.
- Added wake retry to accomodate power on self test delay.
- Added ca\_cert\_def member to [atcacert\\_def\\_s](#) so cert chains can be traversed as a linked list.

## 11.37 Release 03/29/2018

- Added support for response polling by default, which will make commands return faster (define ATCA\_NO←\_POLL to use old delay method).
- Removed atcatls related files as they were of limited value.
- Test framework generates a prompt before locking test configuration.
- Test framework puts device to sleep between tests.
- Fixed mode parameter issue in atcah\_gen\_key\_msg().
- ATECC608A health test error code added.

## 11.38 Release 01/15/2018

- Added AES-128 CBC implementation using AES command
- Added AES-128 CMAC implementation using AES command

## 11.39 Release 11/22/2017

- Added support for FLEXCOM6 on SAMG55 driver

## 11.40 Release 11/17/2017

- Added library support for the ATECC608A device
- Added support for Counter command
- `atca_basic` functions and tests now split into multiple files based on command
- Added support for multiple base64 encoding rules
- Added support for JSON Web Tokens (jwt)
- Fixed `atcab_write_enc()` function to encrypt the data even when the device is unlocked
- Fixed `atcab_base64encode_()` for the extra newline
- Updated `atcab_ecdh_enc()` to work more consistently

## 11.41 Release 07/01/2017

- Removed assumption of `SN[0:1]=0123`, `SN[8]=EE`. SN now needs to be passed in for functions in `atca_host` and `atca_basic` functions will now read the config zone for the SN if needed.
- Renamed `atcab_gendig_host()` to `atcab_gendig()` since it's not a host function. Removed original `atcab_gendig()`, which had limited scope.
- Fixed `atca_hmac()` for host side HMAC calculations. Added `atcab_hmac()`.
- Removed unnecessary `ATCADeviceType` parameters from some `atca_basic` functions.
- Added `atcacert_create_csr()` to create a signed CSR.
- New HAL implementation for Kit protocol over HID on Linux. Please see the Incorporating CryptoAuthLib in a Linux project using USB HID devices section in this file for more information.
- Added `atcacert_write_cert()` for writing certificates to the device.
- Added support for dynamic length certificate serial numbers in `atcacert`.
- Added `atcab_write()` for lower level write commands.
- Fixed `atca_write_auth_mac()`, which had wrong OpCode.
- Added `atcab_verify()` command for lower level verify commands.
- Added `atcab_verify_stored()` for verifying data with a stored public key.

- Removed `atcab_write_bytes_slot()`. Use `atcab_write_bytes_zone()` instead.
- Modified `atcab_write_bytes_zone()` and `atcab_read_bytes_zone()` to specify a slot
- Added `atcab_verify_validate()` and `atcab_verify_invalidate()`
- Improvements to host functions to handle more cases.
- Added `atcab_updateextra()`, `atcab_derive_key()`
- Added support for more certificate formats.
- Added general purpose hardware SHA256 functions. See `atcab_hw_sha2_256()`.
- Removed device specific config read/write. Generic now handles both.
- Removed unnecessary response parameter from lock commands.
- Enhanced and added unit tests.
- Encrypted read and write functions now handle keys with `SlotConfig.NoMac` set
- `atcab_cmp_config_zone()` handles all devices now.
- Fixed some edge cases in `atcab_read_bytes_zone()`.
- Updated `atSHA()` to work with all devices.
- Fixed `atcacert_get_device_locs()` when using stored sn.

## **11.42 Release 01/08/2016**

- New HAL implementations for
  - Single Wire interface for SAMD21 / SAMR21
  - SAMV71 I2C HAL implementation
  - XMega A3Bu HAL implementation
- Added `atcab_version()` method to return current version string of library to application
- New Bus and Discovery API
  - returns a list of ATCA device configurations for each CryptoAuth device found
  - currently implemented on SAMD21/R21 I2C, SAMV71
  - additional discovery implementations to come
- TLS APIs solidified and documented
- Added missing doxygen documentation for some CryptoAuthLib methods
- Stubs for HAL SPI removed as they are unused for SHA204A and ECC508A support
- bug fixes
- updated `atcab_sha()` to accept a variable length message that is  $> 64$  bytes and not a multiple of 64 bytes (the SHA block size).
- refactored Cert I/O and Cert Data tests to be smaller
- 'uncrustify' source formatting
- published on GitHub

## 11.43 Release 9/19/2015

- Kit protocol over HID on Windows
- Kit protocol over CDC on Linux
- TLS integration with ATECC508A
- Certificate I/O and reconstruction
- New SHA2 implementation
- Major update to API docs, Doxygen files found in cryptoauthlib/docs
- load [cryptoauthlib/docs/index.html](http://cryptoauthlib/docs/index.html) with your browser

## Chapter 12

# Security Policy

We take the security of cryptauthlib very seriously. Please submit security vulnerabilities to the Microchip Product Security Incident Response Team (PSIRT) which is responsible for receiving and responding to reports of potential security vulnerabilities in our products, as well as in any related hardware, software, firmware, and tools. Please see below for instructions on how to submit your report.

### 12.1 Supported Versions

The previous API version is maintained for a year after a new version is released.

Version	Supported	Notes
3.7.x	:heavy_check_↔ mark:	
3.6.x	:heavy_check_↔ mark:	Support Ends September 8 2024
3.5.x	:heavy_check_↔ mark:	Support Ends April 4 2024
3.4.x	:heavy_check_↔ mark:	Support Ends March 14 2024
3.3.x	:x:	
3.2.x	:x:	
< 3.2	:x:	

### 12.2 Reporting a Vulnerability

#### How to Report Potential Product Security Vulnerabilities

Once a report is received, the PSIRT will take the necessary steps to review the issue and determine what actions might be required to address any potential impacts to our products. Microchip PSIRT follows a coordinated vulnerability responsible disclosure policy that is available for review.

Please use the above instructions to securely submit your findings - We ask that you refrain from reporting vulnerabilities through the public github issues system.





## Chapter 13

# Deprecated List

### Global **atcab\_init\_device** (ATCADevice ca\_device)

This function is not recommended for use generally. Use of `_ext` is recommended instead. You can use `atcab↵_init_ext` to obtain an initialized instance and associated it with the global structure - but this shouldn't be a required process except in extremely unusual circumstances.

### Global **atidle** (ATCAIface ca\_iface)

This function does not have defined behavior when `ATCA_HAL_LEGACY_API` is undefined.

### Global **atsleep** (ATCAIface ca\_iface)

This function does not have defined behavior when `ATCA_HAL_LEGACY_API` is undefined.

### Global **atwake** (ATCAIface ca\_iface)

This function does not have defined behavior when `ATCA_HAL_LEGACY_API` is undefined.



# Chapter 14

## Module Index

### 14.1 Modules

Here is a list of all modules:

TNG API (tng_) . . . . .	73
Basic Crypto API methods (atcab_) . . . . .	80
Configuration (cfg_) . . . . .	163
ATCADevice (atca_) . . . . .	163
ATCAIface (atca_) . . . . .	166
Certificate manipulation methods (atcacert_) . . . . .	174
Basic Crypto API methods for CryptoAuth Devices (calib_) . . . . .	205
Software crypto methods (atcac_) . . . . .	216
Hardware abstraction layer (hal_) . . . . .	216
Host side crypto methods (atcah_) . . . . .	255
JSON Web Token (JWT) methods (atca_jwt_) . . . . .	260
mbedTLS Wrapper methods (atca_mbedtls_) . . . . .	260
Attributes (pkcs11_attr_) . . . . .	263



## Chapter 15

# Namespace Index

### 15.1 Namespace List

Here is a list of all documented namespaces with brief descriptions:

<a href="#">cryptoauthlib</a>	277
<a href="#">cryptoauthlib.atcab</a>	277
<a href="#">cryptoauthlib.atcacert</a>	327
<a href="#">cryptoauthlib.atcaenum</a>	332
<a href="#">cryptoauthlib.atjwt</a>	333
<a href="#">cryptoauthlib.device</a>	333
<a href="#">cryptoauthlib.exceptions</a>	334
<a href="#">cryptoauthlib.iface</a>	335
<a href="#">cryptoauthlib.library</a>	337
<a href="#">cryptoauthlib.sha206_api</a>	344
<a href="#">cryptoauthlib.status</a>	349
<a href="#">cryptoauthlib.tng</a>	350
<a href="#">test_device</a>	354
<a href="#">test_iface</a>	356



## Chapter 16

# Hierarchical Index

### 16.1 Class Hierarchy

This inheritance list is sorted roughly, but not completely, alphabetically:

<code>_ascii_kit_host_context</code>	357
<code>cryptoauthlib.library._CtypeIterator</code>	366
<code>_kit_host_map_entry</code>	366
<code>atca_check_mac_in_out</code>	373
<code>atca_decrypt_in_out</code>	374
<code>atca_delete_in_out</code>	374
<code>atca_derive_key_in_out</code>	375
<code>atca_derive_key_mac_in_out</code>	375
<code>atca_device</code>	376
<code>atca_diversified_key_in_out</code>	377
<code>atca_evp_ctx</code>	377
<code>atca_gen_dig_in_out</code>	377
<code>atca_gen_key_in_out</code>	378
<code>atca_hal_kit_phy_t</code>	379
<code>atca_hal_list_entry_t</code>	380
<code>atca_hal_shm_t</code>	380
<code>atca_hmac_in_out</code>	380
<code>atca_i2c_host_s</code>	382
<code>atca_iface</code>	382
<code>atca_include_data_in_out</code>	383
<code>atca_io_decrypt_in_out</code>	383
<code>atca_mac_in_out</code>	383
<code>atca_mbedtls_eckey_s</code>	384
<code>atca_nonce_in_out</code>	384
<code>atca_plib_i2c_api</code>	385
<code>atca_resp_mac_in_out</code>	385
<code>atca_secureboot_enc_in_out</code>	386
<code>atca_secureboot_mac_in_out</code>	386
<code>atca_session_key_in_out</code>	386
<code>atca_sha256_ctx</code>	387
<code>atca_sign_internal_in_out</code>	388
<code>atca_spi_host_s</code>	389
<code>atca_temp_key</code>	389
<code>atca_uart_host_s</code>	390
<code>atca_verify_in_out</code>	390



atca_verify_mac . . . . .	390
atca_write_mac_in_out . . . . .	391
atcac_aes_cmac_ctx . . . . .	396
atcac_aes_gcm_ctx . . . . .	396
atcac_hmac_ctx . . . . .	396
atcac_pk_ctx . . . . .	396
atcac_sha1_ctx . . . . .	396
atcac_sha2_256_ctx . . . . .	396
atcac_x509_ctx . . . . .	397
atcacert_build_state_s . . . . .	397
atcacert_cert_element_s . . . . .	397
atcacert_cert_loc_s . . . . .	399
atcacert_def_s . . . . .	404
atcacert_device_loc_s . . . . .	405
atcacert_tm_utc_s . . . . .	408
ATCAHAL_t . . . . .	412
atcal2Cmaster . . . . .	412
ATCAIfaceCfg . . . . .	413
ATCAPacket . . . . .	417
cryptoauthlib.library.AtcaReference . . . . .	418
atcaSWImaster . . . . .	419
atecc508a_config_s . . . . .	421
atecc608_config_s . . . . .	423
atsha204a_config_s . . . . .	425
cal_buffer_s . . . . .	428
CK_AES_CBC_ENCRYPT_DATA_PARAMS . . . . .	432
CK_AES_CCM_PARAMS . . . . .	432
CK_AES_CTR_PARAMS . . . . .	432
CK_AES_GCM_PARAMS . . . . .	433
CK_ARIA_CBC_ENCRYPT_DATA_PARAMS . . . . .	433
CK_ATTRIBUTE . . . . .	433
CK_C_INITIALIZE_ARGS . . . . .	433
CK_CAMELLIA_CBC_ENCRYPT_DATA_PARAMS . . . . .	433
CK_CAMELLIA_CTR_PARAMS . . . . .	434
CK_CCM_PARAMS . . . . .	434
CK_CMS_SIG_PARAMS . . . . .	434
CK_DATE . . . . .	434
CK_DES_CBC_ENCRYPT_DATA_PARAMS . . . . .	434
CK_DSA_PARAMETER_GEN_PARAM . . . . .	435
CK_ECDH1_DERIVE_PARAMS . . . . .	435
CK_ECDH2_DERIVE_PARAMS . . . . .	435
CK_ECDH_AES_KEY_WRAP_PARAMS . . . . .	435
CK_ECMQV_DERIVE_PARAMS . . . . .	436
CK_FUNCTION_LIST . . . . .	436
CK_GCM_PARAMS . . . . .	436
CK_GOSTR3410_DERIVE_PARAMS . . . . .	436
CK_GOSTR3410_KEY_WRAP_PARAMS . . . . .	437
CK_INFO . . . . .	437
CK_KEA_DERIVE_PARAMS . . . . .	437
CK_KEY_DERIVATION_STRING_DATA . . . . .	437
CK_KEY_WRAP_SET_OAEP_PARAMS . . . . .	437
CK_KIP_PARAMS . . . . .	438
CK_MECHANISM . . . . .	438
CK_MECHANISM_INFO . . . . .	438
CK_OTP_PARAM . . . . .	438
CK_OTP_PARAMS . . . . .	438
CK_OTP_SIGNATURE_INFO . . . . .	439
CK_PBE_PARAMS . . . . .	439

CK_PKCS5_PBKD2_PARAMS . . . . .	439
CK_PKCS5_PBKD2_PARAMS2 . . . . .	439
CK_RC2_CBC_PARAMS . . . . .	440
CK_RC2_MAC_GENERAL_PARAMS . . . . .	440
CK_RC5_CBC_PARAMS . . . . .	440
CK_RC5_MAC_GENERAL_PARAMS . . . . .	440
CK_RC5_PARAMS . . . . .	440
CK_RSA_AES_KEY_WRAP_PARAMS . . . . .	440
CK_RSA_PKCS_OAEP_PARAMS . . . . .	441
CK_RSA_PKCS_PSS_PARAMS . . . . .	441
CK_SEED_CBC_ENCRYPT_DATA_PARAMS . . . . .	441
CK_SESSION_INFO . . . . .	441
CK_SKIPJACK_PRIVATE_WRAP_PARAMS . . . . .	441
CK_SKIPJACK_RELAYX_PARAMS . . . . .	442
CK_SLOT_INFO . . . . .	442
CK_SSL3_KEY_MAT_OUT . . . . .	442
CK_SSL3_KEY_MAT_PARAMS . . . . .	442
CK_SSL3_MASTER_KEY_DERIVE_PARAMS . . . . .	443
CK_SSL3_RANDOM_DATA . . . . .	443
CK_TLS12_KEY_MAT_PARAMS . . . . .	443
CK_TLS12_MASTER_KEY_DERIVE_PARAMS . . . . .	443
CK_TLS_KDF_PARAMS . . . . .	443
CK_TLS_MAC_PARAMS . . . . .	444
CK_TLS_PRF_PARAMS . . . . .	444
CK_TOKEN_INFO . . . . .	444
CK_VERSION . . . . .	444
CK_WTLS_KEY_MAT_OUT . . . . .	445
CK_WTLS_KEY_MAT_PARAMS . . . . .	445
CK_WTLS_MASTER_KEY_DERIVE_PARAMS . . . . .	445
CK_WTLS_PRF_PARAMS . . . . .	445
CK_WTLS_RANDOM_DATA . . . . .	445
CK_X9_42_DH1_DERIVE_PARAMS . . . . .	446
CK_X9_42_DH2_DERIVE_PARAMS . . . . .	446
CK_X9_42_MQV_DERIVE_PARAMS . . . . .	446
CL_HashContext . . . . .	446
device_execution_time_t . . . . .	451
devtype_names_t . . . . .	451
Exception	
cryptoauthlib.exceptions.CryptoError . . . . .	450
cryptoauthlib.exceptions.AssertionFailure . . . . .	368
cryptoauthlib.exceptions.BadArgumentError . . . . .	427
cryptoauthlib.exceptions.BadCrcError . . . . .	427
cryptoauthlib.exceptions.BadOpcodeError . . . . .	427
cryptoauthlib.exceptions.CheckmacVerifyFailedError . . . . .	430
cryptoauthlib.exceptions.CommunicationError . . . . .	447
cryptoauthlib.exceptions.ConfigZoneLockedError . . . . .	447
cryptoauthlib.exceptions.CrcError . . . . .	449
cryptoauthlib.exceptions.DataZoneLockedError . . . . .	450
cryptoauthlib.exceptions.EccFaultError . . . . .	451
cryptoauthlib.exceptions.ExecutionError . . . . .	452
cryptoauthlib.exceptions.FunctionError . . . . .	452
cryptoauthlib.exceptions.GenericError . . . . .	452
cryptoauthlib.exceptions.HealthTestError . . . . .	453
cryptoauthlib.exceptions.InvalidIdentifierError . . . . .	456
cryptoauthlib.exceptions.InvalidSizeError . . . . .	457
cryptoauthlib.exceptions.LibraryLoadError . . . . .	458
cryptoauthlib.exceptions.LibraryMemoryError . . . . .	458
cryptoauthlib.exceptions.LibraryNotInitialized . . . . .	459

cryptoauthlib.exceptions.NoDevicesFoundError . . . . .	459
cryptoauthlib.exceptions.NoResponseError . . . . .	460
cryptoauthlib.exceptions.NoUseFlagError . . . . .	460
cryptoauthlib.exceptions.ParityError . . . . .	460
cryptoauthlib.exceptions.ParseError . . . . .	461
cryptoauthlib.exceptions.ReceiveError . . . . .	468
cryptoauthlib.exceptions.ReceiveTimeoutError . . . . .	469
cryptoauthlib.exceptions.ResyncWithWakeupError . . . . .	469
cryptoauthlib.exceptions.StatusUnknownError . . . . .	473
cryptoauthlib.exceptions.TimeOutError . . . . .	473
cryptoauthlib.exceptions.TransmissionError . . . . .	474
cryptoauthlib.exceptions.TransmissionTimeoutError . . . . .	474
cryptoauthlib.exceptions.UnimplementedError . . . . .	475
cryptoauthlib.exceptions.UnsupportedInterface . . . . .	475
cryptoauthlib.exceptions.WakeFailedError . . . . .	477
cryptoauthlib.exceptions.ZoneNotLockedError . . . . .	478
i2c_sam0_instance . . . . .	455
i2c_sam_instance . . . . .	455
i2c_start_instance . . . . .	455
Jwt	
cryptoauthlib.atjwt.PyJWT . . . . .	468
memory_parameters . . . . .	459
object	
cryptoauthlib_mock.atcab_mock . . . . .	391
pkcs11_mech_table_e . . . . .	461
pkcs11_attr_model_s . . . . .	461
pkcs11_conf_filedata_s . . . . .	461
pkcs11_dev_ctx . . . . .	462
pkcs11_dev_res . . . . .	462
pkcs11_dev_state . . . . .	462
pkcs11_ecc_key_info_s . . . . .	463
pkcs11_lib_ctx_s . . . . .	463
pkcs11_object_cache_s . . . . .	465
pkcs11_object_s . . . . .	465
pkcs11_session_ctx_s . . . . .	466
pkcs11_session_mech_ctx_s . . . . .	467
pkcs11_slot_ctx_s . . . . .	467
secure_boot_config_bits . . . . .	469
secure_boot_parameters . . . . .	470
sw_sha256_ctx . . . . .	473
tng_cert_map_element . . . . .	474
Union	
cryptoauthlib.library.AtcaUnion . . . . .	420
cryptoauthlib.iface._ATCAIfaceParams . . . . .	361
cryptoauthlib.iface._U_Address . . . . .	367
build_ext	
setup.CryptoAuthCommandBuildExt . . . . .	449
Distribution	
setup.BinaryDistribution . . . . .	428
ECAAlgorithm	
cryptoauthlib.atjwt.HwEcAlgorithm . . . . .	453
Enum	
cryptoauthlib.atcaenum.AtcaEnum . . . . .	411
cryptoauthlib.atcacert.CertStatus . . . . .	429
cryptoauthlib.atcacert.atcacert_cert_sn_src_t . . . . .	400
cryptoauthlib.atcacert.atcacert_cert_type_t . . . . .	401
cryptoauthlib.atcacert.atcacert_date_format_t . . . . .	403
cryptoauthlib.atcacert.atcacert_device_zone_t . . . . .	406

cryptoauthlib.atcacert.atcacert_std_cert_element_t . . . . .	407
cryptoauthlib.atcacert.atcacert_transform_t . . . . .	409
cryptoauthlib.iface.ATCADeviceType . . . . .	410
cryptoauthlib.iface.ATCAIfaceType . . . . .	416
cryptoauthlib.iface.ATCAKitType . . . . .	417
cryptoauthlib.status.Status . . . . .	471
HMACAAlgorithm	
cryptoauthlib.atjwt.HwHmacAlgorithm . . . . .	454
install	
setup.CryptoAuthCommandInstall . . . . .	449
Structure	
cryptoauthlib.atcab.atca_aes_cbc_ctx . . . . .	369
cryptoauthlib.atcab.atca_aes_cbcmac_ctx . . . . .	369
cryptoauthlib.atcab.atca_aes_ccm_ctx . . . . .	370
cryptoauthlib.atcab.atca_aes_cmac_ctx . . . . .	371
cryptoauthlib.atcab.atca_aes_ctr_ctx . . . . .	372
cryptoauthlib.atcab.atca_aes_gcm_ctx . . . . .	372
cryptoauthlib.atcab.atca_sha256_ctx . . . . .	387
cryptoauthlib.atcab.atca_hmac_sha256_ctx . . . . .	381
cryptoauthlib.atcacert.atcacert_tm_utc_t . . . . .	408
cryptoauthlib.device.AesEnable . . . . .	368
cryptoauthlib.device.ChipMode508 . . . . .	430
cryptoauthlib.device.ChipMode608 . . . . .	431
cryptoauthlib.device.ChipOptions . . . . .	431
cryptoauthlib.device.CountMatch . . . . .	448
cryptoauthlib.device.Counter204 . . . . .	447
cryptoauthlib.device.I2cEnable . . . . .	456
cryptoauthlib.device.KeyConfig . . . . .	457
cryptoauthlib.device.SecureBoot . . . . .	470
cryptoauthlib.device.SlotConfig . . . . .	471
cryptoauthlib.device.UseLock . . . . .	475
cryptoauthlib.device.VolatileKeyPermission . . . . .	476
cryptoauthlib.device.X509Format . . . . .	477
cryptoauthlib.library.AtcaStructure . . . . .	418
cryptoauthlib.atcacert.atcacert_cert_element_t . . . . .	398
cryptoauthlib.atcacert.atcacert_cert_loc_t . . . . .	399
cryptoauthlib.atcacert.atcacert_comp_data_t . . . . .	402
cryptoauthlib.atcacert.atcacert_def_t . . . . .	404
cryptoauthlib.atcacert.atcacert_device_loc_t . . . . .	405
cryptoauthlib.device.Atecc508aConfig . . . . .	422
cryptoauthlib.device.Atecc608Config . . . . .	424
cryptoauthlib.device.Atsha204aConfig . . . . .	426
cryptoauthlib.iface.ATCAIfaceCfg . . . . .	414
cryptoauthlib.iface._ATCACUSTOM . . . . .	357
cryptoauthlib.iface._ATCAHID . . . . .	358
cryptoauthlib.iface._ATCAI2C . . . . .	359
cryptoauthlib.iface._ATCAKIT . . . . .	362
cryptoauthlib.iface._ATCASPI . . . . .	363
cryptoauthlib.iface._ATCASWI . . . . .	364
cryptoauthlib.iface._ATCAUART . . . . .	365



## Chapter 17

# Data Structure Index

### 17.1 Data Structures

Here are the data structures with brief descriptions:

<a href="#">_ascii_kit_host_context</a>	357
<a href="#">cryptoauthlib.iface._ATCACUSTOM</a>	357
<a href="#">cryptoauthlib.iface._ATCAHID</a>	358
<a href="#">cryptoauthlib.iface._ATCAI2C</a>	359
<a href="#">cryptoauthlib.iface._ATCAIfaceParams</a>	361
<a href="#">cryptoauthlib.iface._ATCAKIT</a>	362
<a href="#">cryptoauthlib.iface._ATCASPI</a>	363
<a href="#">cryptoauthlib.iface._ATCASWI</a>	364
<a href="#">cryptoauthlib.iface._ATCAUART</a>	365
<a href="#">cryptoauthlib.library._Ctynpeltetator</a>	366
<a href="#">_kit_host_map_entry</a>	366
<a href="#">cryptoauthlib.iface._U_Address</a>	367
<a href="#">cryptoauthlib.device.AesEnable</a>	368
<a href="#">cryptoauthlib.exceptions.AssertionFailure</a>	368
<a href="#">cryptoauthlib.atcab.atca_aes_cbc_ctx</a>	369
<a href="#">cryptoauthlib.atcab.atca_aes_cbcmac_ctx</a>	369
<a href="#">cryptoauthlib.atcab.atca_aes_ccm_ctx</a>	370
<a href="#">cryptoauthlib.atcab.atca_aes_cmac_ctx</a>	371
<a href="#">cryptoauthlib.atcab.atca_aes_ctr_ctx</a>	372
<a href="#">cryptoauthlib.atcab.atca_aes_gcm_ctx</a>	372
<a href="#">atca_check_mac_in_out</a>	
Input/output parameters for function atcah_check_mac()	373
<a href="#">atca_decrypt_in_out</a>	
Input/output parameters for function atca_decrypt()	374
<a href="#">atca_delete_in_out</a>	
Input/Output paramters for calculating the mac.Used with Delete command	374
<a href="#">atca_derive_key_in_out</a>	
Input/output parameters for function atcah_derive_key()	375
<a href="#">atca_derive_key_mac_in_out</a>	
Input/output parameters for function atcah_derive_key_mac()	375
<a href="#">atca_device</a>	
Atca_device is the C object backing ATCADevice. See the <a href="#">atca_device.h</a> file for details on the ATCADevice methods	376
<a href="#">atca_diversified_key_in_out</a>	
Input/output parameters for function atcah_gendivkey()	377

<a href="#">atca_evp_ctx</a>	377
<a href="#">atca_gen_dig_in_out</a>	
Input/output parameters for function <code>atcah_gen_dig()</code>	377
<a href="#">atca_gen_key_in_out</a>	
Input/output parameters for calculating the PubKey digest put into TempKey by the GenKey command with the <code>atcah_gen_key_msg()</code> function	378
<a href="#">atca_hal_kit_phy_t</a>	379
<a href="#">atca_hal_list_entry_t</a>	
Structure that holds the hal/phy mapping for different interface types	380
<a href="#">atca_hal_shm_t</a>	380
<a href="#">atca_hmac_in_out</a>	
Input/output parameters for function <code>atca_hmac()</code>	380
<a href="#">cryptoauthlib.atcab.atca_hmac_sha256_ctx</a>	381
<a href="#">atca_i2c_host_s</a>	382
<a href="#">atca_iface</a>	
Atca_iface is the context structure for a configured interface	382
<a href="#">atca_include_data_in_out</a>	
Input / output parameters for function <code>atca_include_data()</code>	383
<a href="#">atca_io_decrypt_in_out</a>	383
<a href="#">atca_mac_in_out</a>	
Input/output parameters for function <code>atca_mac()</code>	383
<a href="#">atca_mbedtls_eckey_s</a>	384
<a href="#">atca_nonce_in_out</a>	
Input/output parameters for function <code>atca_nonce()</code>	384
<a href="#">atca_plib_i2c_api</a>	385
<a href="#">atca_resp_mac_in_out</a>	
Input/Output parameters for calculating the output response mac in SHA105 device. Used with the <code>atcah_gen_output_resp_mac()</code> function	385
<a href="#">atca_secureboot_enc_in_out</a>	386
<a href="#">atca_secureboot_mac_in_out</a>	386
<a href="#">atca_session_key_in_out</a>	
Input/Output paramters for calculating the session key by the nonce command. Used with the <code>atcah_gen_session_key()</code> function	386
<a href="#">atca_sha256_ctx</a>	387
<a href="#">cryptoauthlib.atcab.atca_sha256_ctx</a>	387
<a href="#">atca_sign_internal_in_out</a>	
Input/output parameters for calculating the message and digest used by the Sign(internal) command. Used with the <code>atcah_sign_internal_msg()</code> function	388
<a href="#">atca_spi_host_s</a>	389
<a href="#">atca_temp_key</a>	
Structure to hold TempKey fields	389
<a href="#">atca_uart_host_s</a>	390
<a href="#">atca_verify_in_out</a>	
Input/output parameters for function <code>atcah_verify()</code>	390
<a href="#">atca_verify_mac</a>	390
<a href="#">atca_write_mac_in_out</a>	
Input/output parameters for function <code>atcah_write_auth_mac()</code> and <code>atcah_privwrite_auth_mac()</code>	391
<a href="#">cryptoauthlib_mock.atcab_mock</a>	391
<a href="#">atcac_aes_cmac_ctx</a>	396
<a href="#">atcac_aes_gcm_ctx</a>	396
<a href="#">atcac_hmac_ctx</a>	396
<a href="#">atcac_pk_ctx</a>	396
<a href="#">atcac_sha1_ctx</a>	396
<a href="#">atcac_sha2_256_ctx</a>	396
<a href="#">atcac_x509_ctx</a>	397
<a href="#">atcacert_build_state_s</a>	397
<a href="#">atcacert_cert_element_s</a>	397
<a href="#">cryptoauthlib.atcacert.atcacert_cert_element_t</a>	398

atcacert_cert_loc_s	399
cryptoauthlib.atcacert.atcacert_cert_loc_t	399
cryptoauthlib.atcacert.atcacert_cert_sn_src_t	400
cryptoauthlib.atcacert.atcacert_cert_type_t	401
cryptoauthlib.atcacert.atcacert_comp_data_t	402
cryptoauthlib.atcacert.atcacert_date_format_t	403
atcacert_def_s	404
cryptoauthlib.atcacert.atcacert_def_t	404
atcacert_device_loc_s	405
cryptoauthlib.atcacert.atcacert_device_loc_t	405
cryptoauthlib.atcacert.atcacert_device_zone_t	406
cryptoauthlib.atcacert.atcacert_std_cert_element_t	407
atcacert_tm_utc_s	408
cryptoauthlib.atcacert.atcacert_tm_utc_t	408
cryptoauthlib.atcacert.atcacert_transform_t	409
cryptoauthlib.iface.ATCADeviceType	410
cryptoauthlib.atcaenum.AtcaEnum	411
ATCAHAL_t	
HAL Driver Structure	412
atcal2Cmaster	
This is the hal_data for ATCA HAL for ASF SERCOM	412
ATCAIfaceCfg	413
cryptoauthlib.iface.ATCAIfaceCfg	414
cryptoauthlib.iface.ATCAIfaceType	416
cryptoauthlib.iface.ATCAKitType	417
ATCAPacket	417
cryptoauthlib.library.AtcaReference	418
cryptoauthlib.library.AtcaStructure	418
atcaSWImaster	
This is the hal_data for ATCA HAL for ASF SERCOM	419
cryptoauthlib.library.AtcaUnion	420
atecc508a_config_s	421
cryptoauthlib.device.Atecc508aConfig	422
atecc608_config_s	423
cryptoauthlib.device.Atecc608Config	424
atsha204a_config_s	425
cryptoauthlib.device.Atsha204aConfig	426
cryptoauthlib.exceptions.BadArgumentError	427
cryptoauthlib.exceptions.BadCrcError	427
cryptoauthlib.exceptions.BadOpcodeError	427
setup.BinaryDistribution	428
cal_buffer_s	428
cryptoauthlib.atcacert.CertStatus	429
cryptoauthlib.exceptions.CheckmacVerifyFailedError	430
cryptoauthlib.device.ChipMode508	430
cryptoauthlib.device.ChipMode608	431
cryptoauthlib.device.ChipOptions	431
CK_AES_CBC_ENCRYPT_DATA_PARAMS	432
CK_AES_CCM_PARAMS	432
CK_AES_CTR_PARAMS	432
CK_AES_GCM_PARAMS	433
CK_ARIA_CBC_ENCRYPT_DATA_PARAMS	433
CK_ATTRIBUTE	433
CK_C_INITIALIZE_ARGS	433
CK_CAMELLIA_CBC_ENCRYPT_DATA_PARAMS	433
CK_CAMELLIA_CTR_PARAMS	434
CK_CCM_PARAMS	434
CK_CMS_SIG_PARAMS	434



CK_DATE	434
CK_DES_CBC_ENCRYPT_DATA_PARAMS	434
CK_DSA_PARAMETER_GEN_PARAM	435
CK_ECDH1_DERIVE_PARAMS	435
CK_ECDH2_DERIVE_PARAMS	435
CK_ECDH_AES_KEY_WRAP_PARAMS	435
CK_ECMQV_DERIVE_PARAMS	436
CK_FUNCTION_LIST	436
CK_GCM_PARAMS	436
CK_GOSTR3410_DERIVE_PARAMS	436
CK_GOSTR3410_KEY_WRAP_PARAMS	437
CK_INFO	437
CK_KEA_DERIVE_PARAMS	437
CK_KEY_DERIVATION_STRING_DATA	437
CK_KEY_WRAP_SET_OAEP_PARAMS	437
CK_KIP_PARAMS	438
CK_MECHANISM	438
CK_MECHANISM_INFO	438
CK_OTP_PARAM	438
CK_OTP_PARAMS	438
CK_OTP_SIGNATURE_INFO	439
CK_PBE_PARAMS	439
CK_PKCS5_PBKD2_PARAMS	439
CK_PKCS5_PBKD2_PARAMS2	439
CK_RC2_CBC_PARAMS	440
CK_RC2_MAC_GENERAL_PARAMS	440
CK_RC5_CBC_PARAMS	440
CK_RC5_MAC_GENERAL_PARAMS	440
CK_RC5_PARAMS	440
CK_RSA_AES_KEY_WRAP_PARAMS	440
CK_RSA_PKCS_OAEP_PARAMS	441
CK_RSA_PKCS_PSS_PARAMS	441
CK_SEED_CBC_ENCRYPT_DATA_PARAMS	441
CK_SESSION_INFO	441
CK_SKIPJACK_PRIVATE_WRAP_PARAMS	441
CK_SKIPJACK_RELAYX_PARAMS	442
CK_SLOT_INFO	442
CK_SSL3_KEY_MAT_OUT	442
CK_SSL3_KEY_MAT_PARAMS	442
CK_SSL3_MASTER_KEY_DERIVE_PARAMS	443
CK_SSL3_RANDOM_DATA	443
CK_TLS12_KEY_MAT_PARAMS	443
CK_TLS12_MASTER_KEY_DERIVE_PARAMS	443
CK_TLS_KDF_PARAMS	443
CK_TLS_MAC_PARAMS	444
CK_TLS_PRF_PARAMS	444
CK_TOKEN_INFO	444
CK_VERSION	444
CK_WTLS_KEY_MAT_OUT	445
CK_WTLS_KEY_MAT_PARAMS	445
CK_WTLS_MASTER_KEY_DERIVE_PARAMS	445
CK_WTLS_PRF_PARAMS	445
CK_WTLS_RANDOM_DATA	445
CK_X9_42_DH1_DERIVE_PARAMS	446
CK_X9_42_DH2_DERIVE_PARAMS	446
CK_X9_42_MQV_DERIVE_PARAMS	446
CL_HashContext	446
cryptoauthlib.exceptions.CommunicationError	447

cryptoauthlib.exceptions.ConfigZoneLockedError	447
cryptoauthlib.device.Counter204	447
cryptoauthlib.device.CountMatch	448
cryptoauthlib.exceptions.CrcError	449
setup.CryptoAuthCommandBuildExt	449
setup.CryptoAuthCommandInstall	449
cryptoauthlib.exceptions.CryptoError	450
cryptoauthlib.exceptions.DataZoneLockedError	450
device_execution_time_t	
Structure to hold the device execution time and the opcode for the corresponding command	451
devtype_names_t	451
cryptoauthlib.exceptions.EccFaultError	451
cryptoauthlib.exceptions.ExecutionError	452
cryptoauthlib.exceptions.FunctionError	452
cryptoauthlib.exceptions.GenericError	452
cryptoauthlib.exceptions.HealthTestError	453
cryptoauthlib.atjwt.HwEcAlgorithm	453
cryptoauthlib.atjwt.HwHmacAlgorithm	454
i2c_sam0_instance	455
i2c_sam_instance	455
i2c_start_instance	455
cryptoauthlib.device.I2cEnable	456
cryptoauthlib.exceptions.InvalidIdentifierError	456
cryptoauthlib.exceptions.InvalidSizeError	457
cryptoauthlib.device.KeyConfig	457
cryptoauthlib.exceptions.LibraryLoadError	458
cryptoauthlib.exceptions.LibraryMemoryError	458
cryptoauthlib.exceptions.LibraryNotInitialized	459
memory_parameters	459
cryptoauthlib.exceptions.NoDevicesFoundError	459
cryptoauthlib.exceptions.NoResponseError	460
cryptoauthlib.exceptions.NoUseFlagError	460
cryptoauthlib.exceptions.ParityError	460
cryptoauthlib.exceptions.ParseError	461
pkcs11_mech_table_e	461
pkcs11_attr_model_s	461
pkcs11_conf_filedata_s	461
pkcs11_dev_ctx	462
pkcs11_dev_res	462
pkcs11_dev_state	462
pkcs11_ecc_key_info_s	463
pkcs11_lib_ctx_s	463
pkcs11_object_cache_s	465
pkcs11_object_s	465
pkcs11_session_ctx_s	466
pkcs11_session_mech_ctx_s	467
pkcs11_slot_ctx_s	467
cryptoauthlib.atjwt.PyJWT	468
cryptoauthlib.exceptions.ReceiveError	468
cryptoauthlib.exceptions.ReceiveTimeoutError	469
cryptoauthlib.exceptions.ResyncWithWakeupError	469
secure_boot_config_bits	469
secure_boot_parameters	470
cryptoauthlib.device.SecureBoot	470
cryptoauthlib.device.SlotConfig	471
cryptoauthlib.status.Status	471
cryptoauthlib.exceptions.StatusUnknownError	473
sw_sha256_ctx	473

<a href="#">cryptoauthlib.exceptions.TimeOutError</a>	473
<a href="#">tng_cert_map_element</a>	474
<a href="#">cryptoauthlib.exceptions.TransmissionError</a>	474
<a href="#">cryptoauthlib.exceptions.TransmissionTimeoutError</a>	474
<a href="#">cryptoauthlib.exceptions.UnimplementedError</a>	475
<a href="#">cryptoauthlib.exceptions.UnsupportedInterface</a>	475
<a href="#">cryptoauthlib.device.UseLock</a>	475
<a href="#">cryptoauthlib.device.VolatileKeyPermission</a>	476
<a href="#">cryptoauthlib.exceptions.WakeFailedError</a>	477
<a href="#">cryptoauthlib.device.X509Format</a>	477
<a href="#">cryptoauthlib.exceptions.ZoneNotLockedError</a>	478

## Chapter 18

# File Index

### 18.1 File List

Here is a list of all documented files with brief descriptions:

<a href="#">api_206a.c</a>	Provides APIs to use with ATSHA206A device . . . . .	479
<a href="#">api_206a.h</a>	Provides api interfaces to use with ATSHA206A device . . . . .	485
<a href="#">symmetric_authentication.c</a>	Contains API for performing the symmetric Authentication between the Host and the device . .	492
<a href="#">symmetric_authentication.h</a>	Contains API for performing the symmetric Authentication between the Host and the device . .	493
<a href="#">ascii_kit_host.c</a>	KIT protocol interpreter . . . . .	494
<a href="#">ascii_kit_host.h</a>	KIT protocol interpreter . . . . .	495
<a href="#">trust_pkcs11_config.c</a>	PKCS11 Trust Platform Configuration . . . . .	498
<a href="#">io_protection_key.h</a>	Provides required interface to access IO protection key . . . . .	498
<a href="#">secure_boot.c</a>	Provides required APIs to manage secure boot under various scenarios . . . . .	499
<a href="#">secure_boot.h</a>	Provides required APIs to manage secure boot under various scenarios . . . . .	500
<a href="#">secure_boot_memory.h</a>	Provides interface to memory component for the secure boot . . . . .	502
<a href="#">tflxtls_cert_def_4_device.c</a>	TNG TLS device certificate definition . . . . .	502
<a href="#">tflxtls_cert_def_4_device.h</a>	TNG TLS device certificate definition . . . . .	503
<a href="#">tng_atca.c</a>	TNG Helper Functions . . . . .	503
<a href="#">tng_atca.h</a>	TNG Helper Functions . . . . .	504
<a href="#">tng_atcacert_client.c</a>	Client side certificate I/O functions for TNG devices . . . . .	505
<a href="#">tng_atcacert_client.h</a>	Client side certificate I/O functions for TNG devices . . . . .	509
<a href="#">tng_root_cert.c</a>	TNG root certificate (DER) . . . . .	510

<a href="#">tng_root_cert.h</a>	
TNG root certificate (DER)	510
<a href="#">tnglora_cert_def_1_signer.c</a>	
TNG LORA signer certificate definition	510
<a href="#">tnglora_cert_def_1_signer.h</a>	
TNG LORA signer certificate definition	511
<a href="#">tnglora_cert_def_2_device.c</a>	
TNG LORA device certificate definition	511
<a href="#">tnglora_cert_def_2_device.h</a>	
TNG LORA device certificate definition	512
<a href="#">tnglora_cert_def_4_device.c</a>	
TNG LORA device certificate definition	512
<a href="#">tnglora_cert_def_4_device.h</a>	
TNG LORA device certificate definition	513
<a href="#">tngtls_cert_def_1_signer.c</a>	
TNG TLS signer certificate definition	513
<a href="#">tngtls_cert_def_1_signer.h</a>	
TNG TLS signer certificate definition	514
<a href="#">tngtls_cert_def_2_device.c</a>	
TNG TLS device certificate definition	514
<a href="#">tngtls_cert_def_2_device.h</a>	
TNG TLS device certificate definition	515
<a href="#">tngtls_cert_def_3_device.c</a>	
TNG TLS device certificate definition	515
<a href="#">tngtls_cert_def_3_device.h</a>	
TNG TLS device certificate definition	516
<a href="#">wpc_apis.c</a>	
Provides api interfaces for WPC authentication	516
<a href="#">wpc_apis.h</a>	
Provides api interfaces for WPC authentication	517
<a href="#">wpccert_client.c</a>	
Provides api interfaces for accessing WPC certificates from device	518
<a href="#">wpccert_client.h</a>	
Provides api interfaces for accessing WPC certificates from device	519
<a href="#">atca_basic.c</a>	
CryptoAuthLib Basic API methods. These methods provide a simpler way to access the core crypto methods	520
<a href="#">atca_basic.h</a>	
CryptoAuthLib Basic API methods - a simple crypto authentication API. These methods manage a global ATCADevice object behind the scenes. They also manage the wake/idle state transitions so callers don't need to	528
<a href="#">atca_cfgs.c</a>	
Set of default configurations for various ATCA devices and interfaces	537
<a href="#">atca_cfgs.h</a>	
Set of default configurations for various ATCA devices and interfaces	537
<a href="#">atca_compiler.h</a>	
CryptoAuthLib is meant to be portable across architectures, even non-Microchip architectures and compiler environments. This file is for isolating compiler specific macros	537
<a href="#">atca_config_check.h</a>	
Consistency checks for configuration options	538
<a href="#">atca_debug.c</a>	
Debug/Trace for CryptoAuthLib calls	542
<a href="#">atca_device.c</a>	
Microchip CryptoAuth device object	542
<a href="#">atca_device.h</a>	
Microchip Crypto Auth device object	543
<a href="#">atca_devtypes.h</a>	
Microchip Crypto Auth	544

<a href="#">atca_helpers.c</a>	Helpers to support the CryptoAuthLib Basic API methods . . . . .	545
<a href="#">atca_helpers.h</a>	Helpers to support the CryptoAuthLib Basic API methods . . . . .	553
<a href="#">atca_iface.c</a>	Microchip CryptoAuthLib hardware interface object . . . . .	555
<a href="#">atca_iface.h</a>	Microchip Crypto Auth hardware interface object . . . . .	556
<a href="#">atca_platform.h</a>	Configure the platform interfaces for cryptoauthlib . . . . .	560
<a href="#">atca_status.h</a>	Microchip Crypto Auth status codes . . . . .	560
<a href="#">atca_utils_sizes.c</a>	API to Return structure sizes of cryptoauthlib structures . . . . .	566
<a href="#">atca_version.h</a>	Microchip CryptoAuth Library Version . . . . .	568
<a href="#">atcacert.h</a>	Declarations common to all atcacert code . . . . .	568
<a href="#">atcacert_check_config.h</a>	Configuration check and defaults for the atcacert module . . . . .	569
<a href="#">atcacert_client.c</a>	Client side cert i/o methods. These declarations deal with the client-side, the node being authenticated, of the authentication process. It is assumed the client has an ECC CryptoAuthentication device (e.g. ATECC508A) and the certificates are stored on that device . . . . .	569
<a href="#">atcacert_client.h</a>	Client side cert i/o methods. These declarations deal with the client-side, the node being authenticated, of the authentication process. It is assumed the client has an ECC CryptoAuthentication device (e.g. ATECC508A) and the certificates are stored on that device . . . . .	570
<a href="#">atcacert_date.c</a>	Date handling with regard to certificates . . . . .	571
<a href="#">atcacert_date.h</a>	Declarations for date handling with regard to certificates . . . . .	572
<a href="#">atcacert_def.c</a>	Main certificate definition implementation . . . . .	574
<a href="#">atcacert_def.h</a>	Declarations for certificates related to ECC CryptoAuthentication devices. These are the definitions required to define a certificate and its various elements with regards to the CryptoAuthentication ECC devices . . . . .	575
<a href="#">atcacert_der.c</a>	Functions required to work with DER encoded data related to X.509 certificates . . . . .	577
<a href="#">atcacert_der.h</a>	Function declarations required to work with DER encoded data related to X.509 certificates . . . . .	578
<a href="#">atcacert_host_hw.c</a>	Host side methods using CryptoAuth hardware . . . . .	579
<a href="#">atcacert_host_hw.h</a>	Host side methods using CryptoAuth hardware . . . . .	579
<a href="#">atcacert_host_sw.c</a>	Host side methods using software implementations . . . . .	580
<a href="#">atcacert_host_sw.h</a>	Host side methods using software implementations. host-side, the one authenticating a client, of the authentication process. Crypto functions are performed using a software library . . . . .	580
<a href="#">atcacert_pem.c</a>	Functions required to work with PEM encoded data related to X.509 certificates . . . . .	581
<a href="#">atcacert_pem.h</a>	Functions for converting between DER and PEM formats . . . . .	581
<a href="#">cal_buffer.c</a>	Cryptoauthlib buffer management system . . . . .	585

<a href="#">cal_buffer.h</a>	CryptoAuthLib buffer management system . . . . .	587
<a href="#">cal_internal.h</a>	Internal CryptoAuthLib Interfaces . . . . .	590
<a href="#">calib_aes.c</a>	CryptoAuthLib Basic API methods for AES command . . . . .	590
<a href="#">calib_aes_gcm.c</a>	CryptoAuthLib Basic API methods for AES GCM mode . . . . .	591
<a href="#">calib_aes_gcm.h</a>	Unity tests for the cryptoauthlib AES GCM functions . . . . .	591
<a href="#">calib_basic.c</a>	CryptoAuthLib Basic API methods. These methods provide a simpler way to access the core crypto methods . . . . .	591
<a href="#">calib_checkmac.c</a>	CryptoAuthLib Basic API methods for CheckMAC command . . . . .	592
<a href="#">calib_command.c</a>	Microchip CryptoAuthentication device command builder - this is the main object that builds the command byte strings for the given device. It does not execute the command. The basic flow is to call a command method to build the command you want given the parameters and then send that byte string through the device interface . . . . .	593
<a href="#">calib_command.h</a>	Microchip Crypto Auth device command object - this is a command builder only, it does not send the command. The result of a command method is a fully formed packet, ready to send to the ATCAIFace object to dispatch . . . . .	596
<a href="#">calib_config_check.h</a>	Consistency checks for configuration options . . . . .	617
<a href="#">calib_counter.c</a>	CryptoAuthLib Basic API methods for Counter command . . . . .	622
<a href="#">calib_delete.c</a>	CryptoAuthLib Basic API methods for Delete command . . . . .	622
<a href="#">calib_derivekey.c</a>	CryptoAuthLib Basic API methods for DeriveKey command . . . . .	623
<a href="#">calib_device.h</a>	Microchip Crypto Auth Device Data . . . . .	623
<a href="#">calib_ecdh.c</a>	CryptoAuthLib Basic API methods for ECDH command . . . . .	626
<a href="#">calib_execution.c</a>	Implements an execution handler that executes a given command on a device and returns the results . . . . .	627
<a href="#">calib_execution.h</a>	Defines an execution handler that executes a given command on a device and returns the results . . . . .	628
<a href="#">calib_gendig.c</a>	CryptoAuthLib Basic API methods for GenDig command . . . . .	630
<a href="#">calib_genkey.c</a>	CryptoAuthLib Basic API methods for GenKey command . . . . .	631
<a href="#">calib_helpers.c</a>	CryptoAuthLib Basic API - Helper Functions to . . . . .	631
<a href="#">calib_hmac.c</a>	CryptoAuthLib Basic API methods for HMAC command . . . . .	632
<a href="#">calib_info.c</a>	CryptoAuthLib Basic API methods for Info command . . . . .	632
<a href="#">calib_kdf.c</a>	CryptoAuthLib Basic API methods for KDF command . . . . .	633
<a href="#">calib_lock.c</a>	CryptoAuthLib Basic API methods for Lock command . . . . .	633
<a href="#">calib_mac.c</a>	CryptoAuthLib Basic API methods for MAC command . . . . .	634

<a href="#">calib_nonce.c</a>	CryptoAuthLib Basic API methods for Nonce command . . . . .	634
<a href="#">calib_privwrite.c</a>	CryptoAuthLib Basic API methods for PrivWrite command . . . . .	635
<a href="#">calib_random.c</a>	CryptoAuthLib Basic API methods for Random command . . . . .	635
<a href="#">calib_read.c</a>	CryptoAuthLib Basic API methods for Read command . . . . .	636
<a href="#">calib_secureboot.c</a>	CryptoAuthLib Basic API methods for SecureBoot command . . . . .	636
<a href="#">calib_selftest.c</a>	CryptoAuthLib Basic API methods for SelfTest command . . . . .	637
<a href="#">calib_sha.c</a>	CryptoAuthLib Basic API methods for SHA command . . . . .	637
<a href="#">calib_sign.c</a>	CryptoAuthLib Basic API methods for Sign command . . . . .	638
<a href="#">calib_updateextra.c</a>	CryptoAuthLib Basic API methods for UpdateExtra command . . . . .	638
<a href="#">calib_verify.c</a>	CryptoAuthLib Basic API methods for Verify command . . . . .	639
<a href="#">calib_write.c</a>	CryptoAuthLib Basic API methods for Write command . . . . .	639
<a href="#">atca_crypto_hw_aes.h</a>	AES CTR, CBC & CMAC structure definitions . . . . .	640
<a href="#">atca_crypto_hw_aes_cbc.c</a>	CryptoAuthLib Basic API methods for AES CBC mode . . . . .	640
<a href="#">atca_crypto_hw_aes_cbcmac.c</a>	CryptoAuthLib Basic API methods for AES CBC_MAC mode . . . . .	641
<a href="#">atca_crypto_hw_aes_ccm.c</a>	CryptoAuthLib Basic API methods for AES CCM mode . . . . .	641
<a href="#">atca_crypto_hw_aes_cmac.c</a>	CryptoAuthLib Basic API methods for AES CBC_MAC mode . . . . .	642
<a href="#">atca_crypto_hw_aes_ctr.c</a>	CryptoAuthLib Basic API methods for AES CTR mode . . . . .	642
<a href="#">atca_crypto_pad.c</a>	Implementation of PKCS7 Padding for block encryption . . . . .	643
<a href="#">atca_crypto_pbkdf2.c</a>	Implementation of the PBKDF2 algorithm for use in generating password hashes . . . . .	643
<a href="#">atca_crypto_sw.h</a>	Common defines for CryptoAuthLib software crypto wrappers . . . . .	644
<a href="#">atca_crypto_sw_aes_gcm.c</a>	Common Wrapper for host side AES-GCM implementations that feature update APIs rather than an all at once implementation . . . . .	644
<a href="#">atca_crypto_sw_sha1.c</a>	Wrapper API for SHA 1 routines . . . . .	644
<a href="#">atca_crypto_sw_sha1.h</a>	Wrapper API for SHA 1 routines . . . . .	645
<a href="#">atca_crypto_sw_sha2.c</a>	Wrapper API for software SHA 256 routines . . . . .	645
<a href="#">atca_crypto_sw_sha2.h</a>	Wrapper API for software SHA 256 routines . . . . .	646
<a href="#">crypto_hw_config_check.h</a>	Consistency checks for configuration options . . . . .	646
<a href="#">crypto_sw_config_check.h</a>	Consistency checks for configuration options . . . . .	648
<a href="#">sha1_routines.c</a>	Software implementation of the SHA1 algorithm . . . . .	651



<a href="#">sha1_routines.h</a>	Software implementation of the SHA1 algorithm . . . . .	652
<a href="#">sha2_routines.c</a>	Software implementation of the SHA256 algorithm . . . . .	652
<a href="#">sha2_routines.h</a>	Software implementation of the SHA256 algorithm . . . . .	653
<a href="#">cryptoauthlib.h</a>	Single aggregation point for all CryptoAuthLib header files . . . . .	654
<a href="#">atca_hal.c</a>	Low-level HAL - methods used to setup indirection to physical layer interface. this level does the dirty work of abstracting the higher level ATCAIFace methods from the low-level physical interfaces. Its main goal is to keep low-level details from bleeding into the logical interface implementation . . . . .	656
<a href="#">atca_hal.h</a>	Low-level HAL - methods used to setup indirection to physical layer interface . . . . .	657
<a href="#">hal_all_platforms_kit_hidapi.c</a>	HAL for kit protocol over HID for any platform . . . . .	658
<a href="#">hal_freertos.c</a>	FreeRTOS Hardware/OS Abstraction Layer . . . . .	659
<a href="#">hal_gpio_harmony.c</a>	ATCA Hardware abstraction layer for GPIO . . . . .	660
<a href="#">hal_i2c_harmony.c</a>	ATCA Hardware abstraction layer for SAMD21 I2C over Harmony PLIB . . . . .	662
<a href="#">hal_i2c_start.c</a>	ATCA Hardware abstraction layer for SAMD21 I2C over START drivers . . . . .	663
<a href="#">hal_i2c_start.h</a>	ATCA Hardware abstraction layer for SAMD21 I2C over START drivers . . . . .	664
<a href="#">hal_kit_bridge.c</a>	Kit Bridging HAL for cryptoauthlib. This is not intended to be a zero copy driver. It should work with any interface that confirms to a few basic requirements: a) will accept an arbitrary number of bytes and packetize it if necessary for transmission, b) will block for the duration of the transmit . . . . .	665
<a href="#">hal_kit_bridge.h</a>	Kit Bridging HAL for cryptoauthlib. This is not intended to be a zero copy driver. It should work with any interface that confirms to a few basic requirements: a) will accept an arbitrary number of bytes and packetize it if necessary for transmission, b) will block for the duration of the transmit . . . . .	666
<a href="#">hal_linux.c</a>	Timer Utility Functions for Linux . . . . .	667
<a href="#">hal_linux_i2c_userspace.c</a>	ATCA Hardware abstraction layer for Linux using I2C . . . . .	667
<a href="#">hal_linux_uart_userspace.c</a>	ATCA Hardware abstraction layer for Linux using UART . . . . .	668
<a href="#">hal_sam0_i2c_asf.c</a>	ATCA Hardware abstraction layer for SAMD21 I2C over ASF drivers . . . . .	672
<a href="#">hal_sam0_i2c_asf.h</a>	ATCA Hardware abstraction layer for SAMD21 I2C over ASF drivers . . . . .	673
<a href="#">hal_sam_i2c_asf.c</a>	ATCA Hardware abstraction layer for SAM flexcom & twi I2C over ASF drivers . . . . .	673
<a href="#">hal_sam_i2c_asf.h</a>	ATCA Hardware abstraction layer for SAMG55 I2C over ASF drivers . . . . .	674
<a href="#">hal_sam_timer_asf.c</a>	ATCA Hardware abstraction layer for SAMD21 timer/delay over ASF drivers . . . . .	675
<a href="#">hal_spi_harmony.c</a>	ATCA Hardware abstraction layer for SPI over Harmony PLIB . . . . .	676
<a href="#">hal_swi_gpio.c</a>	ATCA Hardware abstraction layer for 1WIRE or SWI over GPIO . . . . .	677
<a href="#">hal_swi_gpio.h</a>	ATCA Hardware abstraction layer for SWI over GPIO drivers . . . . .	680

<a href="#">hal_swi_uart.c</a>	ATCA Hardware abstraction layer for SWI over UART drivers . . . . .	682
<a href="#">hal_timer_start.c</a>	ATCA Hardware abstraction layer for SAMD21 I2C over START drivers . . . . .	683
<a href="#">hal_uart_harmony.c</a>	ATCA Hardware abstraction layer for SWI uart over Harmony PLIB . . . . .	684
<a href="#">hal_uc3_i2c_asf.c</a>	ATCA Hardware abstraction layer for SAMV71 I2C over ASF drivers . . . . .	688
<a href="#">hal_uc3_i2c_asf.h</a>	ATCA Hardware abstraction layer for SAMV71 I2C over ASF drivers . . . . .	689
<a href="#">hal_uc3_timer_asf.c</a>	ATCA Hardware abstraction layer for SAM4S I2C over ASF drivers . . . . .	690
<a href="#">hal_windows.c</a>	ATCA Hardware abstraction layer for windows timer functions . . . . .	690
<a href="#">hal_windows_kit_uart.c</a>	ATCA Hardware abstraction layer for Windows using UART . . . . .	691
<a href="#">kit_protocol.c</a>	Microchip Crypto Auth hardware interface object . . . . .	695
<a href="#">kit_protocol.h</a>	. . . . .	696
<a href="#">swi_uart_samd21_asf.c</a>	ATXMEGA's ATCA Hardware abstraction layer for SWI interface over UART drivers . . . . .	697
<a href="#">swi_uart_samd21_asf.h</a>	ATXMEGA's ATCA Hardware abstraction layer for SWI interface over UART drivers . . . . .	698
<a href="#">swi_uart_start.c</a>	. . . . .	699
<a href="#">swi_uart_start.h</a>	. . . . .	700
<a href="#">atca_host.c</a>	Host side methods to support CryptoAuth computations . . . . .	701
<a href="#">atca_host.h</a>	Definitions and Prototypes for ATCA Utility Functions . . . . .	701
<a href="#">atca_host_config_check.h</a>	Consistency checks for configuration options . . . . .	704
<a href="#">atca_jwt.c</a>	Utilities to create and verify a JSON Web Token (JWT) . . . . .	710
<a href="#">atca_jwt.h</a>	Utilities to create and verify a JSON Web Token (JWT) . . . . .	711
<a href="#">atca_mbedtlsls_interface.h</a>	Configuration Check for MbedTLS Integration Support . . . . .	711
<a href="#">atca_mbedtlsls_wrap.c</a>	Wrapper functions to replace cryptoauthlib software crypto functions with the mbedtls equivalent . . . . .	713
<a href="#">atca_openssl_interface.c</a>	Crypto abstraction functions for external host side cryptography . . . . .	727
<a href="#">atca_openssl_interface.h</a>	OpenSSL Integration Support . . . . .	740
<a href="#">pkcs11_attr.c</a>	PKCS11 Library Object Attributes Handling . . . . .	742
<a href="#">pkcs11_attr.h</a>	PKCS11 Library Object Attribute Handling . . . . .	743
<a href="#">pkcs11_cert.c</a>	PKCS11 Library Certificate Handling . . . . .	744
<a href="#">pkcs11_cert.h</a>	PKCS11 Library Certificate Handling . . . . .	745
<a href="#">pkcs11_config.c</a>	PKCS11 Library Configuration . . . . .	746
<a href="#">pkcs11_debug.c</a>	PKCS11 Library Debugging . . . . .	747
<a href="#">pkcs11_debug.h</a>	PKCS11 Library Debugging . . . . .	747

<a href="#">pkcs11_digest.h</a>	
PKCS11 Library Digest (SHA256) Handling	748
<a href="#">pkcs11_encrypt.c</a>	
PKCS11 Library Encrypt Support	748
<a href="#">pkcs11_encrypt.h</a>	
PKCS11 Library AES Support	749
<a href="#">pkcs11_find.c</a>	
PKCS11 Library Object Find/Searching	750
<a href="#">pkcs11_find.h</a>	
PKCS11 Library Object Find/Searching	750
<a href="#">pkcs11_info.c</a>	
PKCS11 Library Information Functions	751
<a href="#">pkcs11_info.h</a>	
PKCS11 Library Information Functions	752
<a href="#">pkcs11_init.c</a>	
PKCS11 Library Init/Deinit	752
<a href="#">pkcs11_init.h</a>	
PKCS11 Library Initialization & Context	753
<a href="#">pkcs11_key.c</a>	
PKCS11 Library Key Object Handling	754
<a href="#">pkcs11_key.h</a>	
PKCS11 Library Object Handling	756
<a href="#">pkcs11_main.c</a>	
PKCS11 Basic library redirects based on the 2.40 specification docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/os/pkcs11-base-v2.40-os.html	757
<a href="#">pkcs11_mech.c</a>	
PKCS11 Library Mechanism Handling	762
<a href="#">pkcs11_mech.h</a>	
PKCS11 Library Mechanism Handling	762
<a href="#">pkcs11_object.c</a>	
PKCS11 Library Object Handling Base	763
<a href="#">pkcs11_object.h</a>	
PKCS11 Library Object Handling	764
<a href="#">pkcs11_os.c</a>	
PKCS11 Library Operating System Abstraction Functions	766
<a href="#">pkcs11_os.h</a>	
PKCS11 Library Operating System Abstraction	766
<a href="#">pkcs11_session.c</a>	
PKCS11 Library Session Handling	767
<a href="#">pkcs11_session.h</a>	
PKCS11 Library Session Management & Context	768
<a href="#">pkcs11_signature.c</a>	
PKCS11 Library Sign/Verify Handling	769
<a href="#">pkcs11_signature.h</a>	
PKCS11 Library Sign/Verify Handling	770
<a href="#">pkcs11_slot.c</a>	
PKCS11 Library Slot Handling	771
<a href="#">pkcs11_slot.h</a>	
PKCS11 Library Slot Handling & Context	772
<a href="#">pkcs11_token.c</a>	
PKCS11 Library Token Handling	773
<a href="#">pkcs11_token.h</a>	
PKCS11 Library Token Management & Context	774
<a href="#">pkcs11_util.c</a>	
PKCS11 Library Utility Functions	775
<a href="#">pkcs11_util.h</a>	
PKCS11 Library Utilities	776

## 18.1 File List

---

<a href="#">atca_wolfssl_interface.c</a>	
Crypto abstraction functions for external host side cryptography . . . . .	776
<a href="#">atca_wolfssl_interface.h</a>	
Configuration Check for WolfSSL Integration Support . . . . .	776
<a href="#">atca_wolfssl_internal.h</a>	
WolfSSL Integration Support . . . . .	777



# Chapter 19

## Module Documentation

### 19.1 TNG API (tng\_)

These methods provide some convenience functions (mostly around certificates) for TNG devices, which currently include ATECC608A-MAHTN-T.

#### 19.1.0.1 TNG Functions

This folder has a number of convenience functions for working with TNG devices (currently ATECC608A-MAHTN-T).

These devices have standard certificates that can be easily read using the functions in [tng\\_atcacert\\_client.h](#)

#### Functions

- const [atcacert\\_def\\_t](#) \* [tng\\_map\\_get\\_device\\_cert\\_def](#) (int index)  
*Helper function to iterate through all trust cert definitions.*
- ATCA\_STATUS [tng\\_get\\_device\\_cert\\_def](#) (const [atcacert\\_def\\_t](#) \*\*cert\_def)  
*Get the TNG device certificate definition.*
- ATCA\_STATUS [tng\\_get\\_device\\_cert\\_def\\_ext](#) (ATCADevice device, const [atcacert\\_def\\_t](#) \*\*cert\_def)  
*Get the TNG device certificate definition.*
- ATCA\_STATUS [tng\\_get\\_device\\_pubkey](#) (uint8\_t \*public\_key)  
*Uses GenKey command to calculate the public key from the primary device public key.*
  
- const uint8\_t [g\\_tflxtls\\_cert\\_template\\_4\\_device](#) [500]
- const [atcacert\\_def\\_t](#) [g\\_tflxtls\\_cert\\_def\\_4\\_device](#)
- const [atcacert\\_cert\\_element\\_t](#) [g\\_tflxtls\\_cert\\_elements\\_4\\_device](#) []
  
- ATCA\_DLL const [atcacert\\_def\\_t](#) [g\\_tnqlora\\_cert\\_def\\_1\\_signer](#)
  
- ATCA\_DLL const [atcacert\\_def\\_t](#) [g\\_tnqlora\\_cert\\_def\\_2\\_device](#)
  
- const uint8\_t [g\\_cryptoauth\\_root\\_ca\\_002\\_cert](#) []
- const size\_t [g\\_cryptoauth\\_root\\_ca\\_002\\_cert\\_size](#)

- `#define CRYPTOAUTH_ROOT_CA_002_PUBLIC_KEY_OFFSET 266`
- ATCA\_DLL const [atcacert\\_def\\_t](#) `g_tnglora_cert_def_4_device`
- SHARED\_LIB\_EXPORT const `uint8_t` [g\\_tnglora\\_cert\\_template\\_4\\_device](#) []
- SHARED\_LIB\_EXPORT const [atcacert\\_cert\\_element\\_t](#) `g_tnglora_cert_elements_4_device` []
- `#define TNGLORA_CERT_TEMPLATE_4_DEVICE_SIZE 552`
- ATCA\_DLL const [atcacert\\_def\\_t](#) `g_tngtls_cert_def_1_signer`
- SHARED\_LIB\_EXPORT const `uint8_t` [g\\_tngtls\\_cert\\_template\\_1\\_signer](#) []
- SHARED\_LIB\_EXPORT const [atcacert\\_cert\\_element\\_t](#) `g_tngtls_cert_elements_1_signer` []
- `#define TNGTLS_CERT_TEMPLATE_1_SIGNER_SIZE 520`
- ATCA\_DLL const [atcacert\\_def\\_t](#) `g_tngtls_cert_def_2_device`
- SHARED\_LIB\_EXPORT const `uint8_t` [g\\_tngtls\\_cert\\_template\\_2\\_device](#) []
- SHARED\_LIB\_EXPORT const [atcacert\\_cert\\_element\\_t](#) `g_tngtls_cert_elements_2_device` []
- `#define TNGTLS_CERT_TEMPLATE_2_DEVICE_SIZE 505`
- `#define TNGTLS_CERT_ELEMENTS_2_DEVICE_COUNT 2`
- ATCA\_DLL const [atcacert\\_def\\_t](#) `g_tngtls_cert_def_3_device`
- ATCA\_DLL const `uint8_t` [g\\_tngtls\\_cert\\_template\\_3\\_device](#) []
- ATCA\_DLL const [atcacert\\_cert\\_element\\_t](#) `g_tngtls_cert_elements_3_device` []
- `#define TNGTLS_CERT_TEMPLATE_3_DEVICE_SIZE 546`
- int [tng\\_atcacert\\_max\\_device\\_cert\\_size](#) (`size_t` \*max\_cert\_size)  
*Return the maximum possible certificate size in bytes for a TNG device certificate. Certificate can be variable size, so this gives an appropriate buffer size when reading the certificate.*
- int [tng\\_atcacert\\_read\\_device\\_cert](#) (`uint8_t` \*cert, `size_t` \*cert\_size, const `uint8_t` \*signer\_cert)  
*Reads the device certificate for a TNG device.*
- int [tng\\_atcacert\\_device\\_public\\_key](#) (`uint8_t` \*public\_key, `uint8_t` \*cert)  
*Reads the device public key.*
- int [tng\\_atcacert\\_max\\_signer\\_cert\\_size](#) (`size_t` \*max\_cert\_size)  
*Return the maximum possible certificate size in bytes for a TNG signer certificate. Certificate can be variable size, so this gives an appropriate buffer size when reading the certificate.*
- int [tng\\_atcacert\\_read\\_signer\\_cert](#) (`uint8_t` \*cert, `size_t` \*cert\_size)  
*Reads the signer certificate for a TNG device.*
- int [tng\\_atcacert\\_signer\\_public\\_key](#) (`uint8_t` \*public\_key, `uint8_t` \*cert)  
*Reads the signer public key.*
- int [tng\\_atcacert\\_root\\_cert\\_size](#) (`size_t` \*cert\_size)  
*Get the size of the TNG root cert.*
- int [tng\\_atcacert\\_root\\_cert](#) (`uint8_t` \*cert, `size_t` \*cert\_size)  
*Get the TNG root cert.*
- int [tng\\_atcacert\\_root\\_public\\_key](#) (`uint8_t` \*public\_key)  
*Gets the root public key.*

### 19.1.1 Detailed Description

These methods provide some convenience functions (mostly around certificates) for TNG devices, which currently include ATECC608A-MAHTN-T.

### 19.1.2 Function Documentation

#### 19.1.2.1 tng\_atcacert\_device\_public\_key()

```
int tng_atcacert_device_public_key (
    uint8_t * public_key,
    uint8_t * cert )
```

Reads the device public key.

##### Parameters

out	<i>public_key</i>	Public key will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve.
in	<i>cert</i>	If supplied, the device public key is used from this certificate. If set to NULL, the device public key is read from the device.

##### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

#### 19.1.2.2 tng\_atcacert\_max\_device\_cert\_size()

```
int tng_atcacert_max_device_cert_size (
    size_t * max_cert_size )
```

Return the maximum possible certificate size in bytes for a TNG device certificate. Certificate can be variable size, so this gives an appropriate buffer size when reading the certificate.

##### Parameters

out	<i>max_cert_size</i>	Maximum certificate size will be returned here in bytes.
-----	----------------------	--

##### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

#### 19.1.2.3 tng\_atcacert\_max\_signer\_cert\_size()

```
int tng_atcacert_max_signer_cert_size (
    size_t * max_cert_size )
```

Return the maximum possible certificate size in bytes for a TNG signer certificate. Certificate can be variable size, so this gives an appropriate buffer size when reading the certificate.



Parameters

out	<i>max_cert_size</i>	Maximum certificate size will be returned here in bytes.
-----	----------------------	--

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.1.2.4 tng\_atcacert\_read\_device\_cert()

```
int tng_atcacert_read_device_cert (
    uint8_t * cert,
    size_t * cert_size,
    const uint8_t * signer_cert )
```

Reads the device certificate for a TNG device.

Parameters

out	<i>cert</i>	Buffer to received the certificate (DER format).
in, out	<i>cert_size</i>	As input, the size of the cert buffer in bytes. As output, the size of the certificate returned in cert in bytes.
in	<i>signer_cert</i>	If supplied, the signer public key is used from this certificate. If set to NULL, the signer public key is read from the device.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.1.2.5 tng\_atcacert\_read\_signer\_cert()

```
int tng_atcacert_read_signer_cert (
    uint8_t * cert,
    size_t * cert_size )
```

Reads the signer certificate for a TNG device.

Parameters

out	<i>cert</i>	Buffer to received the certificate (DER format).
in, out	<i>cert_size</i>	As input, the size of the cert buffer in bytes. As output, the size of the certificate returned in cert in bytes.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.1.2.6 tng\_atcacert\_root\_cert()

```
int tng_atcacert_root_cert (
    uint8_t * cert,
    size_t * cert_size )
```

Get the TNG root cert.

Parameters

out	cert	Buffer to received the certificate (DER format).
in, out	cert_size	As input, the size of the cert buffer in bytes. As output, the size of the certificate returned in cert in bytes.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.1.2.7 tng\_atcacert\_root\_cert\_size()

```
int tng_atcacert_root_cert_size (
    size_t * cert_size )
```

Get the size of the TNG root cert.

Parameters

out	cert_size	Certificate size will be returned here in bytes.
-----	-----------	--

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.1.2.8 tng\_atcacert\_root\_public\_key()

```
int tng_atcacert_root_public_key (
    uint8_t * public_key )
```

Gets the root public key.

Parameters

out	<i>public_key</i>	Public key will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve.
-----	-------------------	--

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.1.2.9 tng\_atcacert\_signer\_public\_key()

```
int tng_atcacert_signer_public_key (
    uint8_t * public_key,
    uint8_t * cert )
```

Reads the signer public key.

Parameters

out	<i>public_key</i>	Public key will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve.
in	<i>cert</i>	If supplied, the signer public key is used from this certificate. If set to NULL, the signer public key is read from the device.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.1.2.10 tng\_get\_device\_cert\_def()

```
ATCA_STATUS tng_get_device_cert_def (
    const atcacert_def_t ** cert_def )
```

Get the TNG device certificate definition.

Parameters

out	<i>cert_def</i>	TNG device certificate definition is returned here.
-----	-----------------	---

Returns

ATCA\_SUCCESS on success, otherwise an error code.

## 19.1 TNG API (tng\_)

---

### 19.1.2.11 tng\_get\_device\_cert\_def\_ext()

```
ATCA_STATUS tng_get_device_cert_def_ext (
    ATCADevice device,
    const atcacert_def_t ** cert_def )
```

Get the TNG device certificate definition.

#### Parameters

in	<i>device</i>	Pointer to the device context pointer
out	<i>cert_def</i>	TNG device certificate definition is returned here.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.1.2.12 tng\_get\_device\_pubkey()

```
ATCA_STATUS tng_get_device_pubkey (
    uint8_t * public_key )
```

Uses GenKey command to calculate the public key from the primary device public key.

#### Parameters

out	<i>public_key</i>	Public key will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve.
-----	-------------------	--

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.1.2.13 tng\_map\_get\_device\_cert\_def()

```
const atcacert_def_t * tng_map_get_device_cert_def (
    int index )
```

Helper function to iterate through all trust cert definitions.

#### Parameters

in	<i>index</i>	Map index
----	--------------	-----------

## Returns

non-null value if success, otherwise NULL

## 19.2 Basic Crypto API methods (atcab\_)

These methods provide the most convenient, simple API to CryptoAuth chips.

### Macros

- #define **atcab\_get\_addr**(...) **calib\_get\_addr**(\_\_VA\_ARGS\_\_)
- #define **atca\_execute\_command**(...) **calib\_execute\_command**(\_\_VA\_ARGS\_\_)
- #define **SHA\_CONTEXT\_MAX\_SIZE** (109)

### Functions

- ATCA\_STATUS **atcab\_version** (char \*ver\_str)  
*basic API methods are all prefixed with atcab\_ (CryptoAuthLib Basic) the fundamental premise of the basic API is it is based on a single interface instance and that instance is global, so all basic API commands assume that one global device is the one to operate on.*
- ATCA\_STATUS **atcab\_init\_ext** (ATCADevice \*device, ATCAInterfaceCfg \*cfg)  
*Creates and initializes a ATCADevice context.*
- ATCA\_STATUS **atcab\_init** (ATCAInterfaceCfg \*cfg)  
*Creates a global ATCADevice object used by Basic API.*
- ATCA\_STATUS **atcab\_init\_device** (ATCADevice ca\_device)  
*Initialize the global ATCADevice object to point to one of your choosing for use with all the atcab\_ basic API.*
- ATCA\_STATUS **atcab\_release\_ext** (ATCADevice \*device)  
*release (free) the an ATCADevice instance.*
- ATCA\_STATUS **atcab\_release** (void)  
*release (free) the global ATCADevice instance. This must be called in order to release or free up the interface.*
- ATCADevice **atcab\_get\_device** (void)  
*Get the global device object.*
- ATCADeviceType **atcab\_get\_device\_type\_ext** (ATCADevice device)  
*Get the selected device type of rthe device context.*
- ATCADeviceType **atcab\_get\_device\_type** (void)  
*Get the current device type configured for the global ATCADevice.*
- uint8\_t **atcab\_get\_device\_address** (ATCADevice device)  
*Get the current device address based on the configured device and interface.*
- bool **atcab\_is\_ca\_device** (ATCADeviceType dev\_type)  
*Check whether the device is cryptoauth device.*
- bool **atcab\_is\_ca2\_device** (ATCADeviceType dev\_type)  
*Check whether the device is cryptoauth device.*
- bool **atcab\_is\_ta\_device** (ATCADeviceType dev\_type)  
*Check whether the device is Trust Anchor device.*
- ATCA\_STATUS **atcab\_pbkdf2\_sha256\_ext** (ATCADevice device, const uint32\_t iter, const uint16\_t slot, const uint8\_t \*salt, const size\_t salt\_len, uint8\_t \*result, size\_t result\_len)
- ATCA\_STATUS **atcab\_pbkdf2\_sha256** (const uint32\_t iter, const uint16\_t slot, const uint8\_t \*salt, const size\_t salt\_len, uint8\_t \*result, size\_t result\_len)
- ATCA\_STATUS **atcab\_wakeup** (void)

- wakeup the CryptoAuth device*
- ATCA\_STATUS [atcab\\_idle](#) (void)
- idle the CryptoAuth device*
- ATCA\_STATUS [atcab\\_sleep](#) (void)
- invoke sleep on the CryptoAuth device*
- ATCA\_STATUS [atcab\\_get\\_zone\\_size](#) (uint8\_t zone, uint16\_t slot, size\_t \*size)
- Gets the size of the specified zone in bytes.*
- ATCA\_STATUS [atcab\\_get\\_zone\\_size\\_ext](#) (ATCADevice device, uint8\_t zone, uint16\_t slot, size\_t \*size)
- Gets the size of the specified zone in bytes.*
- ATCA\_STATUS [atcab\\_aes](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*aes\_in, uint8\_t \*aes\_out)
- Compute the AES-128 encrypt, decrypt, or GFM calculation.*
- ATCA\_STATUS [atcab\\_aes\\_encrypt](#) (uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*plaintext, uint8\_t \*ciphertext)
- Perform an AES-128 encrypt operation with a key in the device.*
- ATCA\_STATUS [atcab\\_aes\\_encrypt\\_ext](#) (ATCADevice device, uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*plaintext, uint8\_t \*ciphertext)
- Perform an AES-128 encrypt operation with a key in the device.*
- ATCA\_STATUS [atcab\\_aes\\_decrypt](#) (uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*ciphertext, uint8\_t \*plaintext)
- Perform an AES-128 decrypt operation with a key in the device.*
- ATCA\_STATUS [atcab\\_aes\\_decrypt\\_ext](#) (ATCADevice device, uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*ciphertext, uint8\_t \*plaintext)
- Perform an AES-128 decrypt operation with a key in the device.*
- ATCA\_STATUS [atcab\\_aes\\_gfm](#) (const uint8\_t \*h, const uint8\_t \*input, uint8\_t \*output)
- Perform a Galois Field Multiply (GFM) operation.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_init](#) (atca\_aes\_gcm\_ctx\_t \*ctx, uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*iv, size\_t iv\_size)
- Initialize context for AES GCM operation with an existing IV, which is common when starting a decrypt operation.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_init\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*iv, size\_t iv\_size)
- Initialize context for AES GCM operation with an existing IV, which is common when starting a decrypt operation.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_init\\_rand](#) (atca\_aes\_gcm\_ctx\_t \*ctx, uint16\_t key\_id, uint8\_t key\_block, size\_t rand\_size, const uint8\_t \*free\_field, size\_t free\_field\_size, uint8\_t \*iv)
- Initialize context for AES GCM operation with a IV composed of a random and optional fixed(free) field, which is common when starting an encrypt operation.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_aad\\_update](#) (atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*aad, uint32\_t aad\_size)
- Process Additional Authenticated Data (AAD) using GCM mode and a key within the ATECC608 device.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_aad\\_update\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*aad, uint32\_t aad\_size)
- Process Additional Authenticated Data (AAD) using GCM mode and a key within the ATECC608 device.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_encrypt\\_update](#) (atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*plaintext, uint32\_t plaintext\_size, uint8\_t \*ciphertext)
- Encrypt data using GCM mode and a key within the ATECC608 device. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_encrypt\\_update\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*plaintext, uint32\_t plaintext\_size, uint8\_t \*ciphertext)
- Encrypt data using GCM mode and a key within the ATECC608 device. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_encrypt\\_finish](#) (atca\_aes\_gcm\_ctx\_t \*ctx, uint8\_t \*tag, size\_t tag\_size)
- Complete a GCM encrypt operation returning the authentication tag.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_encrypt\\_finish\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, uint8\_t \*tag, size\_t tag\_size)

Complete a GCM encrypt operation returning the authentication tag.

- ATCA\_STATUS [atcab\\_aes\\_gcm\\_decrypt\\_update](#) (atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*ciphertext, uint32\_t ciphertext\_size, uint8\_t \*plaintext)

Decrypt data using GCM mode and a key within the ATECC608 device. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function.

- ATCA\_STATUS [atcab\\_aes\\_gcm\\_decrypt\\_update\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*ciphertext, uint32\_t ciphertext\_size, uint8\_t \*plaintext)

Decrypt data using GCM mode and a key within the ATECC608 device. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function.

- ATCA\_STATUS [atcab\\_aes\\_gcm\\_decrypt\\_finish](#) (atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*tag, size\_t tag\_size, bool \*is\_verified)

Complete a GCM decrypt operation verifying the authentication tag.

- ATCA\_STATUS [atcab\\_aes\\_gcm\\_decrypt\\_finish\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*tag, size\_t tag\_size, bool \*is\_verified)

Complete a GCM decrypt operation verifying the authentication tag.

- ATCA\_STATUS [atcab\\_checkmac](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*challenge, const uint8\_t \*response, const uint8\_t \*other\_data)

Compares a MAC response with input values.

- ATCA\_STATUS [atcab\\_checkmac\\_with\\_response\\_mac](#) (uint8\_t mode, const uint8\_t \*challenge, const uint8\_t \*response, const uint8\_t \*other\_data, uint8\_t \*mac)

Compares a MAC response with input values. SHA105 device can generate optional mac Output response mac mode only supports in SHA105 device.

- ATCA\_STATUS [atcab\\_counter](#) (uint8\_t mode, uint16\_t counter\_id, uint32\_t \*counter\_value)

Compute the Counter functions.

- ATCA\_STATUS [atcab\\_counter\\_increment](#) (uint16\_t counter\_id, uint32\_t \*counter\_value)

Increments one of the device's monotonic counters.

- ATCA\_STATUS [atcab\\_counter\\_read](#) (uint16\_t counter\_id, uint32\_t \*counter\_value)

Read one of the device's monotonic counters.

- ATCA\_STATUS [atcab\\_derivekey](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*mac)

Executes the DeviveKey command for deriving a new key from a nonce (TempKey) and an existing key.

- ATCA\_STATUS [atcab\\_derivekey\\_ext](#) (ATCADevice device, uint8\_t mode, uint16\_t key\_id, const uint8\_t \*mac)

Executes the DeviveKey command for deriving a new key from a nonce (TempKey) and an existing key.

- ATCA\_STATUS [atcab\\_ecdh\\_base](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*public\_key, uint8\_t \*pms, uint8\_t \*out\_nonce)

Base function for generating premaster secret key using ECDH.

- ATCA\_STATUS [atcab\\_ecdh](#) (uint16\_t key\_id, const uint8\_t \*public\_key, uint8\_t \*pms)

ECDH command with a private key in a slot and the premaster secret is returned in the clear.

- ATCA\_STATUS [atcab\\_ecdh\\_enc](#) (uint16\_t key\_id, const uint8\_t \*public\_key, uint8\_t \*pms, const uint8\_t \*read\_key, uint16\_t read\_key\_id, const uint8\_t num\_in[(20)])

ECDH command with a private key in a slot and the premaster secret is read from the next slot.

- ATCA\_STATUS [atcab\\_ecdh\\_ioenc](#) (uint16\_t key\_id, const uint8\_t \*public\_key, uint8\_t \*pms, const uint8\_t \*io\_key)

ECDH command with a private key in a slot and the premaster secret is returned encrypted using the IO protection key.

- ATCA\_STATUS [atcab\\_ecdh\\_tempkey](#) (const uint8\_t \*public\_key, uint8\_t \*pms)

ECDH command with a private key in TempKey and the premaster secret is returned in the clear.

- ATCA\_STATUS [atcab\\_ecdh\\_tempkey\\_ioenc](#) (const uint8\_t \*public\_key, uint8\_t \*pms, const uint8\_t \*io\_key)

ECDH command with a private key in TempKey and the premaster secret is returned encrypted using the IO protection key.

- ATCA\_STATUS [atcab\\_gendig](#) (uint8\_t zone, uint16\_t key\_id, const uint8\_t \*other\_data, uint8\_t other\_data\_size)

Issues a GenDig command, which performs a SHA256 hash on the source data indicated by zone with the contents of TempKey. See the CryptoAuth datasheet for your chip to see what the values of zone correspond to.

- ATCA\_STATUS [atcab\\_gendivkey](#) (const uint8\_t \*other\_data)  
*Issues a GenDivKey command to generate the equivalent diversified key as that programmed into the client side device.*
- ATCA\_STATUS [atcab\\_genkey\\_base](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*other\_data, uint8\_t \*public\_key)  
*Issues GenKey command, which can generate a private key, compute a public key, nd/or compute a digest of a public key.*
- ATCA\_STATUS [atcab\\_genkey](#) (uint16\_t key\_id, uint8\_t \*public\_key)  
*Issues GenKey command, which generates a new random private key in slot/handle and returns the public key.*
- ATCA\_STATUS [atcab\\_genkey\\_ext](#) (ATCADevice device, uint16\_t key\_id, uint8\_t \*public\_key)  
*Issues GenKey command, which generates a new random private key in slot/handle and returns the public key.*
- ATCA\_STATUS [atcab\\_get\\_pubkey](#) (uint16\_t key\_id, uint8\_t \*public\_key)  
*Uses GenKey command to calculate the public key from an existing private key in a slot.*
- ATCA\_STATUS [atcab\\_get\\_pubkey\\_ext](#) (ATCADevice device, uint16\_t key\_id, uint8\_t \*public\_key)  
*Uses GenKey command to calculate the public key from an existing private key in a slot.*
- ATCA\_STATUS [atcab\\_hmac](#) (uint8\_t mode, uint16\_t key\_id, uint8\_t \*digest)  
*Issues a HMAC command, which computes an HMAC/SHA-256 digest of a key stored in the device, a challenge, and other information on the device.*
- ATCA\_STATUS [atcab\\_info\\_base](#) (uint8\_t mode, uint16\_t param2, uint8\_t \*out\_data)  
*Issues an Info command, which return internal device information and can control GPIO and the persistent latch.*
- ATCA\_STATUS [atcab\\_info](#) (uint8\_t \*revision)  
*Use the Info command to get the device revision (DevRev).*
- ATCA\_STATUS [atcab\\_info\\_ext](#) (ATCADevice device, uint8\_t \*revision)  
*Use the Info command to get the device revision (DevRev).*
- ATCA\_STATUS [atcab\\_info\\_lock\\_status](#) (uint16\_t param2, uint8\_t \*is\_locked)  
*Use the Info command to get the lock status.*
- ATCA\_STATUS [atcab\\_info\\_chip\\_status](#) (uint8\_t \*chip\_status)  
*Use the Info command to get the chip status.*
- ATCA\_STATUS [atcab\\_info\\_set\\_latch](#) (bool state)  
*Use the Info command to set the persistent latch state for an ATECC608 device.*
- ATCA\_STATUS [atcab\\_info\\_get\\_latch](#) (bool \*state)  
*Use the Info command to get the persistent latch current state for an ATECC608 device.*
- ATCA\_STATUS [atcab\\_kdf](#) (uint8\_t mode, uint16\_t key\_id, const uint32\_t details, const uint8\_t \*message, uint8\_t \*out\_data, uint8\_t \*out\_nonce)  
*Executes the KDF command, which derives a new key in PRF, AES, or HKDF modes.*
- ATCA\_STATUS [atcab\\_lock](#) (uint8\_t mode, uint16\_t summary\_crc)  
*The Lock command prevents future modifications of the Configuration and/or Data and OTP zones. If the device is so configured, then this command can be used to lock individual data slots. This command fails if the designated area is already locked.*
- ATCA\_STATUS [atcab\\_lock\\_config\\_zone](#) (void)  
*Unconditionally (no CRC required) lock the config zone.*
- ATCA\_STATUS [atcab\\_lock\\_config\\_zone\\_ext](#) (ATCADevice device)  
*Unconditionally (no CRC required) lock the config zone.*
- ATCA\_STATUS [atcab\\_lock\\_config\\_zone\\_crc](#) (uint16\_t summary\_crc)  
*Lock the config zone with summary CRC.*
- ATCA\_STATUS [atcab\\_lock\\_data\\_zone](#) (void)  
*Unconditionally (no CRC required) lock the data zone (slots and OTP). for CryptoAuth devices and lock the setup for Trust Anchor device.*
- ATCA\_STATUS [atcab\\_lock\\_data\\_zone\\_ext](#) (ATCADevice device)  
*Unconditionally (no CRC required) lock the data zone (slots and OTP). for CryptoAuth devices and lock the setup for Trust Anchor device.*
- ATCA\_STATUS [atcab\\_lock\\_data\\_zone\\_crc](#) (uint16\_t summary\_crc)



- Lock the data zone (slots and OTP) with summary CRC.*
- ATCA\_STATUS [atcab\\_lock\\_data\\_slot](#) (uint16\_t slot)  
*Lock an individual slot in the data zone on an ATECC device. Not available for ATSHA devices. Slot must be configured to be slot lockable (KeyConfig.Lockable=1) (for cryptoauth devices) or Lock an individual handle in shared data element on an Trust Anchor device (for Trust Anchor devices).*
  - ATCA\_STATUS [atcab\\_lock\\_data\\_slot\\_ext](#) (ATCADevice device, uint16\_t slot)  
*Lock an individual slot in the data zone on an ATECC device. Not available for ATSHA devices. Slot must be configured to be slot lockable (KeyConfig.Lockable=1) (for cryptoauth devices) or Lock an individual handle in shared data element on an Trust Anchor device (for Trust Anchor devices).*
  - ATCA\_STATUS [atcab\\_mac](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*challenge, uint8\_t \*digest)  
*Executes MAC command, which computes a SHA-256 digest of a key stored in the device, a challenge, and other information on the device.*
  - ATCA\_STATUS [atcab\\_nonce\\_base](#) (uint8\_t mode, uint16\_t zero, const uint8\_t \*num\_in, uint8\_t \*rand\_out)  
*Executes Nonce command, which loads a random or fixed nonce/data into the device for use by subsequent commands.*
  - ATCA\_STATUS [atcab\\_nonce](#) (const uint8\_t \*num\_in)  
*Execute a Nonce command in pass-through mode to initialize TempKey to a specified value.*
  - ATCA\_STATUS [atcab\\_nonce\\_load](#) (uint8\_t target, const uint8\_t \*num\_in, uint16\_t num\_in\_size)  
*Execute a Nonce command in pass-through mode to load one of the device's internal buffers with a fixed value.*
  - ATCA\_STATUS [atcab\\_nonce\\_rand](#) (const uint8\_t \*num\_in, uint8\_t \*rand\_out)  
*Execute a Nonce command to generate a random nonce combining a host nonce (num\_in) and a device random number.*
  - ATCA\_STATUS [atcab\\_nonce\\_rand\\_ext](#) (ATCADevice device, const uint8\_t \*num\_in, uint8\_t \*rand\_out)  
*Execute a Nonce command to generate a random nonce combining a host nonce (num\_in) and a device random number.*
  - ATCA\_STATUS [atcab\\_challenge](#) (const uint8\_t \*num\_in)  
*Execute a Nonce command in pass-through mode to initialize TempKey to a specified value.*
  - ATCA\_STATUS [atcab\\_challenge\\_seed\\_update](#) (const uint8\_t \*num\_in, uint8\_t \*rand\_out)  
*Execute a Nonce command to generate a random challenge combining a host nonce (num\_in) and a device random number.*
  - ATCA\_STATUS [atcab\\_priv\\_write](#) (uint16\_t key\_id, const uint8\_t priv\_key[36], uint16\_t write\_key\_id, const uint8\_t write\_key[32], const uint8\_t num\_in[(20)])  
*Executes PrivWrite command, to write externally generated ECC private keys into the device.*
  - ATCA\_STATUS [atcab\\_random](#) (uint8\_t \*rand\_out)  
*Executes Random command, which generates a 32 byte random number from the device.*
  - ATCA\_STATUS [atcab\\_random\\_ext](#) (ATCADevice device, uint8\_t \*rand\_out)  
*Executes Random command, which generates a 32 byte random number from the device.*
  - ATCA\_STATUS [atcab\\_read\\_zone](#) (uint8\_t zone, uint16\_t slot, uint8\_t block, uint8\_t offset, uint8\_t \*data, uint8\_t len)  
*Executes Read command, which reads either 4 or 32 bytes of data from a given slot, configuration zone, or the OTP zone.*
  - ATCA\_STATUS [atcab\\_read\\_zone\\_ext](#) (ATCADevice device, uint8\_t zone, uint16\_t slot, uint8\_t block, uint8\_t offset, uint8\_t \*data, uint8\_t len)  
*Executes Read command, which reads either 4 or 32 bytes of data from a given slot, configuration zone, or the OTP zone.*
  - ATCA\_STATUS [atcab\\_is\\_locked](#) (uint8\_t zone, bool \*is\_locked)  
*Executes Read command, which reads the configuration zone to see if the specified zone is locked.*
  - ATCA\_STATUS [atcab\\_is\\_config\\_locked](#) (bool \*is\_locked)  
*This function check whether configuration zone is locked or not.*
  - ATCA\_STATUS [atcab\\_is\\_config\\_locked\\_ext](#) (ATCADevice device, bool \*is\_locked)  
*This function check whether configuration zone is locked or not.*
  - ATCA\_STATUS [atcab\\_is\\_data\\_locked](#) (bool \*is\_locked)  
*This function check whether data/setup zone is locked or not.*

- ATCA\_STATUS [atcab\\_is\\_data\\_locked\\_ext](#) (ATCADevice device, bool \*is\_locked)  
*This function check whether data/setup zone is locked or not.*
- ATCA\_STATUS [atcab\\_is\\_slot\\_locked](#) (uint16\_t slot, bool \*is\_locked)  
*This function check whether slot/handle is locked or not.*
- ATCA\_STATUS [atcab\\_is\\_slot\\_locked\\_ext](#) (ATCADevice device, uint16\_t slot, bool \*is\_locked)  
*This function check whether slot/handle is locked or not.*
- ATCA\_STATUS [atcab\\_is\\_private\\_ext](#) (ATCADevice device, uint16\_t slot, bool \*is\_private)  
*Check to see if the key is a private key or not.*
- ATCA\_STATUS [atcab\\_is\\_private](#) (uint16\_t slot, bool \*is\_private)
- ATCA\_STATUS [atcab\\_read\\_bytes\\_zone\\_ext](#) (ATCADevice device, uint8\_t zone, uint16\_t slot, size\_t offset, uint8\_t \*data, size\_t length)
- ATCA\_STATUS [atcab\\_read\\_bytes\\_zone](#) (uint8\_t zone, uint16\_t slot, size\_t offset, uint8\_t \*data, size\_t length)  
*Used to read an arbitrary number of bytes from any zone configured for clear reads.*
- ATCA\_STATUS [atcab\\_read\\_serial\\_number](#) (uint8\_t \*serial\_number)  
*This function returns serial number of the device.*
- ATCA\_STATUS [atcab\\_read\\_serial\\_number\\_ext](#) (ATCADevice device, uint8\_t \*serial\_number)  
*This function returns serial number of the device.*
- ATCA\_STATUS [atcab\\_read\\_pubkey](#) (uint16\_t slot, uint8\_t \*public\_key)  
*Executes Read command to read an ECC P256 public key from a slot configured for clear reads.*
- ATCA\_STATUS [atcab\\_read\\_pubkey\\_ext](#) (ATCADevice device, uint16\_t slot, uint8\_t \*public\_key)  
*Executes Read command to read an ECC P256 public key from a slot configured for clear reads.*
- ATCA\_STATUS [atcab\\_read\\_sig](#) (uint16\_t slot, uint8\_t \*sig)  
*Executes Read command to read a 64 byte ECDSA P256 signature from a slot configured for clear reads.*
- ATCA\_STATUS [atcab\\_read\\_config\\_zone](#) (uint8\_t \*config\_data)  
*Executes Read command to read the complete device configuration zone.*
- ATCA\_STATUS [atcab\\_read\\_config\\_zone\\_ext](#) (ATCADevice device, uint8\_t \*config\_data)  
*Executes Read command to read the complete device configuration zone.*
- ATCA\_STATUS [atcab\\_cmp\\_config\\_zone](#) (uint8\_t \*config\_data, bool \*same\_config)  
*Compares a specified configuration zone with the configuration zone currently on the device.*
- ATCA\_STATUS [atcab\\_read\\_enc](#) (uint16\_t key\_id, uint8\_t block, uint8\_t \*data, const uint8\_t \*enc\_key, const uint16\_t enc\_key\_id, const uint8\_t num\_in[(20)])  
*Executes Read command on a slot configured for encrypted reads and decrypts the data to return it as plaintext.*
- ATCA\_STATUS [atcab\\_secureboot](#) (uint8\_t mode, uint16\_t param2, const uint8\_t \*digest, const uint8\_t \*signature, uint8\_t \*mac)  
*Executes Secure Boot command, which provides support for secure boot of an external MCU or MPU.*
- ATCA\_STATUS [atcab\\_secureboot\\_mac](#) (uint8\_t mode, const uint8\_t \*digest, const uint8\_t \*signature, const uint8\_t \*num\_in, const uint8\_t \*io\_key, bool \*is\_verified)  
*Executes Secure Boot command with encrypted digest and validated MAC response using the IO protection key.*
- ATCA\_STATUS [atcab\\_selftest](#) (uint8\_t mode, uint16\_t param2, uint8\_t \*result)  
*Executes the SelfTest command, which performs a test of one or more of the cryptographic engines within the ATECC608 chip.*
- ATCA\_STATUS [atcab\\_sha\\_base](#) (uint8\_t mode, uint16\_t length, const uint8\_t \*data\_in, uint8\_t \*data\_out, uint16\_t \*data\_out\_size)  
*Executes SHA command, which computes a SHA-256 or HMAC/SHA-256 digest for general purpose use by the host system.*
- ATCA\_STATUS [atcab\\_sha\\_start](#) (void)  
*Executes SHA command to initialize SHA-256 calculation engine.*
- ATCA\_STATUS [atcab\\_sha\\_update](#) (const uint8\_t \*message)  
*Executes SHA command to add 64 bytes of message data to the current context.*
- ATCA\_STATUS [atcab\\_sha\\_end](#) (uint8\_t \*digest, uint16\_t length, const uint8\_t \*message)  
*Executes SHA command to complete SHA-256 or HMAC/SHA-256 operation.*
- ATCA\_STATUS [atcab\\_sha\\_read\\_context](#) (uint8\_t \*context, uint16\_t \*context\_size)

*Executes SHA command to read the SHA-256 context back. Only for ATECC608 with SHA-256 contexts. HMAC not supported.*

- ATCA\_STATUS [atcab\\_sha\\_write\\_context](#) (const uint8\_t \*context, uint16\_t context\_size)  
*Executes SHA command to write (restore) a SHA-256 context into the device. Only supported for ATECC608 with SHA-256 contexts.*
- ATCA\_STATUS [atcab\\_sha](#) (uint16\_t length, const uint8\_t \*message, uint8\_t \*digest)  
*Use the SHA command to compute a SHA-256 digest.*
- ATCA\_STATUS [atcab\\_hw\\_sha2\\_256](#) (const uint8\_t \*data, size\_t data\_size, uint8\_t \*digest)  
*Use the SHA command to compute a SHA-256 digest.*
- ATCA\_STATUS [atcab\\_hw\\_sha2\\_256\\_init](#) (atca\_sha256\_ctx\_t \*ctx)  
*Initialize a SHA context for performing a hardware SHA-256 operation on a device. Note that only one SHA operation can be run at a time.*
- ATCA\_STATUS [atcab\\_hw\\_sha2\\_256\\_update](#) (atca\_sha256\_ctx\_t \*ctx, const uint8\_t \*data, size\_t data\_size)  
*Add message data to a SHA context for performing a hardware SHA-256 operation on a device.*
- ATCA\_STATUS [atcab\\_hw\\_sha2\\_256\\_finish](#) (atca\_sha256\_ctx\_t \*ctx, uint8\_t \*digest)  
*Finish SHA-256 digest for a SHA context for performing a hardware SHA-256 operation on a device.*
- ATCA\_STATUS [atcab\\_sha\\_hmac\\_init](#) (atca\_hmac\_sha256\_ctx\_t \*ctx, uint16\_t key\_slot)  
*Executes SHA command to start an HMAC/SHA-256 operation.*
- ATCA\_STATUS [atcab\\_sha\\_hmac\\_update](#) (atca\_hmac\_sha256\_ctx\_t \*ctx, const uint8\_t \*data, size\_t data\_size)  
*Executes SHA command to add an arbitrary amount of message data to a HMAC/SHA-256 operation.*
- ATCA\_STATUS [atcab\\_sha\\_hmac\\_finish](#) (atca\_hmac\_sha256\_ctx\_t \*ctx, uint8\_t \*digest, uint8\_t target)  
*Executes SHA command to complete a HMAC/SHA-256 operation.*
- ATCA\_STATUS [atcab\\_sha\\_hmac](#) (const uint8\_t \*data, size\_t data\_size, uint16\_t key\_slot, uint8\_t \*digest, uint8\_t target)  
*Use the SHA command to compute an HMAC/SHA-256 operation.*
- ATCA\_STATUS [atcab\\_sha\\_hmac\\_ext](#) (ATCADevice device, const uint8\_t \*data, size\_t data\_size, uint16\_t key\_slot, uint8\_t \*digest, uint8\_t target)  
*Use the SHA command to compute an HMAC/SHA-256 operation.*
- ATCA\_STATUS [atcab\\_sign\\_base](#) (uint8\_t mode, uint16\_t key\_id, uint8\_t \*signature)  
*Executes the Sign command, which generates a signature using the ECDSA algorithm.*
- ATCA\_STATUS [atcab\\_sign](#) (uint16\_t key\_id, const uint8\_t \*msg, uint8\_t \*signature)  
*Executes Sign command, to sign a 32-byte external message using the private key in the specified slot. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
- ATCA\_STATUS [atcab\\_sign\\_ext](#) (ATCADevice device, uint16\_t key\_id, const uint8\_t \*msg, uint8\_t \*signature)  
*Executes Sign command, to sign a 32-byte external message using the private key in the specified slot. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
- ATCA\_STATUS [atcab\\_sign\\_internal](#) (uint16\_t key\_id, bool is\_invalidate, bool is\_full\_sn, uint8\_t \*signature)  
*Executes Sign command to sign an internally generated message.*
- ATCA\_STATUS [atcab\\_updateextra](#) (uint8\_t mode, uint16\_t new\_value)  
*Executes UpdateExtra command to update the values of the two extra bytes within the Configuration zone (bytes 84 and 85).*
- ATCA\_STATUS [atcab\\_verify](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*signature, const uint8\_t \*public\_key, const uint8\_t \*other\_data, uint8\_t \*mac)  
*Executes the Verify command, which takes an ECDSA [R,S] signature and verifies that it is correctly generated from a given message and public key. In all cases, the signature is an input to the command.*
- ATCA\_STATUS [atcab\\_verify\\_extern](#) (const uint8\_t \*message, const uint8\_t \*signature, const uint8\_t \*public\_key, bool \*is\_verified)  
*Executes the Verify command, which verifies a signature (ECDSA verify operation) with all components (message, signature, and public key) supplied. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
- ATCA\_STATUS [atcab\\_verify\\_extern\\_ext](#) (ATCADevice device, const uint8\_t \*message, const uint8\_t \*signature, const uint8\_t \*public\_key, bool \*is\_verified)

- Executes the Verify command, which verifies a signature (ECDSA verify operation) with all components (message, signature, and public key) supplied. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
- ATCA\_STATUS [atcab\\_verify\\_extern\\_mac](#) (const uint8\_t \*message, const uint8\_t \*signature, const uint8\_t \*public\_key, const uint8\_t \*num\_in, const uint8\_t \*io\_key, bool \*is\_verified)  
*Executes the Verify command with verification MAC, which verifies a signature (ECDSA verify operation) with all components (message, signature, and public key) supplied. This function is only available on the ATECC608.*
  - ATCA\_STATUS [atcab\\_verify\\_stored](#) (const uint8\_t \*message, const uint8\_t \*signature, uint16\_t key\_id, bool \*is\_verified)  
*Executes the Verify command, which verifies a signature (ECDSA verify operation) with a public key stored in the device. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
  - ATCA\_STATUS [atcab\\_verify\\_stored\\_ext](#) (ATCADevice device, const uint8\_t \*message, const uint8\_t \*signature, uint16\_t key\_id, bool \*is\_verified)  
*Executes the Verify command, which verifies a signature (ECDSA verify operation) with a public key stored in the device. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
  - ATCA\_STATUS [atcab\\_verify\\_stored\\_with\\_tempkey](#) (const uint8\_t \*signature, uint16\_t key\_id, bool \*is\_verified)  
*Executes the Verify command, which verifies a signature (ECDSA verify operation) with a public key stored in the device. keyConfig.reqrndom bit should be set and the message to be signed should be already loaded into TempKey for all devices.*
  - ATCA\_STATUS [atcab\\_verify\\_stored\\_mac](#) (const uint8\_t \*message, const uint8\_t \*signature, uint16\_t key\_id, const uint8\_t \*num\_in, const uint8\_t \*io\_key, bool \*is\_verified)  
*Executes the Verify command with verification MAC, which verifies a signature (ECDSA verify operation) with a public key stored in the device. This function is only available on the ATECC608.*
  - ATCA\_STATUS [atcab\\_verify\\_validate](#) (uint16\_t key\_id, const uint8\_t \*signature, const uint8\_t \*other\_data, bool \*is\_verified)  
*Executes the Verify command in Validate mode to validate a public key stored in a slot.*
  - ATCA\_STATUS [atcab\\_verify\\_invalidate](#) (uint16\_t key\_id, const uint8\_t \*signature, const uint8\_t \*other\_data, bool \*is\_verified)  
*Executes the Verify command in Invalidate mode which invalidates a previously validated public key stored in a slot.*
  - ATCA\_STATUS [atcab\\_write](#) (uint8\_t zone, uint16\_t address, const uint8\_t \*value, const uint8\_t \*mac)  
*Executes the Write command, which writes either one four byte word or a 32-byte block to one of the EEPROM zones on the device. Depending upon the value of the WriteConfig byte for this slot, the data may be required to be encrypted by the system prior to being sent to the device. This command cannot be used to write slots configured as ECC private keys.*
  - ATCA\_STATUS [atcab\\_write\\_zone](#) (uint8\_t zone, uint16\_t slot, uint8\_t block, uint8\_t offset, const uint8\_t \*data, uint8\_t len)  
*Executes the Write command, which writes either 4 or 32 bytes of data into a device zone.*
  - ATCA\_STATUS [atcab\\_write\\_zone\\_ext](#) (ATCADevice device, uint8\_t zone, uint16\_t slot, uint8\_t block, uint8\_t offset, const uint8\_t \*data, uint8\_t len)  
*Executes the Write command, which writes either 4 or 32 bytes of data into a device zone.*
  - ATCA\_STATUS [atcab\\_write\\_bytes\\_zone\\_ext](#) (ATCADevice device, uint8\_t zone, uint16\_t slot, size\_t offset\_bytes, const uint8\_t \*data, size\_t length)  
*Executes the Write command, which writes data into the configuration, otp, or data zones with a given byte offset and length. Offset and length must be multiples of a word (4 bytes).*
  - ATCA\_STATUS [atcab\\_write\\_bytes\\_zone](#) (uint8\_t zone, uint16\_t slot, size\_t offset\_bytes, const uint8\_t \*data, size\_t length)  
*Executes the Write command, which writes data into the configuration, otp, or data zones with a given byte offset and length. Offset and length must be multiples of a word (4 bytes).*
  - ATCA\_STATUS [atcab\\_write\\_pubkey](#) (uint16\_t slot, const uint8\_t \*public\_key)  
*Uses the write command to write a public key to a slot in the proper format.*
  - ATCA\_STATUS [atcab\\_write\\_pubkey\\_ext](#) (ATCADevice device, uint16\_t slot, const uint8\_t \*public\_key)  
*Uses the write command to write a public key to a slot in the proper format.*
  - ATCA\_STATUS [atcab\\_write\\_config\\_zone](#) (const uint8\_t \*config\_data)  
*Executes the Write command, which writes the configuration zone.*

- ATCA\_STATUS [atcab\\_write\\_config\\_zone\\_ext](#) (ATCADevice device, const uint8\_t \*config\_data)  
*Executes the Write command, which writes the configuration zone.*
- ATCA\_STATUS [atcab\\_write\\_enc](#) (uint16\_t key\_id, uint8\_t block, const uint8\_t \*data, const uint8\_t \*enc\_key, const uint16\_t enc\_key\_id, const uint8\_t num\_in[(20)])  
*Executes the Write command, which performs an encrypted write of a 32 byte block into given slot.*
- ATCA\_STATUS [atcab\\_write\\_config\\_counter](#) (uint16\_t counter\_id, uint32\_t counter\_value)  
*Initialize one of the monotonic counters in device with a specific value.*

## Variables

- [ATCADevice](#) [g\\_atcab\\_device\\_ptr](#)
- ATCA\_STATUS [atcab\\_bin2hex](#) (const uint8\_t \*bin, size\_t bin\_size, char \*hex, size\_t \*hex\_size)  
*Convert a binary buffer to a hex string for easy reading.*
- ATCA\_STATUS [atcab\\_bin2hex\\_](#) (const uint8\_t \*bin, size\_t bin\_size, char \*hex, size\_t \*hex\_size, bool is\_↵ pretty, bool is\_space, bool is\_upper)  
*Function that converts a binary buffer to a hex string suitable for easy reading.*
- ATCA\_STATUS [atcab\\_hex2bin](#) (const char \*ascii\_hex, size\_t ascii\_hex\_len, uint8\_t \*binary, size\_t \*bin\_len)  
*Function that converts a hex string to binary buffer.*
- ATCA\_STATUS [atcab\\_hex2bin\\_](#) (const char \*hex, size\_t hex\_size, uint8\_t \*bin, size\_t \*bin\_size, bool is\_↵ \_space)
- ATCA\_STATUS [packHex](#) (const char \*ascii\_hex, size\_t ascii\_hex\_len, char \*packed\_hex, size\_t \*packed\_↵ \_len)  
*Remove spaces from a ASCII hex string.*
- bool [isDigit](#) (char c)  
*Checks to see if a character is an ASCII representation of a digit ((c ge '0') and (c le '9'))*
- bool [isBlankSpace](#) (char c)  
*Checks to see if a character is blank space.*
- bool [isAlpha](#) (char c)  
*Checks to see if a character is an ASCII representation of hex ((c >= 'A') and (c <= 'F')) || ((c >= 'a') and (c <= 'f'))*
- bool [isHexAlpha](#) (char c)  
*Checks to see if a character is an ASCII representation of hex ((c >= 'A') and (c <= 'F')) || ((c >= 'a') and (c <= 'f'))*
- bool [isHex](#) (char c)  
*Returns true if this character is a valid hex character or if this is blankspace (The character can be included in a valid hexstring).*
- bool [isHexDigit](#) (char c)  
*Returns true if this character is a valid hex character.*
- bool [isBase64](#) (char c, const uint8\_t \*rules)  
*Returns true if this character is a valid base 64 character or if this is space (A character can be included in a valid base 64 string).*
- bool [isBase64Digit](#) (char c, const uint8\_t \*rules)  
*Returns true if this character is a valid base 64 character.*
- const uint8\_t \* [atcab\\_b64rules\\_default](#) (void)
- const uint8\_t \* [atcab\\_b64rules\\_mime](#) (void)
- const uint8\_t \* [atcab\\_b64rules\\_urlsafe](#) (void)
- ATCA\_STATUS [atcab\\_base64decode\\_](#) (const char \*encoded, size\_t encoded\_size, uint8\_t \*data, size\_↵ t \*data\_size, const uint8\_t \*rules)  
*Decode base64 string to data with ruleset option.*
- ATCA\_STATUS [atcab\\_base64encode](#) (const uint8\_t \*byte\_array, size\_t array\_len, char \*encoded, size\_↵ t \*encoded\_len)  
*Encode data as base64 string.*

- ATCA\_STATUS [atcab\\_base64encode](#) (const uint8\_t \*data, size\_t data\_size, char \*encoded, size\_t \*encoded\_size, const uint8\_t \*rules)  
*Encode data as base64 string with ruleset option.*
- ATCA\_STATUS [atcab\\_base64decode](#) (const char \*encoded, size\_t encoded\_len, uint8\_t \*byte\_array, size\_t \*array\_len)  
*Decode base64 string to data.*
- ATCA\_STATUS [atcab\\_reversal](#) (const uint8\_t \*bin, size\_t bin\_size, uint8\_t \*dest, size\_t \*dest\_size)  
*To reverse the input data.*
- int [atcab\\_memset\\_s](#) (void \*dest, size\_t destsz, int ch, size\_t count)  
*Guaranteed to perform memory writes regardless of optimization level. Matches memset\_s signature.*
- size\_t [atcab\\_pointer\\_delta](#) (const void \*start, const void \*end)  
*Helper function to calculate the number of bytes between two pointers.*
- char [lib\\_toupper](#) (char c)  
*Converts a character to uppercase.*
- char [lib\\_tolower](#) (char c)  
*Converts a character to lowercase.*

### 19.2.1 Detailed Description

These methods provide the most convenient, simple API to CryptoAuth chips.

### 19.2.2 Function Documentation

#### 19.2.2.1 atcab\_aes()

```
ATCA_STATUS atcab_aes (
    uint8_t mode,
    uint16_t key_id,
    const uint8_t * aes_in,
    uint8_t * aes_out )
```

Compute the AES-128 encrypt, decrypt, or GFM calculation.

#### Parameters

in	<i>mode</i>	The mode for the AES command.
in	<i>key_id</i>	Key location. Can either be a slot number or ATCA_TEMPKEY_KEYID for TempKey.
in	<i>aes_in</i>	Input data to the AES command (16 bytes).
out	<i>aes_out</i>	Output data from the AES command is returned here (16 bytes).

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.



19.2.2.2 atcab\_aes\_decrypt()

```
ATCA_STATUS atcab_aes_decrypt (
    uint16_t key_id,
    uint8_t key_block,
    const uint8_t * ciphertext,
    uint8_t * plaintext )
```

Perform an AES-128 decrypt operation with a key in the device.

Parameters

in	key_id	Key location. Can either be a slot number or ATCA_TEMPKEY_KEYID for TempKey.
in	key_block	Index of the 16-byte block to use within the key location for the actual key.
in	ciphertext	Input ciphertext to be decrypted (16 bytes).
out	plaintext	Output plaintext is returned here (16 bytes).

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.3 atcab\_aes\_decrypt\_ext()

```
ATCA_STATUS atcab_aes_decrypt_ext (
    ATCADevice device,
    uint16_t key_id,
    uint8_t key_block,
    const uint8_t * ciphertext,
    uint8_t * plaintext )
```

Perform an AES-128 decrypt operation with a key in the device.

Parameters

in	device	Device context pointer
in	key_id	Key location. Can either be a slot number or ATCA_TEMPKEY_KEYID for TempKey.
in	key_block	Index of the 16-byte block to use within the key location for the actual key.
in	ciphertext	Input ciphertext to be decrypted (16 bytes).
out	plaintext	Output plaintext is returned here (16 bytes).

Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.4 atcab\_aes\_encrypt()

```
ATCA_STATUS atcab_aes_encrypt (
    uint16_t key_id,
    uint8_t key_block,
    const uint8_t * plaintext,
    uint8_t * ciphertext )
```

Perform an AES-128 encrypt operation with a key in the device.

#### Parameters

in	<i>key_id</i>	Key location. Can either be a slot number or ATCA_TEMPKEY_KEYID for TempKey.
in	<i>key_block</i>	Index of the 16-byte block to use within the key location for the actual key.
in	<i>plaintext</i>	Input plaintext to be encrypted (16 bytes).
out	<i>ciphertext</i>	Output ciphertext is returned here (16 bytes).

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.5 atcab\_aes\_encrypt\_ext()

```
ATCA_STATUS atcab_aes_encrypt_ext (
    ATCADevice device,
    uint16_t key_id,
    uint8_t key_block,
    const uint8_t * plaintext,
    uint8_t * ciphertext )
```

Perform an AES-128 encrypt operation with a key in the device.

#### Parameters

in	<i>device</i>	Device context pointer
in	<i>key_id</i>	Key location. Can either be a slot number or ATCA_TEMPKEY_KEYID for TempKey.
in	<i>key_block</i>	Index of the 16-byte block to use within the key location for the actual key.
in	<i>plaintext</i>	Input plaintext to be encrypted (16 bytes).
out	<i>ciphertext</i>	Output ciphertext is returned here (16 bytes).

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.



### 19.2.2.6 atcab\_aes\_gcm\_aad\_update()

```
ATCA_STATUS atcab_aes_gcm_aad_update (
    atca_aes_gcm_ctx_t * ctx,
    const uint8_t * aad,
    uint32_t aad_size )
```

Process Additional Authenticated Data (AAD) using GCM mode and a key within the ATECC608 device.

This can be called multiple times. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function. When there is AAD to include, this should be called before [atcab\\_aes\\_gcm\\_encrypt\\_update\(\)](#) or [atcab\\_aes\\_gcm\\_decrypt\\_update\(\)](#).

#### Parameters

in	<i>ctx</i>	AES GCM context
in	<i>aad</i>	Additional authenticated data to be added
in	<i>aad_size</i>	Size of aad in bytes

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.7 atcab\_aes\_gcm\_aad\_update\_ext()

```
ATCA_STATUS atcab_aes_gcm_aad_update_ext (
    ATCADevice device,
    atca_aes_gcm_ctx_t * ctx,
    const uint8_t * aad,
    uint32_t aad_size )
```

Process Additional Authenticated Data (AAD) using GCM mode and a key within the ATECC608 device.

This can be called multiple times. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function. When there is AAD to include, this should be called before [atcab\\_aes\\_gcm\\_encrypt\\_update\(\)](#) or [atcab\\_aes\\_gcm\\_decrypt\\_update\(\)](#).

#### Parameters

in	<i>device</i>	Device context
in	<i>ctx</i>	AES GCM context
in	<i>aad</i>	Additional authenticated data to be added
in	<i>aad_size</i>	Size of aad in bytes

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.8 atcab\_aes\_gcm\_decrypt\_finish()

```
ATCA_STATUS atcab_aes_gcm_decrypt_finish (
    atca_aes_gcm_ctx_t * ctx,
    const uint8_t * tag,
    size_t tag_size,
    bool * is_verified )
```

Complete a GCM decrypt operation verifying the authentication tag.

#### Parameters

in	<i>ctx</i>	AES GCM context structure.
in	<i>tag</i>	Expected authentication tag.
in	<i>tag_size</i>	Size of tag in bytes (12 to 16 bytes).
out	<i>is_verified</i>	Returns whether or not the tag verified.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.9 atcab\_aes\_gcm\_decrypt\_finish\_ext()

```
ATCA_STATUS atcab_aes_gcm_decrypt_finish_ext (
    ATCADevice device,
    atca_aes_gcm_ctx_t * ctx,
    const uint8_t * tag,
    size_t tag_size,
    bool * is_verified )
```

Complete a GCM decrypt operation verifying the authentication tag.

#### Parameters

in	<i>device</i>	Device context
in	<i>ctx</i>	AES GCM context structure.
in	<i>tag</i>	Expected authentication tag.
in	<i>tag_size</i>	Size of tag in bytes (12 to 16 bytes).
out	<i>is_verified</i>	Returns whether or not the tag verified.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.10 `atcab_aes_gcm_decrypt_update()`

```
ATCA_STATUS atcab_aes_gcm_decrypt_update (
    atca_aes_gcm_ctx_t * ctx,
    const uint8_t * ciphertext,
    uint32_t ciphertext_size,
    uint8_t * plaintext )
```

Decrypt data using GCM mode and a key within the ATECC608 device. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function.

Parameters

in	<i>ctx</i>	AES GCM context structure.
in	<i>ciphertext</i>	Ciphertext to be decrypted.
in	<i>ciphertext_size</i>	Size of ciphertext in bytes.
out	<i>plaintext</i>	Decrypted data is returned here.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.11 `atcab_aes_gcm_decrypt_update_ext()`

```
ATCA_STATUS atcab_aes_gcm_decrypt_update_ext (
    ATCADevice device,
    atca_aes_gcm_ctx_t * ctx,
    const uint8_t * ciphertext,
    uint32_t ciphertext_size,
    uint8_t * plaintext )
```

Decrypt data using GCM mode and a key within the ATECC608 device. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function.

Parameters

in	<i>device</i>	Device context
in	<i>ctx</i>	AES GCM context structure.
in	<i>ciphertext</i>	Ciphertext to be decrypted.
in	<i>ciphertext_size</i>	Size of ciphertext in bytes.
out	<i>plaintext</i>	Decrypted data is returned here.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.12 atcab\_aes\_gcm\_encrypt\_finish()

```
ATCA_STATUS atcab_aes_gcm_encrypt_finish (
    atca_aes_gcm_ctx_t * ctx,
    uint8_t * tag,
    size_t tag_size )
```

Complete a GCM encrypt operation returning the authentication tag.

#### Parameters

in	<i>ctx</i>	AES GCM context structure.
out	<i>tag</i>	Authentication tag is returned here.
in	<i>tag_size</i>	Tag size in bytes (12 to 16 bytes).

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.13 atcab\_aes\_gcm\_encrypt\_finish\_ext()

```
ATCA_STATUS atcab_aes_gcm_encrypt_finish_ext (
    ATCADevice device,
    atca_aes_gcm_ctx_t * ctx,
    uint8_t * tag,
    size_t tag_size )
```

Complete a GCM encrypt operation returning the authentication tag.

#### Parameters

in	<i>device</i>	Device context
in	<i>ctx</i>	AES GCM context structure.
out	<i>tag</i>	Authentication tag is returned here.
in	<i>tag_size</i>	Tag size in bytes (12 to 16 bytes).

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.14 atcab\_aes\_gcm\_encrypt\_update()

```
ATCA_STATUS atcab_aes_gcm_encrypt_update (
    atca_aes_gcm_ctx_t * ctx,
    const uint8_t * plaintext,
```

```
uint32_t plaintext_size,
uint8_t * ciphertext )
```

Encrypt data using GCM mode and a key within the ATECC608 device. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function.

Parameters

in	<i>ctx</i>	AES GCM context structure.
in	<i>plaintext</i>	Plaintext to be encrypted (16 bytes).
in	<i>plaintext_size</i>	Size of plaintext in bytes.
out	<i>ciphertext</i>	Encrypted data is returned here.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.15 atcab\_aes\_gcm\_encrypt\_update\_ext()

```
ATCA_STATUS atcab_aes_gcm_encrypt_update_ext (
    ATCADevice device,
    atca_aes_gcm_ctx_t * ctx,
    const uint8_t * plaintext,
    uint32_t plaintext_size,
    uint8_t * ciphertext )
```

Encrypt data using GCM mode and a key within the ATECC608 device. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function.

Parameters

in	<i>device</i>	Device context
in	<i>ctx</i>	AES GCM context structure.
in	<i>plaintext</i>	Plaintext to be encrypted (16 bytes).
in	<i>plaintext_size</i>	Size of plaintext in bytes.
out	<i>ciphertext</i>	Encrypted data is returned here.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.16 atcab\_aes\_gcm\_init()

```
ATCA_STATUS atcab_aes_gcm_init (
    atca_aes_gcm_ctx_t * ctx,
```

## 19.2 Basic Crypto API methods (atcab\_)

```
uint16_t key_id,  
uint8_t key_block,  
const uint8_t * iv,  
size_t iv_size )
```

Initialize context for AES GCM operation with an existing IV, which is common when starting a decrypt operation.

### Parameters

in	<i>ctx</i>	AES GCM context to be initialized.
in	<i>key_id</i>	Key location. Can either be a slot number or ATCA_TEMPKEY_KEYID for TempKey.
in	<i>key_block</i>	Index of the 16-byte block to use within the key location for the actual key.
in	<i>iv</i>	Initialization vector.
in	<i>iv_size</i>	Size of IV in bytes. Standard is 12 bytes.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.17 atcab\_aes\_gcm\_init\_ext()

```
ATCA_STATUS atcab_aes_gcm_init_ext (   
    ATCADevice device,  
    atca_aes_gcm_ctx_t * ctx,  
    uint16_t key_id,  
    uint8_t key_block,  
    const uint8_t * iv,  
    size_t iv_size )
```

Initialize context for AES GCM operation with an existing IV, which is common when starting a decrypt operation.

### Parameters

in	<i>device</i>	Device context
in	<i>ctx</i>	AES GCM context to be initialized.
in	<i>key_id</i>	Key location. Can either be a slot number or ATCA_TEMPKEY_KEYID for TempKey.
in	<i>key_block</i>	Index of the 16-byte block to use within the key location for the actual key.
in	<i>iv</i>	Initialization vector.
in	<i>iv_size</i>	Size of IV in bytes. Standard is 12 bytes.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.18 atcab\_aes\_gcm\_init\_rand()

```
ATCA_STATUS atcab_aes_gcm_init_rand (   
    atca_aes_gcm_ctx_t * ctx,
```

```
uint16_t key_id,
uint8_t key_block,
size_t rand_size,
const uint8_t * free_field,
size_t free_field_size,
uint8_t * iv )
```

Initialize context for AES GCM operation with a IV composed of a random and optional fixed(free) field, which is common when starting an encrypt operation.

Parameters

in	<i>ctx</i>	AES CTR context to be initialized.
in	<i>key_id</i>	Key location. Can either be a slot number or ATCA_TEMPKEY_KEYID for TempKey.
in	<i>key_block</i>	Index of the 16-byte block to use within the key location for the actual key.
in	<i>rand_size</i>	Size of the random field in bytes. Minimum and recommended size is 12 bytes. Max is 32 bytes.
in	<i>free_field</i>	Fixed data to include in the IV after the random field. Can be NULL if not used.
in	<i>free_field_size</i>	Size of the free field in bytes.
out	<i>iv</i>	Initialization vector is returned here. Its size will be rand_size and free_field_size combined.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.19 atcab\_aes\_gfm()

```
ATCA_STATUS atcab_aes_gfm (
    const uint8_t * h,
    const uint8_t * input,
    uint8_t * output )
```

Perform a Galois Field Multiply (GFM) operation.

Parameters

in	<i>h</i>	First input value (16 bytes).
in	<i>input</i>	Second input value (16 bytes).
out	<i>output</i>	GFM result is returned here (16 bytes).

Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.20 atcab\_base64decode()

```
ATCA_STATUS atcab_base64decode (
    const char * encoded,
    size_t encoded_len,
    uint8_t * byte_array,
    size_t * array_len )
```

Decode base64 string to data.

#### Parameters

in	<i>encoded</i>	Base64 string to be decoded.
in	<i>encoded_len</i>	Size of the base64 string in bytes.
out	<i>byte_array</i>	Decoded data will be returned here.
in, out	<i>array_len</i>	As input, the size of the byte_array buffer. As output, the length of the decoded data.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.21 atcab\_base64decode\_()

```
ATCA_STATUS atcab_base64decode_ (
    const char * encoded,
    size_t encoded_size,
    uint8_t * data,
    size_t * data_size,
    const uint8_t * rules )
```

Decode base64 string to data with ruleset option.

#### Parameters

in	<i>encoded</i>	Base64 string to be decoded.
in	<i>encoded_size</i>	Size of the base64 string in bytes.
out	<i>data</i>	Decoded data will be returned here.
in, out	<i>data_size</i>	As input, the size of the byte_array buffer. As output, the length of the decoded data.
in	<i>rules</i>	base64 ruleset to use

### 19.2.2.22 atcab\_base64encode()

```
ATCA_STATUS atcab_base64encode (
    const uint8_t * byte_array,
    size_t array_len,
```



```
char * encoded,
size_t * encoded_len )
```

Encode data as base64 string.

Parameters

in	<i>byte_array</i>	Data to be encode in base64.
in	<i>array_len</i>	Size of <i>byte_array</i> in bytes.
in	<i>encoded</i>	Base64 output is returned here.
in, out	<i>encoded_len</i>	As input, the size of the encoded buffer. As output, the length of the encoded base64 character string.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.23 atcab\_base64encode\_()

```
ATCA_STATUS atcab_base64encode_ (
    const uint8_t * data,
    size_t data_size,
    char * encoded,
    size_t * encoded_size,
    const uint8_t * rules )
```

Encode data as base64 string with ruleset option.

Parameters

in	<i>data</i>	The input byte array that will be converted to base 64 encoded characters
in	<i>data_size</i>	The length of the byte array
in	<i>encoded</i>	The output converted to base 64 encoded characters.
in, out	<i>encoded_size</i>	Input: The size of the encoded buffer, Output: The length of the encoded base 64 character string
in	<i>rules</i>	ruleset to use during encoding

19.2.2.24 atcab\_bin2hex()

```
ATCA_STATUS atcab_bin2hex (
    const uint8_t * bin,
    size_t bin_size,
    char * hex,
    size_t * hex_size )
```

Convert a binary buffer to a hex string for easy reading.

### Parameters

in	<i>bin</i>	Input data to convert.
in	<i>bin_size</i>	Size of data to convert.
out	<i>hex</i>	Buffer that receives hex string.
in, out	<i>hex_size</i>	As input, the size of the hex buffer. As output, the size of the output hex.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.25 atcab\_bin2hex\_()

```
ATCA_STATUS atcab_bin2hex_ (  
    const uint8_t * bin,  
    size_t bin_size,  
    char * hex,  
    size_t * hex_size,  
    bool is_pretty,  
    bool is_space,  
    bool is_upper )
```

Function that converts a binary buffer to a hex string suitable for easy reading.

### Parameters

in	<i>bin</i>	Input data to convert.
in	<i>bin_size</i>	Size of data to convert.
out	<i>hex</i>	Buffer that receives hex string.
in, out	<i>hex_size</i>	As input, the size of the hex buffer. As output, the size of the output hex.
in	<i>is_pretty</i>	Indicates whether new lines should be added for pretty printing.
in	<i>is_space</i>	Convert the output hex with space between it.
in	<i>is_upper</i>	Convert the output hex to upper case.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.26 atcab\_challenge()

```
ATCA_STATUS atcab_challenge (  
    const uint8_t * num_in )
```

Execute a Nonce command in pass-through mode to initialize TempKey to a specified value.

Parameters

in	<i>num_in</i>	Data to be loaded into TempKey (32 bytes).
----	---------------	--

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.27 atcab\_challenge\_seed\_update()

```
ATCA_STATUS atcab_challenge_seed_update (
    const uint8_t * num_in,
    uint8_t * rand_out )
```

Execute a Nonce command to generate a random challenge combining a host nonce (num\_in) and a device random number.

Parameters

in	<i>num_in</i>	Host nonce to be combined with the device random number (20 bytes).
out	<i>rand_out</i>	Internally generated 32-byte random number that was used in the nonce/challenge calculation is returned here. Can be NULL if not needed.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.28 atcab\_checkmac()

```
ATCA_STATUS atcab_checkmac (
    uint8_t mode,
    uint16_t key_id,
    const uint8_t * challenge,
    const uint8_t * response,
    const uint8_t * other_data )
```

Compares a MAC response with input values.

Parameters

in	<i>mode</i>	Controls which fields within the device are used in the message
in	<i>key_id</i>	Key location in the CryptoAuth device to use for the MAC
in	<i>challenge</i>	Challenge data (32 bytes)
in	<i>response</i>	MAC response data (32 bytes)
in	<i>other_data</i>	OtherData parameter (13 bytes)

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.29 atcab\_checkmac\_with\_response\_mac()

```
ATCA_STATUS atcab_checkmac_with_response_mac (
    uint8_t mode,
    const uint8_t * challenge,
    const uint8_t * response,
    const uint8_t * other_data,
    uint8_t * mac )
```

Compares a MAC response with input values. SHA105 device can generate optional mac Output response mac mode only supports in SHA105 device.

### Parameters

in	<i>mode</i>	Controls which fields within the device are used in the message
in	<i>challenge</i>	Challenge data (32 bytes)
in	<i>response</i>	MAC response data (32 bytes)
in	<i>other_data</i>	OtherData parameter (13 bytes)
out	<i>mac</i>	MAC response (32 bytes)

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.30 atcab\_cmp\_config\_zone()

```
ATCA_STATUS atcab_cmp_config_zone (
    uint8_t * config_data,
    bool * same_config )
```

Compares a specified configuration zone with the configuration zone currently on the device.

This only compares the static portions of the configuration zone and skips those that are unique per device (first 16 bytes) and areas that can change after the configuration zone has been locked (e.g. LastKeyUse).

### Parameters

in	<i>config_data</i>	Full configuration data to compare the device against.
out	<i>same_config</i>	Result is returned here. True if the static portions on the configuration zones are the same.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.31 atcab\_counter()

```
ATCA_STATUS atcab_counter (
    uint8_t mode,
    uint16_t counter_id,
    uint32_t * counter_value )
```

Compute the Counter functions.

Parameters

in	<i>mode</i>	the mode used for the counter
in	<i>counter_id</i>	The counter to be used
out	<i>counter_value</i>	pointer to the counter value returned from device

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.32 atcab\_counter\_increment()

```
ATCA_STATUS atcab_counter_increment (
    uint16_t counter_id,
    uint32_t * counter_value )
```

Increments one of the device's monotonic counters.

Parameters

in	<i>counter_id</i>	Counter to be incremented
out	<i>counter_value</i>	New value of the counter is returned here. Can be NULL if not needed.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.33 atcab\_counter\_read()

```
ATCA_STATUS atcab_counter_read (
    uint16_t counter_id,
    uint32_t * counter_value )
```

## 19.2 Basic Crypto API methods (atcab\_)

---

Read one of the device's monotonic counters.

### Parameters

in	<i>counter_id</i>	Counter to be read
out	<i>counter_value</i>	Counter value is returned here.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.34 atcab\_derivekey()

```
ATCA_STATUS atcab_derivekey (
    uint8_t mode,
    uint16_t key_id,
    const uint8_t * mac )
```

Executes the DeviveKey command for deriving a new key from a nonce (TempKey) and an existing key.

### Parameters

in	<i>mode</i>	Bit 2 must match the value in TempKey.SourceFlag
in	<i>key_id</i>	Key slot to be written
in	<i>mac</i>	Optional 32 byte MAC used to validate operation. NULL if not required.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.35 atcab\_derivekey\_ext()

```
ATCA_STATUS atcab_derivekey_ext (
    ATCADevice device,
    uint8_t mode,
    uint16_t key_id,
    const uint8_t * mac )
```

Executes the DeviveKey command for deriving a new key from a nonce (TempKey) and an existing key.

### Parameters

in	<i>device</i>	Device context
in	<i>mode</i>	Bit 2 must match the value in TempKey.SourceFlag
in	<i>key_id</i>	Key slot to be written
in	<i>mac</i>	Optional 32 byte MAC used to validate operation. NULL if not required.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.36 atcab\_ecdh()

```
ATCA_STATUS atcab_ecdh (
    uint16_t key_id,
    const uint8_t * public_key,
    uint8_t * pms )
```

ECDH command with a private key in a slot and the premaster secret is returned in the clear.

Parameters

in	<i>key_id</i>	Slot of private key for ECDH computation
in	<i>public_key</i>	Public key input to ECDH calculation. X and Y integers in big-endian format. 64 bytes for P256 key.
out	<i>pms</i>	Computed ECDH premaster secret is returned here. 32 bytes.

Returns

ATCA\_SUCCESS on success

19.2.2.37 atcab\_ecdh\_base()

```
ATCA_STATUS atcab_ecdh_base (
    uint8_t mode,
    uint16_t key_id,
    const uint8_t * public_key,
    uint8_t * pms,
    uint8_t * out_nonce )
```

Base function for generating premaster secret key using ECDH.

Parameters

in	<i>mode</i>	Mode to be used for ECDH computation
in	<i>key_id</i>	Slot of key for ECDH computation
in	<i>public_key</i>	Public key input to ECDH calculation. X and Y integers in big-endian format. 64 bytes for P256 key.
out	<i>pms</i>	Computed ECDH pre-master secret is returned here (32 bytes) if returned directly. Otherwise NULL.
out	<i>out_nonce</i>	Nonce used to encrypt pre-master secret. NULL if output encryption not used.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.38 atcab\_ecdh\_enc()

```
ATCA_STATUS atcab_ecdh_enc (
    uint16_t key_id,
    const uint8_t * public_key,
    uint8_t * pms,
    const uint8_t * read_key,
    uint16_t read_key_id,
    const uint8_t num_in[ (20) ] )
```

ECDH command with a private key in a slot and the premaster secret is read from the next slot.

This function only works for even numbered slots with the proper configuration.

Parameters

in	key_id	Slot of key for ECDH computation
in	public_key	Public key input to ECDH calculation. X and Y integers in big-endian format. 64 bytes for P256 key.
out	pms	Computed ECDH premaster secret is returned here (32 bytes).
in	read_key	Read key for the premaster secret slot (key_id 1).
in	read_key_id	Read key slot for read_key.
in	num_in	20 byte host nonce to inject into Nonce calculation

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.39 atcab\_ecdh\_ioenc()

```
ATCA_STATUS atcab_ecdh_ioenc (
    uint16_t key_id,
    const uint8_t * public_key,
    uint8_t * pms,
    const uint8_t * io_key )
```

ECDH command with a private key in a slot and the premaster secret is returned encrypted using the IO protection key.

Parameters

in	key_id	Slot of key for ECDH computation
in	public_key	Public key input to ECDH calculation. X and Y integers in big-endian format. 64 bytes for P256 key.
out	pms	Computed ECDH premaster secret is returned here (32 bytes).
in	io_key	IO protection key.



Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.40 atcab\_ecdh\_tempkey()

```
ATCA_STATUS atcab_ecdh_tempkey (
    const uint8_t * public_key,
    uint8_t * pms )
```

ECDH command with a private key in TempKey and the premaster secret is returned in the clear.

Parameters

in	<i>public_key</i>	Public key input to ECDH calculation. X and Y integers in big-endian format. 64 bytes for P256 key.
out	<i>pms</i>	Computed ECDH premaster secret is returned here (32 bytes).

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.41 atcab\_ecdh\_tempkey\_ioenc()

```
ATCA_STATUS atcab_ecdh_tempkey_ioenc (
    const uint8_t * public_key,
    uint8_t * pms,
    const uint8_t * io_key )
```

ECDH command with a private key in TempKey and the premaster secret is returned encrypted using the IO protection key.

Parameters

in	<i>public_key</i>	Public key input to ECDH calculation. X and Y integers in big-endian format. 64 bytes for P256 key.
out	<i>pms</i>	Computed ECDH premaster secret is returned here (32 bytes).
in	<i>io_key</i>	IO protection key.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.42 atcab\_gendig()

```
ATCA_STATUS atcab_gendig (
    uint8_t zone,
    uint16_t key_id,
    const uint8_t * other_data,
    uint8_t other_data_size )
```

Issues a GenDig command, which performs a SHA256 hash on the source data indicated by zone with the contents of TempKey. See the CryptoAuth datasheet for your chip to see what the values of zone correspond to.

#### Parameters

in	<i>zone</i>	Designates the source of the data to hash with TempKey.
in	<i>key_id</i>	Indicates the key, OTP block, or message order for shared nonce mode.
in	<i>other_data</i>	Four bytes of data for SHA calculation when using a NoMac key, 32 bytes for "Shared Nonce" mode, otherwise ignored (can be NULL).
in	<i>other_data_size</i>	Size of other_data in bytes.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.43 atcab\_gendivkey()

```
ATCA_STATUS atcab_gendivkey (
    const uint8_t * other_data )
```

Issues a GenDivKey command to generate the equivalent diversified key as that programmed into the client side device.

#### Parameters

in	<i>device</i>	Device context pointer
in	<i>other_data</i>	Must match data used when generating the diversified key in the client device

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.44 atcab\_genkey()

```
ATCA_STATUS atcab_genkey (
    uint16_t key_id,
    uint8_t * public_key )
```

Issues GenKey command, which generates a new random private key in slot/handle and returns the public key.

Parameters

in	<i>key_id</i>	Slot number where an ECC private key is configured. Can also be ATCA_TEMPKEY_KEYID to generate a private key in TempKey.
out	<i>public_key</i>	Public key will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve. Set to NULL if public key isn't required.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.45 atcab\_genkey\_base()

```
ATCA_STATUS atcab_genkey_base (
    uint8_t mode,
    uint16_t key_id,
    const uint8_t * other_data,
    uint8_t * public_key )
```

Issues GenKey command, which can generate a private key, compute a public key, nd/or compute a digest of a public key.

Parameters

in	<i>mode</i>	Mode determines what operations the GenKey command performs.
in	<i>key_id</i>	Slot to perform the GenKey command on.
in	<i>other_data</i>	OtherData for PubKey digest calculation. Can be set to NULL otherwise.
out	<i>public_key</i>	If the mode indicates a public key will be calculated, it will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve. Set to NULL if public key isn't required.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.46 atcab\_genkey\_ext()

```
ATCA_STATUS atcab_genkey_ext (
    ATCADevice device,
    uint16_t key_id,
    uint8_t * public_key )
```

Issues GenKey command, which generates a new random private key in slot/handle and returns the public key.

## 19.2 Basic Crypto API methods (atcab\_)

---

### Parameters

in	<i>device</i>	Device context
in	<i>key_id</i>	Slot number where an ECC private key is configured. Can also be ATCA_TEMPKEY_KEYID to generate a private key in TempKey.
out	<i>public_key</i>	Public key will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve. Set to NULL if public key isn't required.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.47 atcab\_get\_device()

```
ATCADevice atcab_get_device (  
    void )
```

Get the global device object.

### Returns

instance of global ATCADevice

#### 19.2.2.48 atcab\_get\_device\_address()

```
uint8_t atcab_get_device_address (  
    ATCADevice device )
```

Get the current device address based on the configured device and interface.

### Returns

the device address if applicable else 0xFF

#### 19.2.2.49 atcab\_get\_device\_type()

```
ATCADeviceType atcab_get_device_type (  
    void )
```

Get the current device type configured for the global ATCADevice.

### Returns

Device type if basic api is initialized or ATCA\_DEV\_UNKNOWN.

#### 19.2.2.50 atcab\_get\_device\_type\_ext()

```
ATCADeviceType atcab_get_device_type_ext (  
    ATCADevice device )
```

Get the selected device type of the device context.

Parameters

in	<i>device</i>	Device context pointer
----	---------------	------------------------

Returns

Device type if basic api is initialized or ATCA\_DEV\_UNKNOWN.

19.2.2.51 atcab\_get\_pubkey()

```
ATCA_STATUS atcab_get_pubkey (
    uint16_t key_id,
    uint8_t * public_key )
```

Uses GenKey command to calculate the public key from an existing private key in a slot.

Parameters

in	<i>key_id</i>	Slot number of the private key.
out	<i>public_key</i>	Public key will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve. Set to NULL if public key isn't required.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.52 atcab\_get\_pubkey\_ext()

```
ATCA_STATUS atcab_get_pubkey_ext (
    ATCADevice device,
    uint16_t key_id,
    uint8_t * public_key )
```

Uses GenKey command to calculate the public key from an existing private key in a slot.

Parameters

in	<i>key_id</i>	Slot number of the private key.
out	<i>public_key</i>	Public key will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve. Set to NULL if public key isn't required.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.53 atcab\_get\_zone\_size()

```
ATCA_STATUS atcab_get_zone_size (
    uint8_t zone,
    uint16_t slot,
    size_t * size )
```

Gets the size of the specified zone in bytes.

#### Parameters

in	<i>zone</i>	Zone to get size information from. Config(0), OTP(1), or Data(2) which requires a slot.
in	<i>slot</i>	If zone is Data(2), the slot to query for size.
out	<i>size</i>	Zone size is returned here.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.54 atcab\_get\_zone\_size\_ext()

```
ATCA_STATUS atcab_get_zone_size_ext (
    ATCADevice device,
    uint8_t zone,
    uint16_t slot,
    size_t * size )
```

Gets the size of the specified zone in bytes.

#### Parameters

in	<i>device</i>	Device context
in	<i>zone</i>	Zone to get size information from. Config(0), OTP(1), or Data(2) which requires a slot.
in	<i>slot</i>	If zone is Data(2), the slot to query for size.
out	<i>size</i>	Zone size is returned here.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.55 atcab\_hex2bin()

```
ATCA_STATUS atcab_hex2bin (
    const char * ascii_hex,
```

```
size_t ascii_hex_len,  
uint8_t * binary,  
size_t * bin_len )
```

Function that converts a hex string to binary buffer.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>ascii_hex</i>	Input buffer to convert
in	<i>ascii_hex_len</i>	Length of buffer to convert
out	<i>binary</i>	Buffer that receives binary
in, out	<i>bin_len</i>	As input, the size of the bin buffer. As output, the size of the bin data.

19.2.2.56 atcab\_hmac()

```
ATCA_STATUS atcab_hmac (  
    uint8_t mode,  
    uint16_t key_id,  
    uint8_t * digest )
```

Issues a HMAC command, which computes an HMAC/SHA-256 digest of a key stored in the device, a challenge, and other information on the device.

Parameters

in	<i>mode</i>	Controls which fields within the device are used in the message.
in	<i>key_id</i>	Which key is to be used to generate the response. Bits 0:3 only are used to select a slot but all 16 bits are used in the HMAC message.
out	<i>digest</i>	HMAC digest is returned in this buffer (32 bytes).

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.57 atcab\_hw\_sha2\_256()

```
ATCA_STATUS atcab_hw_sha2_256 (  
    const uint8_t * data,  
    size_t data_size,  
    uint8_t * digest )
```

Use the SHA command to compute a SHA-256 digest.

### Parameters

in	<i>data</i>	Message data to be hashed.
in	<i>data_size</i>	Size of data in bytes.
out	<i>digest</i>	Digest is returned here (32 bytes).

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.58 atcab\_hw\_sha2\_256\_finish()

```
ATCA_STATUS atcab_hw_sha2_256_finish (
    atca_sha256_ctx_t * ctx,
    uint8_t * digest )
```

Finish SHA-256 digest for a SHA context for performing a hardware SHA-256 operation on a device.

### Parameters

in	<i>ctx</i>	SHA256 context
out	<i>digest</i>	SHA256 digest is returned here (32 bytes)

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.59 atcab\_hw\_sha2\_256\_init()

```
ATCA_STATUS atcab_hw_sha2_256_init (
    atca_sha256_ctx_t * ctx )
```

Initialize a SHA context for performing a hardware SHA-256 operation on a device. Note that only one SHA operation can be run at a time.

### Parameters

in	<i>ctx</i>	SHA256 context
----	------------	----------------

### Returns

ATCA\_SUCCESS on success, otherwise an error code.



19.2.2.60 atcab\_hw\_sha2\_256\_update()

```
ATCA_STATUS atcab_hw_sha2_256_update (
    atca_sha256_ctx_t * ctx,
    const uint8_t * data,
    size_t data_size )
```

Add message data to a SHA context for performing a hardware SHA-256 operation on a device.

Parameters

in	<i>ctx</i>	SHA256 context
in	<i>data</i>	Message data to be added to hash.
in	<i>data_size</i>	Size of data in bytes.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.61 atcab\_idle()

```
ATCA_STATUS atcab_idle (
    void )
```

idle the CryptoAuth device

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.62 atcab\_info()

```
ATCA_STATUS atcab_info (
    uint8_t * revision )
```

Use the Info command to get the device revision (DevRev).

Parameters

out	<i>revision</i>	Device revision is returned here (4 bytes).
-----	-----------------	---

Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.63 atcab\_info\_base()

```
ATCA_STATUS atcab_info_base (
    uint8_t mode,
    uint16_t param2,
    uint8_t * out_data )
```

Issues an Info command, which return internal device information and can control GPIO and the persistent latch.

#### Parameters

in	<i>mode</i>	Selects which mode to be used for info command.
in	<i>param2</i>	Selects the particular fields for the mode.
out	<i>out_data</i>	Response from info command (4 bytes). Can be set to NULL if not required.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.64 atcab\_info\_chip\_status()

```
ATCA_STATUS atcab_info_chip_status (
    uint8_t * chip_status )
```

Use the Info command to get the chip status.

#### Parameters

out	<i>chip_status</i>	returns chip status here
-----	--------------------	--------------------------

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.65 atcab\_info\_ext()

```
ATCA_STATUS atcab_info_ext (
    ATCADevice device,
    uint8_t * revision )
```

Use the Info command to get the device revision (DevRev).

#### Parameters

in	<i>device</i>	Device context
out	<i>revision</i>	Device revision is returned here (4 bytes).

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.66 atcab\_info\_get\_latch()

```
ATCA_STATUS atcab_info_get_latch (
    bool * state )
```

Use the Info command to get the persistent latch current state for an ATECC608 device.

Parameters

out	state	The state is returned here. Set (true) or Cier (false).
-----	-------	---

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.67 atcab\_info\_lock\_status()

```
ATCA_STATUS atcab_info_lock_status (
    uint16_t param2,
    uint8_t * is_locked )
```

Use the Info command to get the lock status.

Parameters

in	param2	selects the zone and slot
out	is_locked	returns lock status here

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.68 atcab\_info\_set\_latch()

```
ATCA_STATUS atcab_info_set_latch (
    bool state )
```

Use the Info command to set the persistent latch state for an ATECC608 device.

### Parameters

out	state	Persistent latch state. Set (true) or clear (false).
-----	-------	--

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.69 atcab\_init()

```
ATCA_STATUS atcab_init (
    ATCAIfaceCfg * cfg )
```

Creates a global ATCADevice object used by Basic API.

### Parameters

in	cfg	Logical interface configuration. Some predefined configurations can be found in <a href="#">atca_cfgs.h</a>
----	-----	---

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.70 atcab\_init\_device()

```
ATCA_STATUS atcab_init_device (
    ATCADevice ca_device )
```

Initialize the global ATCADevice object to point to one of your choosing for use with all the atcab\_ basic API.

**Deprecated** This function is not recommended for use generally. Use of `_ext` is recommended instead. You can use `atcab_init_ext` to obtain an initialized instance and associated it with the global structure - but this shouldn't be a required process except in extremely unusual circumstances.

### Parameters

in	ca_device	ATCADevice instance to use as the global Basic API crypto device instance
----	-----------	---

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.71 atcab\_init\_ext()

```
ATCA_STATUS atcab_init_ext (
    ATCADevice * device,
    ATCAIfaceCfg * cfg )
```

Creates and initializes a ATCADevice context.

Parameters

out	device	Pointer to the device context pointer
in	cfg	Logical interface configuration. Some predefined configurations can be found in <a href="#">atca_cfgs.h</a>

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.72 atcab\_is\_ca2\_device()

```
bool atcab_is_ca2_device (
    ATCADeviceType dev_type )
```

Check whether the device is cryptoauth device.

Returns

True if device is cryptoauth device or False.

19.2.2.73 atcab\_is\_ca\_device()

```
bool atcab_is_ca_device (
    ATCADeviceType dev_type )
```

Check whether the device is cryptoauth device.

Returns

True if device is cryptoauth device or False.

19.2.2.74 atcab\_is\_config\_locked()

```
ATCA_STATUS atcab_is_config_locked (
    bool * is_locked )
```

This function check whether configuration zone is locked or not.

### Parameters

out	<i>is_locked</i>	Lock state returned here. True if locked.
-----	------------------	---

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.75 atcab\_is\_config\_locked\_ext()

```
ATCA_STATUS atcab_is_config_locked_ext (
    ATCADevice device,
    bool * is_locked )
```

This function check whether configuration zone is locked or not.

### Parameters

in	<i>device</i>	Device context
out	<i>is_locked</i>	Lock state returned here. True if locked.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.76 atcab\_is\_data\_locked()

```
ATCA_STATUS atcab_is_data_locked (
    bool * is_locked )
```

This function check whether data/setup zone is locked or not.

### Parameters

out	<i>is_locked</i>	Lock state returned here. True if locked.
-----	------------------	---

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.77 atcab\_is\_data\_locked\_ext()

```
ATCA_STATUS atcab_is_data_locked_ext (
    ATCADevice device,
    bool * is_locked )
```

This function check whether data/setup zone is locked or not.

Parameters

in	<i>device</i>	Device context
out	<i>is_locked</i>	Lock state returned here. True if locked.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.78 atcab\_is\_locked()

```
ATCA_STATUS atcab_is_locked (
    uint8_t zone,
    bool * is_locked )
```

Executes Read command, which reads the configuration zone to see if the specified zone is locked.

Parameters

in	<i>zone</i>	The zone to query for locked (use LOCK_ZONE_CONFIG or LOCK_ZONE_DATA).
out	<i>is_locked</i>	Lock state returned here. True if locked.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.79 atcab\_is\_private\_ext()

```
ATCA_STATUS atcab_is_private_ext (
    ATCADevice device,
    uint16_t slot,
    bool * is_private )
```

Check to see if the key is a private key or not.

This function will issue the Read command as many times as is required to read the requested data.

### Parameters

in	<i>slot</i>	Slot number to read from if zone is ATCA_ZONE_DATA(2). Ignored for all other zones.
out	<i>is_private</i>	Returned valud if successful. True if key is private.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.80 atcab\_is\_slot\_locked()

```
ATCA_STATUS atcab_is_slot_locked (
    uint16_t slot,
    bool * is_locked )
```

This function check whether slot/handle is locked or not.

### Parameters

in	<i>slot</i>	Slot to query for locked
out	<i>is_locked</i>	Lock state returned here. True if locked.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.81 atcab\_is\_slot\_locked\_ext()

```
ATCA_STATUS atcab_is_slot_locked_ext (
    ATCADevice device,
    uint16_t slot,
    bool * is_locked )
```

This function check whether slot/handle is locked or not.

### Parameters

in	<i>device</i>	Device context
in	<i>slot</i>	Slot to query for locked
out	<i>is_locked</i>	Lock state returned here. True if locked.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.



19.2.2.82 atcab\_is\_ta\_device()

```
bool atcab_is_ta_device (
    ATCADeviceType dev_type )
```

Check whether the device is Trust Anchor device.

Returns

True if device is Trust Anchor device or False.

19.2.2.83 atcab\_kdf()

```
ATCA_STATUS atcab_kdf (
    uint8_t mode,
    uint16_t key_id,
    const uint32_t details,
    const uint8_t * message,
    uint8_t * out_data,
    uint8_t * out_nonce )
```

Executes the KDF command, which derives a new key in PRF, AES, or HKDF modes.

Generally this function combines a source key with an input string and creates a result key/digest/array.

Parameters

in	<i>mode</i>	Mode determines KDF algorithm (PRF,AES,HKDF), source key location, and target key locations.
in	<i>key_id</i>	Source and target key slots if locations are in the EEPROM. Source key slot is the LSB and target key slot is the MSB.
in	<i>details</i>	Further information about the computation, depending on the algorithm (4 bytes).
in	<i>message</i>	Input value from system (up to 128 bytes). Actual size of message is 16 bytes for AES algorithm or is encoded in the MSB of the details parameter for other algorithms.
out	<i>out_data</i>	Output of the KDF function is returned here. If the result remains in the device, this can be NULL.
out	<i>out_nonce</i>	If the output is encrypted, a 32 byte random nonce generated by the device is returned here. If output encryption is not used, this can be NULL.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.84 atcab\_lock()

```
ATCA_STATUS atcab_lock (
    uint8_t mode,
    uint16_t summary_crc )
```

The Lock command prevents future modifications of the Configuration and/or Data and OTP zones. If the device is so configured, then this command can be used to lock individual data slots. This command fails if the designated area is already locked.

#### Parameters

in	<i>mode</i>	Zone, and/or slot, and summary check (bit 7).
in	<i>summary_crc</i>	CRC of the config or data zones. Ignored for slot locks or when mode bit 7 is set.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.85 atcab\_lock\_config\_zone()

```
ATCA_STATUS atcab_lock_config_zone (
    void )
```

Unconditionally (no CRC required) lock the config zone.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.86 atcab\_lock\_config\_zone\_crc()

```
ATCA_STATUS atcab_lock_config_zone_crc (
    uint16_t summary_crc )
```

Lock the config zone with summary CRC.

The CRC is calculated over the entire config zone contents. 48 bytes for TA100, 88 bytes for ATSHA devices, 128 bytes for ATECC devices. Lock will fail if the provided CRC doesn't match the internally calculated one.

#### Parameters

in	<i>summary_crc</i>	Expected CRC over the config zone.
----	--------------------	------------------------------------

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

**19.2.2.87 atcab\_lock\_config\_zone\_ext()**

```
ATCA_STATUS atcab_lock_config_zone_ext (
    ATCADevice device )
```

Unconditionally (no CRC required) lock the config zone.

**Parameters**

in	<i>device</i>	Device context
----	---------------	----------------

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

**19.2.2.88 atcab\_lock\_data\_slot()**

```
ATCA_STATUS atcab_lock_data_slot (
    uint16_t slot )
```

Lock an individual slot in the data zone on an ATECC device. Not available for ATSHA devices. Slot must be configured to be slot lockable (KeyConfig.Lockable=1) (for cryptoauth devices) or Lock an individual handle in shared data element on an Trust Anchor device (for Trust Anchor devices).

**Parameters**

in	<i>slot</i>	Slot to be locked in data zone.
----	-------------	---------------------------------

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

**19.2.2.89 atcab\_lock\_data\_slot\_ext()**

```
ATCA_STATUS atcab_lock_data_slot_ext (
    ATCADevice device,
    uint16_t slot )
```

Lock an individual slot in the data zone on an ATECC device. Not available for ATSHA devices. Slot must be configured to be slot lockable (KeyConfig.Lockable=1) (for cryptoauth devices) or Lock an individual handle in shared data element on an Trust Anchor device (for Trust Anchor devices).

### Parameters

in	<i>device</i>	Device context
in	<i>slot</i>	Slot to be locked in data zone.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.90 atcab\_lock\_data\_zone()

```
ATCA_STATUS atcab_lock_data_zone (
    void )
```

Unconditionally (no CRC required) lock the data zone (slots and OTP). for CryptoAuth devices and lock the setup for Trust Anchor device.

ConfigZone must be locked and DataZone must be unlocked for the zone to be successfully locked.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.91 atcab\_lock\_data\_zone\_crc()

```
ATCA_STATUS atcab_lock_data_zone_crc (
    uint16_t summary_crc )
```

Lock the data zone (slots and OTP) with summary CRC.

The CRC is calculated over the concatenated contents of all the slots and OTP at the end. Private keys (Key↔Config.Private=1) are skipped. Lock will fail if the provided CRC doesn't match the internally calculated one.

### Parameters

in	<i>summary_crc</i>	Expected CRC over the data zone.
----	--------------------	----------------------------------

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.92 atcab\_lock\_data\_zone\_ext()

```
ATCA_STATUS atcab_lock_data_zone_ext (
    ATCADevice device )
```

Unconditionally (no CRC required) lock the data zone (slots and OTP). for CryptoAuth devices and lock the setup for Trust Anchor device.

Parameters

in	device	Device context ConfigZone must be locked and DataZone must be unlocked for the zone to be successfully locked.
----	--------	--

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.93 atcab\_mac()

```
ATCA_STATUS atcab_mac (
    uint8_t mode,
    uint16_t key_id,
    const uint8_t * challenge,
    uint8_t * digest )
```

Executes MAC command, which computes a SHA-256 digest of a key stored in the device, a challenge, and other information on the device.

Parameters

in	mode	Controls which fields within the device are used in the message
in	key_id	Key in the CryptoAuth device to use for the MAC
in	challenge	Challenge message (32 bytes). May be NULL if mode indicates a challenge isn't required.
out	digest	MAC response is returned here (32 bytes).

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.94 atcab\_nonce()

```
ATCA_STATUS atcab_nonce (
    const uint8_t * num_in )
```

Execute a Nonce command in pass-through mode to initialize TempKey to a specified value.

## 19.2 Basic Crypto API methods (atcab\_)

---

### Parameters

in	<i>num_in</i>	Data to be loaded into TempKey (32 bytes).
----	---------------	--

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.95 atcab\_nonce\_base()

```
ATCA_STATUS atcab_nonce_base (
    uint8_t mode,
    uint16_t zero,
    const uint8_t * num_in,
    uint8_t * rand_out )
```

Executes Nonce command, which loads a random or fixed nonce/data into the device for use by subsequent commands.

### Parameters

in	<i>mode</i>	Controls the mechanism of the internal RNG or fixed write.
in	<i>zero</i>	Param2, normally 0, but can be used to indicate a nonce calculation mode (bit 15).
in	<i>num_in</i>	Input value to either be included in the nonce calculation in random modes (20 bytes) or to be written directly (32 bytes or 64 bytes(ATECC608)) in pass-through mode.
out	<i>rand_out</i>	If using a random mode, the internally generated 32-byte random number that was used in the nonce calculation is returned here. Can be NULL if not needed.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.96 atcab\_nonce\_load()

```
ATCA_STATUS atcab_nonce_load (
    uint8_t target,
    const uint8_t * num_in,
    uint16_t num_in_size )
```

Execute a Nonce command in pass-through mode to load one of the device's internal buffers with a fixed value.

For the ATECC608, available targets are TempKey (32 or 64 bytes), Message Digest Buffer (32 or 64 bytes), or the Alternate Key Buffer (32 bytes). For all other devices, only TempKey (32 bytes) is available.

Parameters

in	<i>target</i>	Target device buffer to load. Can be NONCE_MODE_TARGET_TEMPKEY, NONCE_MODE_TARGET_MSGDIGBUF, or NONCE_MODE_TARGET_ALTKEYBUF.
in	<i>num_in</i>	Data to load into the buffer.
in	<i>num_in_size</i>	Size of num_in in bytes. Can be 32 or 64 bytes depending on device and target.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.97 atcab\_nonce\_rand()

```
ATCA_STATUS atcab_nonce_rand (
    const uint8_t * num_in,
    uint8_t * rand_out )
```

Execute a Nonce command to generate a random nonce combining a host nonce (num\_in) and a device random number.

Parameters

in	<i>num_in</i>	Host nonce to be combined with the device random number (20 bytes).
out	<i>rand_out</i>	Internally generated 32-byte random number that was used in the nonce/challenge calculation is returned here. Can be NULL if not needed.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.98 atcab\_nonce\_rand\_ext()

```
ATCA_STATUS atcab_nonce_rand_ext (
    ATCADevice device,
    const uint8_t * num_in,
    uint8_t * rand_out )
```

Execute a Nonce command to generate a random nonce combining a host nonce (num\_in) and a device random number.

Parameters

in	<i>device</i>	Device context
in	<i>num_in</i>	Host nonce to be combined with the device random number (20 bytes).
out	<i>rand_out</i>	Internally generated 32-byte random number that was used in the nonce/challenge calculation is returned here. Can be NULL if not needed.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.99 atcab\_priv\_write()

```
ATCA_STATUS atcab_priv_write (
    uint16_t key_id,
    const uint8_t priv_key[36],
    uint16_t write_key_id,
    const uint8_t write_key[32],
    const uint8_t num_in[ (20) ] )
```

Executes PrivWrite command, to write externally generated ECC private keys into the device.

### Parameters

in	<i>key_id</i>	Slot to write the external private key into.
in	<i>priv_key</i>	External private key (36 bytes) to be written. The first 4 bytes should be zero for P256 curve.
in	<i>write_key_id</i>	Write key slot. Ignored if write_key is NULL.
in	<i>write_key</i>	Write key (32 bytes). If NULL, perform an unencrypted PrivWrite, which is only available when the data zone is unlocked.
in	<i>num_in</i>	20 byte host nonce to inject into Nonce calculation

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.100 atcab\_random()

```
ATCA_STATUS atcab_random (
    uint8_t * rand_out )
```

Executes Random command, which generates a 32 byte random number from the device.

### Parameters

out	<i>rand_out</i>	32 bytes of random data is returned here.
-----	-----------------	---

### Returns

ATCA\_SUCCESS on success, otherwise an error code.



19.2.2.101    **atcab\_random\_ext()**

```
ATCA_STATUS atcab_random_ext (
    ATCADevice device,
    uint8_t * rand_out )
```

Executes Random command, which generates a 32 byte random number from the device.

Parameters

in	<i>device</i>	Device context pointer
out	<i>rand_out</i>	32 bytes of random data is returned here.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.102    **atcab\_read\_bytes\_zone()**

```
ATCA_STATUS atcab_read_bytes_zone (
    uint8_t zone,
    uint16_t slot,
    size_t offset,
    uint8_t * data,
    size_t length )
```

Used to read an arbitrary number of bytes from any zone configured for clear reads.

This function will issue the Read command as many times as is required to read the requested data.

Parameters

in	<i>zone</i>	Zone to read data from. Option are ATCA_ZONE_CONFIG(0), ATCA_ZONE_OTP(1), or ATCA_ZONE_DATA(2).
in	<i>slot</i>	Slot number to read from if zone is ATCA_ZONE_DATA(2). Ignored for all other zones.
in	<i>offset</i>	Byte offset within the zone to read from.
out	<i>data</i>	Read data is returned here.
in	<i>length</i>	Number of bytes to read starting from the offset.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.103    **atcab\_read\_config\_zone()**

```
ATCA_STATUS atcab_read_config_zone (
    uint8_t * config_data )
```

## 19.2 Basic Crypto API methods (atcab\_)

Executes Read command to read the complete device configuration zone.

### Parameters

out	<i>config_data</i>	Configuration zone data is returned here. 88 bytes for ATSHA devices, 128 bytes for ATECC devices and 48 bytes for Trust Anchor devices.
-----	--------------------	--

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.104 atcab\_read\_config\_zone\_ext()

```
ATCA_STATUS atcab_read_config_zone_ext (
    ATCADevice device,
    uint8_t * config_data )
```

Executes Read command to read the complete device configuration zone.

### Parameters

in	<i>device</i>	device context
out	<i>config_data</i>	Configuration zone data is returned here. 88 bytes for ATSHA devices, 128 bytes for ATECC devices and 48 bytes for Trust Anchor devices.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.105 atcab\_read\_enc()

```
ATCA_STATUS atcab_read_enc (
    uint16_t key_id,
    uint8_t block,
    uint8_t * data,
    const uint8_t * enc_key,
    const uint16_t enc_key_id,
    const uint8_t num_in[ (20) ] )
```

Executes Read command on a slot configured for encrypted reads and decrypts the data to return it as plaintext.

Data zone must be locked for this command to succeed. Can only read 32 byte blocks.

### Parameters

in	<i>key_id</i>	The slot ID to read from.
----	---------------	---------------------------

## Parameters

in	<i>block</i>	Index of the 32 byte block within the slot to read.
out	<i>data</i>	Decrypted (plaintext) data from the read is returned here (32 bytes).
in	<i>enc_key</i>	32 byte ReadKey for the slot being read.
in	<i>enc_key_id</i>	KeyID of the ReadKey being used.
in	<i>num_in</i>	20 byte host nonce to inject into Nonce calculation

returns ATCA\_SUCCESS on success, otherwise an error code.

**19.2.2.106 atcab\_read\_pubkey()**

```
ATCA_STATUS atcab_read_pubkey (
    uint16_t slot,
    uint8_t * public_key )
```

Executes Read command to read an ECC P256 public key from a slot configured for clear reads.

This function assumes the public key is stored using the ECC public key format specified in the datasheet.

## Parameters

in	<i>slot</i>	Slot number to read from. Only slots 8 to 15 are large enough for a public key.
out	<i>public_key</i>	Public key is returned here (64 bytes). Format will be the 32 byte X and Y big-endian integers concatenated.

## Returns

ATCA\_SUCCESS on success, otherwise an error code.

**19.2.2.107 atcab\_read\_pubkey\_ext()**

```
ATCA_STATUS atcab_read_pubkey_ext (
    ATCADevice device,
    uint16_t slot,
    uint8_t * public_key )
```

Executes Read command to read an ECC P256 public key from a slot configured for clear reads.

This function assumes the public key is stored using the ECC public key format specified in the datasheet.

## Parameters

in	<i>device</i>	Device context pointer
in	<i>slot</i>	Slot number to read from. Only slots 8 to 15 are large enough for a public key.
out	<i>public_key</i>	Public key is returned here (64 bytes). Format will be the 32 byte X and Y big-endian integers concatenated.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.108 atcab\_read\_serial\_number()

```
ATCA_STATUS atcab_read_serial_number (
    uint8_t * serial_number )
```

This function returns serial number of the device.

### Parameters

out	<i>serial_number</i>	9 byte serial number is returned here.
-----	----------------------	--

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.109 atcab\_read\_serial\_number\_ext()

```
ATCA_STATUS atcab_read_serial_number_ext (
    ATCADevice device,
    uint8_t * serial_number )
```

This function returns serial number of the device.

### Parameters

in	<i>device</i>	Device context
out	<i>serial_number</i>	9 byte serial number is returned here.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.110 atcab\_read\_sig()

```
ATCA_STATUS atcab_read_sig (
    uint16_t slot,
    uint8_t * sig )
```

Executes Read command to read a 64 byte ECDSA P256 signature from a slot configured for clear reads.

Parameters

in	<i>slot</i>	Slot number to read from. Only slots 8 to 15 are large enough for a signature.
out	<i>sig</i>	Signature will be returned here (64 bytes). Format will be the 32 byte R and S big-endian integers concatenated.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.111 atcab\_read\_zone()

```
ATCA_STATUS atcab_read_zone (
    uint8_t zone,
    uint16_t slot,
    uint8_t block,
    uint8_t offset,
    uint8_t * data,
    uint8_t len )
```

Executes Read command, which reads either 4 or 32 bytes of data from a given slot, configuration zone, or the OTP zone.

When reading a slot or OTP, data zone must be locked and the slot configuration must not be secret for a slot to be successfully read.

Parameters

in	<i>zone</i>	Zone to be read from device. Options are ATCA_ZONE_CONFIG, ATCA_ZONE_OTP, or ATCA_ZONE_DATA.
in	<i>slot</i>	Slot number for data zone and ignored for other zones.
in	<i>block</i>	32 byte block index within the zone.
in	<i>offset</i>	4 byte work index within the block. Ignored for 32 byte reads.
out	<i>data</i>	Read data is returned here.
in	<i>len</i>	Length of the data to be read. Must be either 4 or 32.

returns ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.112 atcab\_read\_zone\_ext()

```
ATCA_STATUS atcab_read_zone_ext (
    ATCADevice device,
    uint8_t zone,
    uint16_t slot,
    uint8_t block,
    uint8_t offset,
    uint8_t * data,
    uint8_t len )
```

## 19.2 Basic Crypto API methods (atcab\_)

---

Executes Read command, which reads either 4 or 32 bytes of data from a given slot, configuration zone, or the OTP zone.

When reading a slot or OTP, data zone must be locked and the slot configuration must not be secret for a slot to be successfully read.

### Parameters

in	<i>device</i>	Device context
in	<i>zone</i>	Zone to be read from device. Options are ATCA_ZONE_CONFIG, ATCA_ZONE_OTP, or ATCA_ZONE_DATA.
in	<i>slot</i>	Slot number for data zone and ignored for other zones.
in	<i>block</i>	32 byte block index within the zone.
in	<i>offset</i>	4 byte work index within the block. Ignored for 32 byte reads.
out	<i>data</i>	Read data is returned here.
in	<i>len</i>	Length of the data to be read. Must be either 4 or 32.

returns ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.113 atcab\_release()

```
ATCA_STATUS atcab_release (
    void )
```

release (free) the global ATCADevice instance. This must be called in order to release or free up the interface.

### Returns

Returns ATCA\_SUCCESS .

### 19.2.2.114 atcab\_release\_ext()

```
ATCA_STATUS atcab_release_ext (
    ATCADevice * device )
```

release (free) the an ATCADevice instance.

### Parameters

in	<i>device</i>	Pointer to the device context pointer
----	---------------	---------------------------------------

### Returns

Returns ATCA\_SUCCESS .

### 19.2.2.115 atcab\_reversal()

```
ATCA_STATUS atcab_reversal (
    const uint8_t * bin,
    size_t bin_size,
    uint8_t * dest,
    size_t * dest_size )
```

To reverse the input data.

#### Parameters

in	<i>bin</i>	Input data to reverse.
in	<i>bin_size</i>	Size of data to reverse.
out	<i>dest</i>	Buffer to store reversed binary data.
in	<i>dest_size</i>	The size of the dest buffer.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.116 atcab\_secureboot()

```
ATCA_STATUS atcab_secureboot (
    uint8_t mode,
    uint16_t param2,
    const uint8_t * digest,
    const uint8_t * signature,
    uint8_t * mac )
```

Executes Secure Boot command, which provides support for secure boot of an external MCU or MPU.

#### Parameters

in	<i>mode</i>	Mode determines what operations the SecureBoot command performs.
in	<i>param2</i>	Not used, must be 0.
in	<i>digest</i>	Digest of the code to be verified (32 bytes).
in	<i>signature</i>	Signature of the code to be verified (64 bytes). Can be NULL when using the FullStore mode.
out	<i>mac</i>	Validating MAC will be returned here (32 bytes). Can be NULL if not required.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.117 atcab\_secureboot\_mac()

```
ATCA_STATUS atcab_secureboot_mac (
    uint8_t mode,
    const uint8_t * digest,
    const uint8_t * signature,
    const uint8_t * num_in,
    const uint8_t * io_key,
    bool * is_verified )
```

Executes Secure Boot command with encrypted digest and validated MAC response using the IO protection key.

#### Parameters

in	<i>mode</i>	Mode determines what operations the SecureBoot command performs.
in	<i>digest</i>	Digest of the code to be verified (32 bytes). This is the plaintext digest (not encrypted).
in	<i>signature</i>	Signature of the code to be verified (64 bytes). Can be NULL when using the FullStore mode.
in	<i>num_in</i>	Host nonce (20 bytes).
in	<i>io_key</i>	IO protection key (32 bytes).
out	<i>is_verified</i>	Verify result is returned here.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.118 atcab\_selftest()

```
ATCA_STATUS atcab_selftest (
    uint8_t mode,
    uint16_t param2,
    uint8_t * result )
```

Executes the SelfTest command, which performs a test of one or more of the cryptographic engines within the ATECC608 chip.

#### Parameters

in	<i>mode</i>	Functions to test. Can be a bit field combining any of the following: SELFTEST_MODE_RNG, SELFTEST_MODE_ECDSA_VERIFY, SELFTEST_MODE_ECDSA_SIGN, SELFTEST_MODE_ECDH, SELFTEST_MODE_AES, SELFTEST_MODE_SHA, SELFTEST_MODE_ALL.
in	<i>param2</i>	Currently unused, should be 0.
out	<i>result</i>	Results are returned here as a bit field.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.



19.2.2.119    **atcab\_sha()**

```
ATCA_STATUS atcab_sha (
    uint16_t length,
    const uint8_t * message,
    uint8_t * digest )
```

Use the SHA command to compute a SHA-256 digest.

Parameters

in	<i>length</i>	Size of message parameter in bytes.
in	<i>message</i>	Message data to be hashed.
out	<i>digest</i>	Digest is returned here (32 bytes).

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.120    **atcab\_sha\_base()**

```
ATCA_STATUS atcab_sha_base (
    uint8_t mode,
    uint16_t length,
    const uint8_t * data_in,
    uint8_t * data_out,
    uint16_t * data_out_size )
```

Executes SHA command, which computes a SHA-256 or HMAC/SHA-256 digest for general purpose use by the host system.

Only the Start(0) and Compute(1) modes are available for ATSHA devices.

Parameters

in	<i>mode</i>	SHA command mode Start(0), Update/Compute(1), End(2), Public(3), HMACstart(4), HMACend(5), Read_Context(6), or Write_Context(7). Also message digest target location for the ATECC608.
in	<i>length</i>	Number of bytes in the message parameter or KeySlot for the HMAC key if Mode is HMACstart(4) or Public(3).
in	<i>data_in</i>	Message bytes to be hashed or Write_Context if restoring a context on the ATECC608. Can be NULL if not required by the mode.
out	<i>data_out</i>	Data returned by the command (digest or context).
in, out	<i>data_out_size</i>	As input, the size of the data_out buffer. As output, the number of bytes returned in data_out.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.121 atcab\_sha\_end()

```
ATCA_STATUS atcab_sha_end (
    uint8_t * digest,
    uint16_t length,
    const uint8_t * message )
```

Executes SHA command to complete SHA-256 or HMAC/SHA-256 operation.

#### Parameters

out	<i>digest</i>	Digest from SHA-256 or HMAC/SHA-256 will be returned here (32 bytes).
in	<i>length</i>	Length of any remaining data to include in hash. Max 64 bytes.
in	<i>message</i>	Remaining data to include in hash. NULL if length is 0.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.122 atcab\_sha\_hmac()

```
ATCA_STATUS atcab_sha_hmac (
    const uint8_t * data,
    size_t data_size,
    uint16_t key_slot,
    uint8_t * digest,
    uint8_t target )
```

Use the SHA command to compute an HMAC/SHA-256 operation.

#### Parameters

in	<i>data</i>	Message data to be hashed.
in	<i>data_size</i>	Size of data in bytes.
in	<i>key_slot</i>	Slot key id to use for the HMAC calculation
out	<i>digest</i>	Digest is returned here (32 bytes).
in	<i>target</i>	Where to save the digest internal to the device. For ATECC608, can be SHA_MODE_TARGET_TEMPKEY, SHA_MODE_TARGET_MSGDIGBUF, or SHA_MODE_TARGET_OUT_ONLY. For all other devices, SHA_MODE_TARGET_TEMPKEY is the only option.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.123    `atcab_sha_hmac_ext()`

```
ATCA_STATUS atcab_sha_hmac_ext (
    ATCADevice device,
    const uint8_t * data,
    size_t data_size,
    uint16_t key_slot,
    uint8_t * digest,
    uint8_t target )
```

Use the SHA command to compute an HMAC/SHA-256 operation.

Parameters

in	<i>device</i>	Device context pointer
in	<i>data</i>	Message data to be hashed.
in	<i>data_size</i>	Size of data in bytes.
in	<i>key_slot</i>	Slot key id to use for the HMAC calculation
out	<i>digest</i>	Digest is returned here (32 bytes).
in	<i>target</i>	Where to save the digest internal to the device. For ATECC608, can be SHA_MODE_TARGET_TEMPKEY, SHA_MODE_TARGET_MSGDIGBUF, or SHA_MODE_TARGET_OUT_ONLY. For all other devices, SHA_MODE_TARGET_TEMPKEY is the only option.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.124    `atcab_sha_hmac_finish()`

```
ATCA_STATUS atcab_sha_hmac_finish (
    atca_hmac_sha256_ctx_t * ctx,
    uint8_t * digest,
    uint8_t target )
```

Executes SHA command to complete a HMAC/SHA-256 operation.

Parameters

in	<i>ctx</i>	HMAC/SHA-256 context
out	<i>digest</i>	HMAC/SHA-256 result is returned here (32 bytes).
in	<i>target</i>	Where to save the digest internal to the device. For ATECC608, can be SHA_MODE_TARGET_TEMPKEY, SHA_MODE_TARGET_MSGDIGBUF, or SHA_MODE_TARGET_OUT_ONLY. For all other devices, SHA_MODE_TARGET_TEMPKEY is the only option.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.125 atcab\_sha\_hmac\_init()

```
ATCA_STATUS atcab_sha_hmac_init (
    atca_hmac_sha256_ctx_t * ctx,
    uint16_t key_slot )
```

Executes SHA command to start an HMAC/SHA-256 operation.

#### Parameters

in	<i>ctx</i>	HMAC/SHA-256 context
in	<i>key_slot</i>	Slot key id to use for the HMAC calculation

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.126 atcab\_sha\_hmac\_update()

```
ATCA_STATUS atcab_sha_hmac_update (
    atca_hmac_sha256_ctx_t * ctx,
    const uint8_t * data,
    size_t data_size )
```

Executes SHA command to add an arbitrary amount of message data to a HMAC/SHA-256 operation.

#### Parameters

in	<i>ctx</i>	HMAC/SHA-256 context
in	<i>data</i>	Message data to add
in	<i>data_size</i>	Size of message data in bytes

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.127 atcab\_sha\_read\_context()

```
ATCA_STATUS atcab_sha_read_context (
    uint8_t * context,
    uint16_t * context_size )
```

Executes SHA command to read the SHA-256 context back. Only for ATECC608 with SHA-256 contexts. HMAC not supported.

Parameters

out	<i>context</i>	Context data is returned here.
in, out	<i>context_size</i>	As input, the size of the context buffer in bytes. As output, the size of the returned context data.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.128 atcab\_sha\_start()

```
ATCA_STATUS atcab_sha_start (
    void )
```

Executes SHA command to initialize SHA-256 calculation engine.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.129 atcab\_sha\_update()

```
ATCA_STATUS atcab_sha_update (
    const uint8_t * message )
```

Executes SHA command to add 64 bytes of message data to the current context.

Parameters

in	<i>message</i>	64 bytes of message data to add to add to operation.
----	----------------	--

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.130 atcab\_sha\_write\_context()

```
ATCA_STATUS atcab_sha_write_context (
    const uint8_t * context,
    uint16_t context_size )
```

Executes SHA command to write (restore) a SHA-256 context into the the device. Only supported for ATECC608 with SHA-256 contexts.

## 19.2 Basic Crypto API methods (atcab\_)

---

### Parameters

in	<i>context</i>	Context data to be restored.
in	<i>context_size</i>	Size of the context data in bytes.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.131 atcab\_sign()

```
ATCA_STATUS atcab_sign (
    uint16_t key_id,
    const uint8_t * msg,
    uint8_t * signature )
```

Executes Sign command, to sign a 32-byte external message using the private key in the specified slot. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.

### Parameters

in	<i>key_id</i>	Slot of the private key to be used to sign the message.
in	<i>msg</i>	32-byte message to be signed. Typically the SHA256 hash of the full message.
out	<i>signature</i>	Signature will be returned here. Format is R and S integers in big-endian format. 64 bytes for P256 curve.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.132 atcab\_sign\_base()

```
ATCA_STATUS atcab_sign_base (
    uint8_t mode,
    uint16_t key_id,
    uint8_t * signature )
```

Executes the Sign command, which generates a signature using the ECDSA algorithm.

### Parameters

in	<i>mode</i>	Mode determines what the source of the message to be signed.
in	<i>key_id</i>	Private key slot used to sign the message.
out	<i>signature</i>	Signature is returned here. Format is R and S integers in big-endian format. 64 bytes for P256 curve.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.133 atcab\_sign\_ext()

```
ATCA_STATUS atcab_sign_ext (
    ATCADevice device,
    uint16_t key_id,
    const uint8_t * msg,
    uint8_t * signature )
```

Executes Sign command, to sign a 32-byte external message using the private key in the specified slot. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.

Parameters

in	<i>device</i>	Device context pointer
in	<i>key_id</i>	Slot of the private key to be used to sign the message.
in	<i>msg</i>	32-byte message to be signed. Typically the SHA256 hash of the full message.
out	<i>signature</i>	Signature will be returned here. Format is R and S integers in big-endian format. 64 bytes for P256 curve.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.134 atcab\_sign\_internal()

```
ATCA_STATUS atcab_sign_internal (
    uint16_t key_id,
    bool is_invalidate,
    bool is_full_sn,
    uint8_t * signature )
```

Executes Sign command to sign an internally generated message.

Parameters

in	<i>key_id</i>	Slot of the private key to be used to sign the message.
in	<i>is_invalidate</i>	Set to true if the signature will be used with the Verify(Invalid) command. false for all other cases.
in	<i>is_full_sn</i>	Set to true if the message should incorporate the device's full serial number.
out	<i>signature</i>	Signature is returned here. Format is R and S integers in big-endian format. 64 bytes for P256 curve.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.135 atcab\_sleep()

```
ATCA_STATUS atcab_sleep (
    void )
```

invoke sleep on the CryptoAuth device

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.136 atcab\_updateextra()

```
ATCA_STATUS atcab_updateextra (
    uint8_t mode,
    uint16_t new_value )
```

Executes UpdateExtra command to update the values of the two extra bytes within the Configuration zone (bytes 84 and 85).

Can also be used to decrement the limited use counter associated with the key in slot NewValue.

### Parameters

in	<i>mode</i>	Mode determines what operations the UpdateExtra command performs.
in	<i>new_value</i>	Value to be written.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.137 atcab\_verify()

```
ATCA_STATUS atcab_verify (
    uint8_t mode,
    uint16_t key_id,
    const uint8_t * signature,
    const uint8_t * public_key,
```



```
const uint8_t * other_data,
uint8_t * mac )
```

Executes the Verify command, which takes an ECDSA [R,S] signature and verifies that it is correctly generated from a given message and public key. In all cases, the signature is an input to the command.

For the Stored, External, and ValidateExternal Modes, the contents of TempKey (or Message Digest Buffer in some cases for the ATECC608) should contain the 32 byte message.

#### Parameters

in	<i>mode</i>	Verify command mode and options
in	<i>key_id</i>	Stored mode, the slot containing the public key to be used for the verification. ValidateExternal mode, the slot containing the public key to be validated. External mode, KeyID contains the curve type to be used to Verify the signature. Validate or Invalidate mode, the slot containing the public key to be (in)validated.
in	<i>signature</i>	Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve.
in	<i>public_key</i>	If mode is External, the public key to be used for verification. X and Y integers in big-endian format. 64 bytes for P256 curve. NULL for all other modes.
in	<i>other_data</i>	If mode is Validate, the bytes used to generate the message for the validation (19 bytes). NULL for all other modes.
out	<i>mac</i>	If mode indicates a validating MAC, then the MAC will be returned here. Can be NULL otherwise.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.138 atcab\_verify\_extern()

```
ATCA_STATUS atcab_verify_extern (
    const uint8_t * message,
    const uint8_t * signature,
    const uint8_t * public_key,
    bool * is_verified )
```

Executes the Verify command, which verifies a signature (ECDSA verify operation) with all components (message, signature, and public key) supplied. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.

#### Parameters

in	<i>message</i>	32 byte message to be verified. Typically the SHA256 hash of the full message.
in	<i>signature</i>	Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve.
in	<i>public_key</i>	The public key to be used for verification. X and Y integers in big-endian format. 64 bytes for P256 curve.
out	<i>is_verified</i>	Boolean whether or not the message, signature, public key verified.

### Returns

ATCA\_SUCCESS on verification success or failure, because the command still completed successfully.

#### 19.2.2.139 atcab\_verify\_extern\_ext()

```
ATCA_STATUS atcab_verify_extern_ext (
    ATCADevice device,
    const uint8_t * message,
    const uint8_t * signature,
    const uint8_t * public_key,
    bool * is_verified )
```

Executes the Verify command, which verifies a signature (ECDSA verify operation) with all components (message, signature, and public key) supplied. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.

### Parameters

in	<i>device</i>	Device context pointer
in	<i>message</i>	32 byte message to be verified. Typically the SHA256 hash of the full message.
in	<i>signature</i>	Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve.
in	<i>public_key</i>	The public key to be used for verification. X and Y integers in big-endian format. 64 bytes for P256 curve.
out	<i>is_verified</i>	Boolean whether or not the message, signature, public key verified.

### Returns

ATCA\_SUCCESS on verification success or failure, because the command still completed successfully.

#### 19.2.2.140 atcab\_verify\_extern\_mac()

```
ATCA_STATUS atcab_verify_extern_mac (
    const uint8_t * message,
    const uint8_t * signature,
    const uint8_t * public_key,
    const uint8_t * num_in,
    const uint8_t * io_key,
    bool * is_verified )
```

Executes the Verify command with verification MAC, which verifies a signature (ECDSA verify operation) with all components (message, signature, and public key) supplied. This function is only available on the ATECC608.

### Parameters

in	<i>message</i>	32 byte message to be verified. Typically the SHA256 hash of the full message.
in	<i>signature</i>	Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve.

**Parameters**

in	<i>public_key</i>	The public key to be used for verification. X and Y integers in big-endian format. 64 bytes for P256 curve.
in	<i>num_in</i>	System nonce (32 byte) used for the verification MAC.
in	<i>io_key</i>	IO protection key for verifying the validation MAC.
out	<i>is_verified</i>	Boolean whether or not the message, signature, public key verified.

**Returns**

ATCA\_SUCCESS on verification success or failure, because the command still completed successfully.

**19.2.2.141 atcab\_verify\_invalidate()**

```
ATCA_STATUS atcab_verify_invalidate (
    uint16_t key_id,
    const uint8_t * signature,
    const uint8_t * other_data,
    bool * is_verified )
```

Executes the Verify command in Invalidate mode which invalidates a previously validated public key stored in a slot.

This command can only be run after GenKey has been used to create a PubKey digest of the public key to be invalidated in TempKey (mode=0x10).

**Parameters**

in	<i>key_id</i>	Slot containing the public key to be invalidated.
in	<i>signature</i>	Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve.
in	<i>other_data</i>	19 bytes of data used to build the verification message.
out	<i>is_verified</i>	Boolean whether or not the message, signature, validation public key verified.

**Returns**

ATCA\_SUCCESS on verification success or failure, because the command still completed successfully.

**19.2.2.142 atcab\_verify\_stored()**

```
ATCA_STATUS atcab_verify_stored (
    const uint8_t * message,
    const uint8_t * signature,
    uint16_t key_id,
    bool * is_verified )
```

Executes the Verify command, which verifies a signature (ECDSA verify operation) with a public key stored in the device. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.

## 19.2 Basic Crypto API methods (atcab\_)

### Parameters

in	<i>message</i>	32 byte message to be verified. Typically the SHA256 hash of the full message.
in	<i>signature</i>	Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve.
in	<i>key_id</i>	Slot containing the public key to be used in the verification.
out	<i>is_verified</i>	Boolean whether or not the message, signature, public key verified.

### Returns

ATCA\_SUCCESS on verification success or failure, because the command still completed successfully.

### 19.2.2.143 atcab\_verify\_stored\_ext()

```
ATCA_STATUS atcab_verify_stored_ext (
    ATCADevice device,
    const uint8_t * message,
    const uint8_t * signature,
    uint16_t key_id,
    bool * is_verified )
```

Executes the Verify command, which verifies a signature (ECDSA verify operation) with a public key stored in the device. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.

### Parameters

in	<i>device</i>	Device context pointer
in	<i>message</i>	32 byte message to be verified. Typically the SHA256 hash of the full message.
in	<i>signature</i>	Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve.
in	<i>key_id</i>	Slot containing the public key to be used in the verification.
out	<i>is_verified</i>	Boolean whether or not the message, signature, public key verified.

### Returns

ATCA\_SUCCESS on verification success or failure, because the command still completed successfully.

### 19.2.2.144 atcab\_verify\_stored\_mac()

```
ATCA_STATUS atcab_verify_stored_mac (
    const uint8_t * message,
    const uint8_t * signature,
    uint16_t key_id,
    const uint8_t * num_in,
    const uint8_t * io_key,
    bool * is_verified )
```

Executes the Verify command with verification MAC, which verifies a signature (ECDSA verify operation) with a public key stored in the device. This function is only available on the ATECC608.

Parameters

in	<i>message</i>	32 byte message to be verified. Typically the SHA256 hash of the full message.
in	<i>signature</i>	Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve.
in	<i>key_id</i>	Slot containing the public key to be used in the verification.
in	<i>num_in</i>	System nonce (32 byte) used for the verification MAC.
in	<i>io_key</i>	IO protection key for verifying the validation MAC.
out	<i>is_verified</i>	Boolean whether or not the message, signature, public key verified.

Returns

ATCA\_SUCCESS on verification success or failure, because the command still completed successfully.

19.2.2.145 atcab\_verify\_stored\_with\_tempkey()

```
ATCA_STATUS atcab_verify_stored_with_tempkey (
    const uint8_t * signature,
    uint16_t key_id,
    bool * is_verified )
```

Executes the Verify command, which verifies a signature (ECDSA verify operation) with a public key stored in the device. keyConfig.reqrandom bit should be set and the message to be signed should be already loaded into TempKey for all devices.

Please refer to TEST(atca\_cmd\_basic\_test, verify\_stored\_on\_reqrandom\_set) in atca\_tests\_verify.c for proper use of this api

Parameters

in	<i>device</i>	Device context pointer
in	<i>signature</i>	Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve.
in	<i>key_id</i>	Slot containing the public key to be used in the verification.
out	<i>is_verified</i>	Boolean whether or not the message, signature, public key verified.

Returns

ATCA\_SUCCESS on verification success or failure, because the command still completed successfully.

19.2.2.146 atcab\_verify\_validate()

```
ATCA_STATUS atcab_verify_validate (
    uint16_t key_id,
    const uint8_t * signature,
    const uint8_t * other_data,
    bool * is_verified )
```

## 19.2 Basic Crypto API methods (atcab\_)

---

Executes the Verify command in Validate mode to validate a public key stored in a slot.

This command can only be run after GenKey has been used to create a PubKey digest of the public key to be validated in TempKey (mode=0x10).

### Parameters

in	<i>key_id</i>	Slot containing the public key to be validated.
in	<i>signature</i>	Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve.
in	<i>other_data</i>	19 bytes of data used to build the verification message.
out	<i>is_verified</i>	Boolean whether or not the message, signature, validation public key verified.

### Returns

ATCA\_SUCCESS on verification success or failure, because the command still completed successfully.

### 19.2.2.147 atcab\_version()

```
ATCA_STATUS atcab_version (
    char * ver_str )
```

basic API methods are all prefixed with atcab\_ (CryptoAuthLib Basic) the fundamental premise of the basic API is it is based on a single interface instance and that instance is global, so all basic API commands assume that one global device is the one to operate on.

returns a version string for the CryptoAuthLib release. The format of the version string returned is "yyyymmdd"

### Parameters

out	<i>ver_str</i>	ptr to space to receive version string
-----	----------------	--

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.148 atcab\_wakeup()

```
ATCA_STATUS atcab_wakeup (
    void )
```

wakeup the CryptoAuth device

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.149    **atcab\_write()**

```
ATCA_STATUS atcab_write (
    uint8_t zone,
    uint16_t address,
    const uint8_t * value,
    const uint8_t * mac )
```

Executes the Write command, which writes either one four byte word or a 32-byte block to one of the EEPROM zones on the device. Depending upon the value of the WriteConfig byte for this slot, the data may be required to be encrypted by the system prior to being sent to the device. This command cannot be used to write slots configured as ECC private keys.

Parameters

in	<i>zone</i>	Zone/Param1 for the write command.
in	<i>address</i>	Address/Param2 for the write command.
in	<i>value</i>	Plain-text data to be written or cipher-text for encrypted writes. 32 or 4 bytes depending on bit 7 in the zone.
in	<i>mac</i>	MAC required for encrypted writes (32 bytes). Set to NULL if not required.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.150    **atcab\_write\_bytes\_zone()**

```
ATCA_STATUS atcab_write_bytes_zone (
    uint8_t zone,
    uint16_t slot,
    size_t offset_bytes,
    const uint8_t * data,
    size_t length )
```

Executes the Write command, which writes data into the configuration, otp, or data zones with a given byte offset and length. Offset and length must be multiples of a word (4 bytes).

Config zone must be unlocked for writes to that zone. If data zone is unlocked, only 32-byte writes are allowed to slots and OTP and the offset and length must be multiples of 32 or the write will fail.

Parameters

in	<i>zone</i>	Zone to write data to: ATCA_ZONE_CONFIG(0), ATCA_ZONE_OTP(1), or ATCA_ZONE_DATA(2).
in	<i>slot</i>	If zone is ATCA_ZONE_DATA(2), the slot number to write to. Ignored for all other zones.
in	<i>offset_bytes</i>	Byte offset within the zone to write to. Must be a multiple of a word (4 bytes).
in	<i>data</i>	Data to be written.
in	<i>length</i>	Number of bytes to be written. Must be a multiple of a word (4 bytes).

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.151 atcab\_write\_config\_counter()

```
ATCA_STATUS atcab_write_config_counter (
    uint16_t counter_id,
    uint32_t counter_value )
```

Initialize one of the monotonic counters in device with a specific value.

The monotonic counters are stored in the configuration zone using a special format. This encodes a binary count value into the 8 byte encoded value required. Can only be set while the configuration zone is unlocked.

### Parameters

in	<i>counter_id</i>	Counter to be written.
in	<i>counter_value</i>	Counter value to set.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.2.2.152 atcab\_write\_config\_zone()

```
ATCA_STATUS atcab_write_config_zone (
    const uint8_t * config_data )
```

Executes the Write command, which writes the configuration zone.

First 16 bytes are skipped as they are not writable. LockValue and LockConfig are also skipped and can only be changed via the Lock command.

This command may fail if UserExtra and/or Selector bytes have already been set to non-zero values.

### Parameters

in	<i>config_data</i>	Data to the config zone data. This should be 88 bytes for SHA devices and 128 bytes for ECC devices.
----	--------------------	--

### Returns

ATCA\_SUCCESS on success, otherwise an error code.



19.2.2.153    **atcab\_write\_config\_zone\_ext()**

```
ATCA_STATUS atcab_write_config_zone_ext (
    ATCADevice device,
    const uint8_t * config_data )
```

Executes the Write command, which writes the configuration zone.

First 16 bytes are skipped as they are not writable. LockValue and LockConfig are also skipped and can only be changed via the Lock command.

This command may fail if UserExtra and/or Selector bytes have already been set to non-zero values.

Parameters

in	<i>device</i>	Device context
in	<i>config_data</i>	Data to the config zone data. This should be 88 bytes for SHA devices and 128 bytes for ECC devices.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.2.2.154    **atcab\_write\_enc()**

```
ATCA_STATUS atcab_write_enc (
    uint16_t key_id,
    uint8_t block,
    const uint8_t * data,
    const uint8_t * enc_key,
    const uint16_t enc_key_id,
    const uint8_t num_in[ (20) ] )
```

Executes the Write command, which performs an encrypted write of a 32 byte block into given slot.

The function takes clear text bytes and encrypts them for writing over the wire. Data zone must be locked and the slot configuration must be set to encrypted write for the block to be successfully written.

Parameters

in	<i>key_id</i>	Slot ID to write to.
in	<i>block</i>	Index of the 32 byte block to write in the slot.
in	<i>data</i>	32 bytes of clear text data to be written to the slot
in	<i>enc_key</i>	WriteKey to encrypt with for writing
in	<i>enc_key_id</i>	The KeyID of the WriteKey
in	<i>num_in</i>	20 byte host nonce to inject into Nonce calculation

returns ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.155 atcab\_write\_pubkey()

```
ATCA_STATUS atcab_write_pubkey (
    uint16_t slot,
    const uint8_t * public_key )
```

Uses the write command to write a public key to a slot in the proper format.

#### Parameters

in	<i>slot</i>	Slot number to write. Only slots 8 to 15 are large enough to store a public key.
in	<i>public_key</i>	Public key to write into the slot specified. X and Y integers in big-endian format. 64 bytes for P256 curve.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.156 atcab\_write\_pubkey\_ext()

```
ATCA_STATUS atcab_write_pubkey_ext (
    ATCADevice device,
    uint16_t slot,
    const uint8_t * public_key )
```

Uses the write command to write a public key to a slot in the proper format.

#### Parameters

in	<i>device</i>	Device context
in	<i>slot</i>	Slot number to write. Only slots 8 to 15 are large enough to store a public key.
in	<i>public_key</i>	Public key to write into the slot specified. X and Y integers in big-endian format. 64 bytes for P256 curve.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.157 atcab\_write\_zone()

```
ATCA_STATUS atcab_write_zone (
    uint8_t zone,
    uint16_t slot,
    uint8_t block,
    uint8_t offset,
```

```
const uint8_t * data,  
uint8_t len )
```

Executes the Write command, which writes either 4 or 32 bytes of data into a device zone.

## 19.2 Basic Crypto API methods (atcab\_)

### Parameters

in	<i>zone</i>	Device zone to write to (0=config, 1=OTP, 2=data).
in	<i>slot</i>	If writing to the data zone, it is the slot to write to, otherwise it should be 0.
in	<i>block</i>	32-byte block to write to.
in	<i>offset</i>	4-byte word within the specified block to write to. If performing a 32-byte write, this should be 0.
in	<i>data</i>	Data to be written.
in	<i>len</i>	Number of bytes to be written. Must be either 4 or 32.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.158 atcab\_write\_zone\_ext()

```
ATCA_STATUS atcab_write_zone_ext (
    ATCADevice device,
    uint8_t zone,
    uint16_t slot,
    uint8_t block,
    uint8_t offset,
    const uint8_t * data,
    uint8_t len )
```

Executes the Write command, which writes either 4 or 32 bytes of data into a device zone.

### Parameters

in	<i>device</i>	Device context
in	<i>zone</i>	Device zone to write to (0=config, 1=OTP, 2=data).
in	<i>slot</i>	If writing to the data zone, it is the slot to write to, otherwise it should be 0.
in	<i>block</i>	32-byte block to write to.
in	<i>offset</i>	4-byte word within the specified block to write to. If performing a 32-byte write, this should be 0.
in	<i>data</i>	Data to be written.
in	<i>len</i>	Number of bytes to be written. Must be either 4 or 32.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.2.2.159 isAlpha()

```
bool isAlpha (
    char c )
```

Checks to see if a character is an ASCII representation of hex ((c >= 'A') and (c <= 'F')) || ((c >= 'a') and (c <= 'f'))

Parameters

in	<i>c</i>	character to check
----	----------	--------------------

Returns

True if the character is a hex

19.2.2.160 isBase64()

```
bool isBase64 (
    char c,
    const uint8_t * rules )
```

Returns true if this character is a valid base 64 character or if this is space (A character can be included in a valid base 64 string).

Parameters

in	<i>c</i>	character to check
in	<i>rules</i>	base64 ruleset to use

Returns

True if the character can be included in a valid base 64 string

19.2.2.161 isBase64Digit()

```
bool isBase64Digit (
    char c,
    const uint8_t * rules )
```

Returns true if this character is a valid base 64 character.

Parameters

in	<i>c</i>	character to check
in	<i>rules</i>	base64 ruleset to use

Returns

True if the character can be included in a valid base 64 string

### 19.2.2.162 isBlankSpace()

```
bool isBlankSpace (
    char c )
```

Checks to see if a character is blank space.

#### Parameters

in	c	character to check
----	---	--------------------

#### Returns

True if the character is blankspace

### 19.2.2.163 isDigit()

```
bool isDigit (
    char c )
```

Checks to see if a character is an ASCII representation of a digit ((c ge '0') and (c le '9'))

#### Parameters

in	c	character to check
----	---	--------------------

#### Returns

True if the character is a digit

### 19.2.2.164 isHex()

```
bool isHex (
    char c )
```

Returns true if this character is a valid hex character or if this is blankspace (The character can be included in a valid hexstring).

#### Parameters

in	c	character to check
----	---	--------------------

Returns

True if the character can be included in a valid hexstring

19.2.2.165 isHexAlpha()

```
bool isHexAlpha (
    char c )
```

Checks to see if a character is an ASCII representation of hex ((c >= 'A') and (c <= 'F')) || ((c >= 'a') and (c <= 'f'))

Parameters

in	c	character to check
----	---	--------------------

Returns

True if the character is a hex

19.2.2.166 isHexDigit()

```
bool isHexDigit (
    char c )
```

Returns true if this character is a valid hex character.

Parameters

in	c	character to check
----	---	--------------------

Returns

True if the character can be included in a valid hexstring

19.2.2.167 packHex()

```
ATCA_STATUS packHex (
    const char * ascii_hex,
    size_t ascii_hex_len,
    char * packed_hex,
    size_t * packed_len )
```

Remove spaces from a ASCII hex string.

## 19.3 Configuration (cfg\_)

---

### Parameters

in	<i>ascii_hex</i>	Initial hex string to remove blankspace from
in	<i>ascii_hex_len</i>	Length of the initial hex string
in	<i>packed_hex</i>	Resulting hex string without blankspace
in, out	<i>packed_len</i>	In: Size to packed_hex buffer Out: Number of bytes in the packed hex string

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

## 19.3 Configuration (cfg\_)

Logical device configurations describe the CryptoAuth device type and logical interface.

Logical device configurations describe the CryptoAuth device type and logical interface.

## 19.4 ATCADevice (atca\_)

ATCADevice object - composite of command and interface objects.

### Data Structures

- struct [atca\\_device](#)  
*atca\_device* is the C object backing ATCADevice. See the [atca\\_device.h](#) file for details on the ATCADevice methods

### Macros

- #define **ATSHA204A** (0U)  
*The supported Device type in Cryptoauthlib library.*
- #define **ATECC108A** (1U)
- #define **ATECC508A** (2U)
- #define **ATECC608A** (3U)
- #define **ATECC608B** (3U)
- #define **ATECC608** (3U)
- #define **ATSHA206A** (4U)
- #define **TA100** (0x10U)
- #define **TA101** (0x11U)
- #define **ECC204** (0x20U)
- #define **TA010** (0x21U)
- #define **ECC206** (0x22U)
- #define **RNG90** (0x23U)
- #define **SHA104** (0x24U)
- #define **SHA105** (0x25U)
- #define **SHA106** (0x26U)
- #define **ATCA\_DEV\_UNKNOWN** (0x7EU)
- #define **ATCA\_DEV\_INVALID** (0x7FU)



## Typedefs

- typedef void(\* **ctx\_cb**) (void \*ctx)  
*Callback function to clean up the session context.*
- typedef struct **atca\_device** \* **ATCADevice**
- typedef uint8\_t **ATCADeviceType**

## Enumerations

- enum **ATCADeviceState** { **ATCA\_DEVICE\_STATE\_UNKNOWN** = 0 , **ATCA\_DEVICE\_STATE\_SLEEP** , **ATCA\_DEVICE\_STATE\_IDLE** , **ATCA\_DEVICE\_STATE\_ACTIVE** }  
*ATCADeviceState says about device state.*

## Functions

- **ATCADevice** **newATCADevice** (**ATCAIfaceCfg** \*cfg)  
*constructor for a Microchip CryptoAuth device*
- void **deleteATCADevice** (**ATCADevice** \*ca\_dev)  
*destructor for a device NULLs reference after object is freed*
- **ATCA\_STATUS** **initATCADevice** (**ATCAIfaceCfg** \*cfg, **ATCADevice** ca\_dev)  
*Initializer for an Microchip CryptoAuth device.*
- **ATCAIface** **atGetIFace** (**ATCADevice** dev)  
*returns a reference to the ATCAIface interface object for the device*
- **ATCA\_STATUS** **releaseATCADevice** (**ATCADevice** ca\_dev)  
*Release any resources associated with the device.*

### 19.4.1 Detailed Description

ATCADevice object - composite of command and interface objects.

### 19.4.2 Function Documentation

#### 19.4.2.1 atGetIFace()

```
ATCAIface atGetIFace (
    ATCADevice dev )
```

returns a reference to the ATCAIface interface object for the device

#### Parameters

in	dev	reference to a device
----	-----	-----------------------

## 19.4 ATCADevice (atca\_)

---

### Returns

reference to the ATCAIface object for the device

### 19.4.2.2 deleteATCADevice()

```
void deleteATCADevice (
    ATCADevice * ca_dev )
```

destructor for a device NULLs reference after object is freed

### Parameters

in	ca_dev	pointer to a reference to a device
----	--------	------------------------------------

### 19.4.2.3 initATCADevice()

```
ATCA_STATUS initATCADevice (
    ATCAIfaceCfg * cfg,
    ATCADevice ca_dev )
```

Initializer for an Microchip CryptoAuth device.

### Parameters

in	cfg	pointer to an interface configuration object
in, out	ca_dev	As input, pre-allocated structure to be initialized. mCommands and mIface members should point to existing structures to be initialized.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.4.2.4 newATCADevice()

```
ATCADevice newATCADevice (
    ATCAIfaceCfg * cfg )
```

constructor for a Microchip CryptoAuth device

### Parameters

in	cfg	Interface configuration object
----	-----	--------------------------------

**Returns**

Reference to a new ATCADevice on success. NULL on failure.

**19.4.2.5 releaseATCADevice()**

```
ATCA_STATUS releaseATCADevice (
    ATCADevice ca_dev )
```

Release any resources associated with the device.

**Parameters**

in	ca_dev	Device to release
----	--------	-------------------

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

**19.5 ATCAIface (atca\_)**

Abstract interface to all CryptoAuth device types. This interface connects to the HAL implementation and abstracts the physical details of the device communication from all the upper layers of CryptoAuthLib.

**Data Structures**

- struct [devtype\\_names\\_t](#)
- struct [ATCAIfaceCfg](#)
- struct [ATCAHAL\\_t](#)  
*HAL Driver Structure.*
- struct [atca\\_iface](#)  
*atca\_iface is the context structure for a configured interface*

**Macros**

- #define **ATCA\_IFACECFG\_NAME**(x) (x)
- #define **ATCA\_IFACECFG\_I2C\_ADDRESS**(c) (c)->cfg.atcai2c.address
- #define **ATCA\_IFACECFG\_I2C\_BAUD**(c) (c)->cfg.atcai2c.baud
- #define **ATCA\_IFACECFG\_VALUE**(c, v) (c)->cfg.v

**Typedefs**

- typedef struct [atca\\_iface](#) \* **ATCAIface**
- typedef struct [atca\\_iface](#) **atca\_iface\_t**  
*atca\_iface is the context structure for a configured interface*

## Enumerations

- enum [ATCAIfaceType](#) {  
[ATCA\\_I2C\\_IFACE](#) = 0 , [ATCA\\_SWI\\_IFACE](#) = 1 , [ATCA\\_UART\\_IFACE](#) = 2 , [ATCA\\_SPI\\_IFACE](#) = 3 ,  
[ATCA\\_HID\\_IFACE](#) = 4 , [ATCA\\_KIT\\_IFACE](#) = 5 , [ATCA\\_CUSTOM\\_IFACE](#) = 6 , [ATCA\\_I2C\\_GPIO\\_IFACE](#) = 7 ,  
[ATCA\\_SWI\\_GPIO\\_IFACE](#) = 8 , [ATCA\\_SPI\\_GPIO\\_IFACE](#) = 9 , [ATCA\\_UNKNOWN\\_IFACE](#) = 0xFE }
- enum [ATCAKitType](#) {  
[ATCA\\_KIT\\_AUTO\\_IFACE](#) , [ATCA\\_KIT\\_I2C\\_IFACE](#) , [ATCA\\_KIT\\_SWI\\_IFACE](#) , [ATCA\\_KIT\\_SPI\\_IFACE](#) ,  
[ATCA\\_KIT\\_UNKNOWN\\_IFACE](#) }

## Functions

- ATCA\_STATUS [initATCAIface](#) ([ATCAIfaceCfg](#) \*cfg, [ATCAIface](#) ca\_iface)  
*Initializer for ATCAIface objects.*
- ATCA\_STATUS [atinit](#) ([ATCAIface](#) ca\_iface)  
*Performs the HAL initialization by calling intermediate HAL wrapper function. If using the basic API, the [atcab\\_init\(\)](#) function should be called instead.*
- ATCA\_STATUS [atsend](#) ([ATCAIface](#) ca\_iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*Sends the data to the device by calling intermediate HAL wrapper function.*
- ATCA\_STATUS [atreceive](#) ([ATCAIface](#) ca\_iface, uint8\_t word\_address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*Receives data from the device by calling intermediate HAL wrapper function.*
- ATCA\_STATUS [atcontrol](#) ([ATCAIface](#) ca\_iface, uint8\_t option, void \*param, size\_t paramlen)  
*Perform control operations with the underlying hal driver.*
- ATCA\_STATUS [atwake](#) ([ATCAIface](#) ca\_iface)  
*Wakes up the device by calling intermediate HAL wrapper function. The [atcab\\_wakeup\(\)](#) function should be used instead.*
- ATCA\_STATUS [atidle](#) ([ATCAIface](#) ca\_iface)  
*Puts the device into idle state by calling intermediate HAL wrapper function. The [atcab\\_idle\(\)](#) function should be used instead.*
- ATCA\_STATUS [atsleep](#) ([ATCAIface](#) ca\_iface)  
*Puts the device into sleep state by calling intermediate HAL wrapper function. The [atcab\\_sleep\(\)](#) function should be used instead.*
- [ATCAIfaceCfg](#) \* [atgetifacecfg](#) ([ATCAIface](#) ca\_iface)  
*Returns the logical interface configuration for the device.*
- void \* [atgetifacehaldat](#) ([ATCAIface](#) ca\_iface)  
*Returns the HAL data pointer for the device.*
- bool [iface\\_type\\_is\\_kit](#) ([ATCAIfaceType](#) iface\_type)  
*Check if the given interface is a "kit protocol" one.*
- bool [atca\\_iface\\_is\\_kit](#) ([ATCAIface](#) ca\_iface)  
*Check if the given interface is configured as a "kit protocol" one where transactions are atomic.*
- bool [atca\\_iface\\_is\\_swi](#) ([ATCAIface](#) ca\_iface)  
*Check if the given interface is configured as a SWI.*
- int [atca\\_iface\\_get\\_retries](#) ([ATCAIface](#) ca\_iface)  
*Retrive the number of retries for a configured interface.*
- uint16\_t [atca\\_iface\\_get\\_wake\\_delay](#) ([ATCAIface](#) ca\_iface)  
*Retrive the wake/retry delay for a configured interface/device.*
- uint8\_t [ifacecfg\\_get\\_address](#) ([ATCAIfaceCfg](#) \*cfg)  
*Retrieves the device address given an interface configuration.*
- ATCA\_STATUS [ifacecfg\\_set\\_address](#) ([ATCAIfaceCfg](#) \*cfg, uint8\_t address, [ATCAKitType](#) kitiface)  
*Change the address of the selected device.*
- ATCA\_STATUS [releaseATCAIface](#) ([ATCAIface](#) ca\_iface)  
*Instruct the HAL driver to release any resources associated with this interface.*
- void [deleteATCAIface](#) ([ATCAIface](#) \*ca\_iface)  
*Instruct the HAL driver to release any resources associated with this interface, then delete the object.*
- [ATCADeviceType](#) [iface\\_get\\_device\\_type\\_by\\_name](#) (const char \*name)  
*Get the ATCADeviceType for a string that looks like a part number.*

19.5.1 Detailed Description

Abstract interface to all CryptoAuth device types. This interface connects to the HAL implementation and abstracts the physical details of the device communication from all the upper layers of CryptoAuthLib.

19.5.2 Enumeration Type Documentation

19.5.2.1 ATCAIfaceType

enum ATCAIfaceType

Enumerator

ATCA_I2C_IFACE	Native I2C Driver
ATCA_SWI_IFACE	SWI or 1-Wire over UART/USART
ATCA_UART_IFACE	Kit v1 over UART/USART
ATCA_SPI_IFACE	Native SPI Driver
ATCA_HID_IFACE	Kit v1 over HID
ATCA_KIT_IFACE	Kit v2 (Binary/Bridging)
ATCA_CUSTOM_IFACE	Custom HAL functions provided during interface init
ATCA_I2C_GPIO_IFACE	I2C "Bitbang" Driver
ATCA_SWI_GPIO_IFACE	SWI or 1-Wire using a GPIO
ATCA_SPI_GPIO_IFACE	SWI or 1-Wire using a GPIO

19.5.3 Function Documentation

19.5.3.1 atca\_iface\_is\_kit()

```
bool atca_iface_is_kit (
    ATCAIface ca_iface )
```

Check if the given interface is configured as a "kit protocol" one where transactions are atomic.

Returns

true if the interface is considered a kit

## 19.5 ATCAIface (atca\_)

---

### 19.5.3.2 atca\_iface\_is\_swi()

```
bool atca_iface_is_swi (
    ATCAIface ca_iface )
```

Check if the given interface is configured as a SWI.

#### Returns

true if the interface is considered a kit

### 19.5.3.3 atcontrol()

```
ATCA_STATUS atcontrol (
    ATCAIface ca_iface,
    uint8_t option,
    void * param,
    size_t paramlen )
```

Perform control operations with the underlying hal driver.

#### Parameters

in	<i>ca_iface</i>	Device to interact with.
in	<i>option</i>	Control parameter identifier
in	<i>param</i>	Optional pointer to parameter value
in	<i>paramlen</i>	Length of the parameter

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.5.3.4 atgetifacecfg()

```
ATCAIfaceCfg * atgetifacecfg (
    ATCAIface ca_iface )
```

Returns the logical interface configuration for the device.

#### Parameters

in	<i>ca_iface</i>	Device interface.
----	-----------------	-------------------

Returns

Logical interface configuration.

19.5.3.5 atgetifacehaldat()

```
void * atgetifacehaldat (
    ATCAIface ca_iface )
```

Returns the HAL data pointer for the device.

Parameters

in	ca_iface	Device interface.
----	----------	-------------------

Returns

HAL data pointer.

19.5.3.6 atidle()

```
ATCA_STATUS atidle (
    ATCAIface ca_iface )
```

Puts the device into idle state by calling intermediate HAL wrapper function. The [atcab\\_idle\(\)](#) function should be used instead.

**Deprecated** This function does not have defined behavior when ATCA\_HAL\_LEGACY\_API is undefined.

Parameters

in	ca_iface	Device to interact with.
----	----------	--------------------------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.5.3.7 atinit()

```
ATCA_STATUS atinit (
    ATCAIface ca_iface )
```

Performs the HAL initialization by calling intermediate HAL wrapper function. If using the basic API, the [atcab\\_init\(\)](#) function should be called instead.

## 19.5 ATCAIface (atca\_)

---

### Parameters

in	<i>ca_iface</i>	Device to interact with.
----	-----------------	--------------------------

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.5.3.8 atreceive()

```
ATCA_STATUS atreceive (
    ATCAIface ca_iface,
    uint8_t word_address,
    uint8_t * rxdata,
    uint16_t * rxlength )
```

Receives data from the device by calling intermediate HAL wrapper function.

### Parameters

in	<i>ca_iface</i>	Device to interact with.
in	<i>word_address</i>	device transaction type
out	<i>rxdata</i>	Data received will be returned here.
in, out	<i>rxlength</i>	As input, the size of the rxdata buffer. As output, the number of bytes received.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.5.3.9 atsend()

```
ATCA_STATUS atsend (
    ATCAIface ca_iface,
    uint8_t word_address,
    uint8_t * txdata,
    int txlength )
```

Sends the data to the device by calling intermediate HAL wrapper function.

### Parameters

in	<i>ca_iface</i>	Device to interact with.
in	<i>word_address</i>	device transaction type
in	<i>txdata</i>	Data to be transmitted to the device.
in	<i>txlength</i>	Number of bytes to be transmitted to the device.



Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.5.3.10 `atsleep()`

```
ATCA_STATUS atsleep (
    ATCAIface ca_iface )
```

Puts the device into sleep state by calling intermediate HAL wrapper function. The `atcab_sleep()` function should be used instead.

**Deprecated** This function does not have defined behavior when ATCA\_HAL\_LEGACY\_API is undefined.

Parameters

in	<i>ca_iface</i>	Device to interact with.
----	-----------------	--------------------------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.5.3.11 `atwake()`

```
ATCA_STATUS atwake (
    ATCAIface ca_iface )
```

Wakes up the device by calling intermediate HAL wrapper function. The `atcab_wakeup()` function should be used instead.

**Deprecated** This function does not have defined behavior when ATCA\_HAL\_LEGACY\_API is undefined.

Parameters

in	<i>ca_iface</i>	Device to interact with.
----	-----------------	--------------------------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.5.3.12 deleteATCAIface()

```
void deleteATCAIface (
    ATCAIface * ca_iface )
```

Instruct the HAL driver to release any resources associated with this interface, then delete the object.

#### Parameters

in	<i>ca_iface</i>	Device interface.
----	-----------------	-------------------

### 19.5.3.13 ifacecfg\_set\_address()

```
ATCA_STATUS ifacecfg_set_address (
    ATCAIfaceCfg * cfg,
    uint8_t address,
    ATCAKitType kitiface )
```

Change the address of the selected device.

#### Parameters

in	<i>cfg</i>	Interface configuration structure to update
in	<i>address</i>	Desired address
in	<i>kitiface</i>	Optional parameter to set the kit iface type

### 19.5.3.14 ifacetype\_is\_kit()

```
bool ifacetype_is_kit (
    ATCAIfaceType iface_type )
```

Check if the given interface is a "kit protocol" one.

#### Returns

true if the interface type is considered a kit

### 19.5.3.15 initATCAIface()

```
ATCA_STATUS initATCAIface (
    ATCAIfaceCfg * cfg,
    ATCAIface ca_iface )
```

Initializer for ATCAIface objects.

Parameters

in	<i>cfg</i>	Logical configuration for the interface
in	<i>ca_iface</i>	Interface structure to initialize.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.5.3.16 releaseATCAIface()

```
ATCA_STATUS releaseATCAIface (  
    ATCAIface ca_iface )
```

Instruct the HAL driver to release any resources associated with this interface.

Parameters

in	<i>ca_iface</i>	Device interface.
----	-----------------	-------------------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.6 Certificate manipulation methods (atcacert\_)

These methods provide convenient ways to perform certification I/O with CryptoAuth chips and perform certificate manipulation in memory.

Data Structures

- struct [atcacert\\_tm\\_utc\\_s](#)
- struct [atcacert\\_device\\_loc\\_s](#)
- struct [atcacert\\_cert\\_loc\\_s](#)
- struct [atcacert\\_cert\\_element\\_s](#)
- struct [atcacert\\_def\\_s](#)
- struct [atcacert\\_build\\_state\\_s](#)

Macros

- #define **FALSE** (0)
- #define **TRUE** (1)
- #define [ATCACERT\\_E\\_SUCCESS](#) ATCA\_SUCCESS
- #define [ATCACERT\\_E\\_ERROR](#) ATCA\_GEN\_FAIL
- #define [ATCACERT\\_E\\_BAD\\_PARAMS](#) ATCA\_BAD\_PARAM

- #define `ATCACERT_E_BUFFER_TOO_SMALL` `ATCA_SMALL_BUFFER`
- #define `ATCACERT_E_UNIMPLEMENTED` `ATCA_UNIMPLEMENTED`
- #define `ATCACERT_E_DECODING_ERROR` 4
- #define `ATCACERT_E_INVALID_DATE` 5
- #define `ATCACERT_E_UNEXPECTED_ELEM_SIZE` 7
- #define `ATCACERT_E_ELEM_MISSING` 8
- #define `ATCACERT_E_ELEM_OUT_OF_BOUNDS` 9
- #define `ATCACERT_E_BAD_CERT` 10
- #define `ATCACERT_E_WRONG_CERT_DEF` 11
- #define `ATCACERT_E_VERIFY_FAILED` 12
- #define `ATCACERT_E_INVALID_TRANSFORM` 13
- #define `DATEFMT_ISO8601_SEP` (0U)  
*ISO8601 full date YYYY-MM-DDThh:mm:ssZ.*
- #define `DATEFMT_RFC5280.UTC` (1U)  
*RFC 5280 (X.509) 4.1.2.5.1 UTCTime format YYMMDDhhmmssZ.*
- #define `DATEFMT_POSIX_UINT32_BE` (2U)  
*POSIX (aka UNIX) date format. Seconds since Jan 1, 1970. 32 bit unsigned integer, big endian.*
- #define `DATEFMT_POSIX_UINT32_LE` (3U)  
*POSIX (aka UNIX) date format. Seconds since Jan 1, 1970. 32 bit unsigned integer, little endian.*
- #define `DATEFMT_RFC5280_GEN` (4U)  
*RFC 5280 (X.509) 4.1.2.5.2 GeneralizedTime format YYYYMMDDhhmmssZ.*
- #define `DATEFMT_INVALID` (0xFFU)
- #define `DATEFMT_ISO8601_SEP_SIZE` (20)
- #define `DATEFMT_RFC5280.UTC_SIZE` (13)
- #define `DATEFMT_POSIX_UINT32_BE_SIZE` (4)
- #define `DATEFMT_POSIX_UINT32_LE_SIZE` (4)
- #define `DATEFMT_RFC5280_GEN_SIZE` (15)
- #define `DATEFMT_MAX_SIZE` `DATEFMT_ISO8601_SEP_SIZE`
- #define `ATCACERT_DATE_FORMAT_SIZES_COUNT` 5
- #define `ATCACERT_COMP_CERT_MAX_SIZE` 72u
- #define `atcacert_date_enc_posix_uint32_be` `atcacert_date_enc_posix_be`
- #define `atcacert_date_dec_posix_uint32_be` `atcacert_date_dec_posix_be`
- #define `atcacert_date_enc_posix_uint32_le` `atcacert_date_enc_posix_le`
- #define `atcacert_date_dec_posix_uint32_le` `atcacert_date_dec_posix_le`

## Typedefs

- typedef struct `atcacert_tm_utc_s` `atcacert_tm_utc_t`
- typedef uint8\_t `atcacert_date_format_t`
- typedef enum `atcacert_cert_type_e` `atcacert_cert_type_t`
- typedef enum `atcacert_cert_sn_src_e` `atcacert_cert_sn_src_t`
- typedef enum `atcacert_device_zone_e` `atcacert_device_zone_t`
- typedef enum `atcacert_transform_e` `atcacert_transform_t`  
*How to transform the data from the device to the certificate.*
- typedef enum `atcacert_std_cert_element_e` `atcacert_std_cert_element_t`
- typedef struct `ATCA_PACKED atcacert_device_loc_s` `atcacert_device_loc_t`
- typedef struct `ATCA_PACKED atcacert_cert_loc_s` `atcacert_cert_loc_t`
- typedef struct `ATCA_PACKED atcacert_cert_element_s` `atcacert_cert_element_t`
- typedef struct `atcacert_def_s` `atcacert_def_t`
- typedef struct `atcacert_build_state_s` `atcacert_build_state_t`

## Enumerations

- enum `atcacert_cert_type_e` { `CERTTYPE_X509`, `CERTTYPE_CUSTOM`, `CERTTYPE_X509_FULL_STORED` }
  - enum `atcacert_cert_sn_src_e` {  
`SNSRC_STORED` = 0x0 , `SNSRC_STORED_DYNAMIC` = 0x7 , `SNSRC_DEVICE_SN` = 0x8 ,  
`SNSRC_SIGNER_ID` = 0x9 ,  
`SNSRC_PUB_KEY_HASH` = 0xA , `SNSRC_DEVICE_SN_HASH` = 0xB , `SNSRC_PUB_KEY_HASH_POS`  
= 0xC , `SNSRC_DEVICE_SN_HASH_POS` = 0xD ,  
`SNSRC_PUB_KEY_HASH_RAW` = 0xE , `SNSRC_DEVICE_SN_HASH_RAW` = 0xF }
  - enum `atcacert_device_zone_e` {  
`DEVZONE_CONFIG` = 0x00 , `DEVZONE_OTP` = 0x01 , `DEVZONE_DATA` = 0x02 , `DEVZONE_GENKEY` =  
0x03 ,  
`DEVZONE_NONE` = 0x07 }
  - enum `atcacert_transform_e` {  
`TF_NONE` , `TF_REVERSE` , `TF_BIN2HEX_UC` , `TF_BIN2HEX_LC` ,  
`TF_HEX2BIN_UC` , `TF_HEX2BIN_LC` , `TF_BIN2HEX_SPACE_UC` , `TF_BIN2HEX_SPACE_LC` ,  
`TF_HEX2BIN_SPACE_UC` , `TF_HEX2BIN_SPACE_LC` }
- How to transform the data from the device to the certificate.*
- enum `atcacert_std_cert_element_e` {  
`STDCERT_PUBLIC_KEY` , `STDCERT_SIGNATURE` , `STDCERT_ISSUE_DATE` , `STDCERT_EXPIRE_↵`  
`DATE` ,  
`STDCERT_SIGNER_ID` , `STDCERT_CERT_SN` , `STDCERT_AUTH_KEY_ID` , `STDCERT_SUBJ_KEY_ID` ,  
`STDCERT_NUM_ELEMENTS` }

## Functions

- ATCA\_STATUS `atcacert_read_device_loc` (const `atcacert_device_loc_t` \*device\_loc, uint8\_t \*data)  
*Read the data from a device location.*
- ATCA\_STATUS `atcacert_read_device_loc_ext` (ATCADevice device, const `atcacert_device_loc_t` \*device\_↵  
loc, uint8\_t \*data)  
*Read the data from a device location.*
- ATCA\_STATUS `atcacert_read_cert` (const `atcacert_def_t` \*cert\_def, const uint8\_t ca\_public\_key[64], uint8\_↵  
\_t \*cert, size\_t \*cert\_size)  
*Reads the certificate specified by the certificate definition from the ATECC508A device.*
- ATCA\_STATUS `atcacert_read_cert_ext` (ATCADevice device, const `atcacert_def_t` \*cert\_def, const uint8\_t  
ca\_public\_key[64], uint8\_t \*cert, size\_t \*cert\_size)  
*Reads the certificate specified by the certificate definition from the ATECC508A device.*
- ATCA\_STATUS `atcacert_write_cert` (const `atcacert_def_t` \*cert\_def, const uint8\_t \*cert, size\_t cert\_size)  
*Take a full certificate and write it to the ATECC508A device according to the certificate definition.*
- ATCA\_STATUS `atcacert_write_cert_ext` (ATCADevice device, const `atcacert_def_t` \*cert\_def, const uint8\_t  
\*cert, size\_t cert\_size)  
*Take a full certificate and write it to the ATECC508A device according to the certificate definition.*
- ATCA\_STATUS `atcacert_create_csr` (const `atcacert_def_t` \*csr\_def, uint8\_t \*csr, size\_t \*csr\_size)  
*Creates a CSR specified by the CSR definition from the ATECC508A device. This process involves reading the  
dynamic CSR data from the device and combining it with the template found in the CSR definition, then signing it.  
Return the CSR int der format.*
- ATCA\_STATUS `atcacert_create_csr_pem` (const `atcacert_def_t` \*csr\_def, char \*csr, size\_t \*csr\_size)  
*Creates a CSR specified by the CSR definition from the ATECC508A device. This process involves reading the  
dynamic CSR data from the device and combining it with the template found in the CSR definition, then signing it.  
Return the CSR int der format.*
- ATCA\_STATUS `atcacert_get_response` (uint8\_t device\_private\_key\_slot, const uint8\_t challenge[32], uint8\_↵  
\_t response[64])  
*Calculates the response to a challenge sent from the host.*

- ATCA\_STATUS [atcacert\\_read\\_subj\\_key\\_id](#) (const [atcacert\\_def\\_t](#) \*cert\_def, uint8\_t subj\_key\_id[20])  
*Reads the subject key ID based on a certificate definition.*
- ATCA\_STATUS [atcacert\\_read\\_subj\\_key\\_id\\_ext](#) (ATCADevice device, const [atcacert\\_def\\_t](#) \*cert\_def, uint8\_t subj\_key\_id[20])  
*Reads the subject key ID based on a certificate definition.*
- ATCA\_STATUS [atcacert\\_read\\_cert\\_size](#) (const [atcacert\\_def\\_t](#) \*cert\_def, size\_t \*cert\_size)  
*Return the actual certificate size in bytes for a given cert def. Certificate can be variable size, so this gives the absolute buffer size when reading the certificates.*
- ATCA\_STATUS [atcacert\\_read\\_cert\\_size\\_ext](#) (ATCADevice device, const [atcacert\\_def\\_t](#) \*cert\_def, size\_t \*cert\_size)  
*Return the actual certificate size in bytes for a given cert def. Certificate can be variable size, so this gives the absolute buffer size when reading the certificates.*
- ATCA\_STATUS [atcacert\\_date\\_enc](#) (atcacert\_date\_format\_t format, const [atcacert\\_tm\\_utc\\_t](#) \*timestamp, uint8\_t \*formatted\_date, size\_t \*formatted\_date\_size)  
*Format a timestamp according to the format type.*
- ATCA\_STATUS [atcacert\\_date\\_dec](#) (atcacert\_date\_format\_t format, const uint8\_t \*formatted\_date, size\_t formatted\_date\_size, [atcacert\\_tm\\_utc\\_t](#) \*timestamp)  
*Parse a formatted timestamp according to the specified format.*
- ATCA\_STATUS [atcacert\\_date\\_enc\\_compcert](#) (const [atcacert\\_tm\\_utc\\_t](#) \*issue\_date, uint8\_t expire\_years, uint8\_t enc\_dates[3])  
*Encode the issue and expire dates in the format used by the compressed certificate.*
- ATCA\_STATUS [atcacert\\_date\\_enc\\_compcert\\_ext](#) (const [atcacert\\_tm\\_utc\\_t](#) \*issue\_date, uint8\_t expire\_years, uint8\_t comp\_cert[72u])  
*Encode the issue and expire dates in the format used by the compressed certificate.*
- ATCA\_STATUS [atcacert\\_date\\_dec\\_compcert](#) (const uint8\_t enc\_dates[3], atcacert\_date\_format\_t expire\_date\_format, [atcacert\\_tm\\_utc\\_t](#) \*issue\_date, [atcacert\\_tm\\_utc\\_t](#) \*expire\_date)  
*Decode the issue and expire dates from the format used by the compressed certificate.*
- ATCA\_STATUS [atcacert\\_date\\_dec\\_compcert\\_ext](#) (const uint8\_t comp\_cert[72u], atcacert\_date\_format\_t expire\_date\_format, [atcacert\\_tm\\_utc\\_t](#) \*issue\_date, [atcacert\\_tm\\_utc\\_t](#) \*expire\_date)  
*Decode the issue and expire dates from the format used by the compressed certificate.*
- atcacert\_date\_format\_t [atcacert\\_date\\_from\\_asn1\\_tag](#) (const uint8\_t tag)  
*Convert the asn1 tag for the supported time formats into the local time format.*
- ATCA\_STATUS [atcacert\\_date\\_get\\_max\\_date](#) (atcacert\_date\_format\_t format, [atcacert\\_tm\\_utc\\_t](#) \*timestamp)  
*Return the maximum date available for the given format.*
- ATCA\_STATUS [atcacert\\_date\\_enc\\_iso8601\\_sep](#) (const [atcacert\\_tm\\_utc\\_t](#) \*timestamp, uint8\_t formatted\_date[(20)])
- ATCA\_STATUS [atcacert\\_date\\_dec\\_iso8601\\_sep](#) (const uint8\_t formatted\_date[(20)], [atcacert\\_tm\\_utc\\_t](#) \*timestamp)
- ATCA\_STATUS [atcacert\\_date\\_enc\\_rfc5280\\_utc](#) (const [atcacert\\_tm\\_utc\\_t](#) \*timestamp, uint8\_t formatted\_date[(13)])
- ATCA\_STATUS [atcacert\\_date\\_dec\\_rfc5280\\_utc](#) (const uint8\_t formatted\_date[(13)], [atcacert\\_tm\\_utc\\_t](#) \*timestamp)
- ATCA\_STATUS [atcacert\\_date\\_enc\\_rfc5280\\_gen](#) (const [atcacert\\_tm\\_utc\\_t](#) \*timestamp, uint8\_t formatted\_date[(15)])
- ATCA\_STATUS [atcacert\\_date\\_dec\\_rfc5280\\_gen](#) (const uint8\_t formatted\_date[(15)], [atcacert\\_tm\\_utc\\_t](#) \*timestamp)
- ATCA\_STATUS [atcacert\\_date\\_enc\\_posix\\_be](#) (const [atcacert\\_tm\\_utc\\_t](#) \*timestamp, uint8\_t formatted\_date[(4)])
- ATCA\_STATUS [atcacert\\_date\\_dec\\_posix\\_be](#) (const uint8\_t formatted\_date[(4)], [atcacert\\_tm\\_utc\\_t](#) \*timestamp)
- ATCA\_STATUS [atcacert\\_date\\_enc\\_posix\\_le](#) (const [atcacert\\_tm\\_utc\\_t](#) \*timestamp, uint8\_t formatted\_date[(4)])
- ATCA\_STATUS [atcacert\\_date\\_dec\\_posix\\_le](#) (const uint8\_t formatted\_date[(4)], [atcacert\\_tm\\_utc\\_t](#) \*timestamp)

- int `atcacert_date_cmp` (const `atcacert_tm_utc_t` \*timestamp1, const `atcacert_tm_utc_t` \*timestamp2)  
*Compare two dates.*
- ATCA\_STATUS `atcacert_get_subject` (const `atcacert_def_t` \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, `cal_buffer` \*cert\_subj\_buf)  
*Gets the subject name from a certificate.*
- ATCA\_STATUS `atcacert_get_subj_public_key` (const `atcacert_def_t` \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, uint8\_t subj\_public\_key[64])  
*Gets the subject public key from a certificate.*
- ATCA\_STATUS `atcacert_get_subj_key_id` (const `atcacert_def_t` \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, uint8\_t subj\_key\_id[20])  
*Gets the subject key ID from a certificate.*
- ATCA\_STATUS `atcacert_get_issuer` (const `atcacert_def_t` \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, uint8\_t cert\_issuer[128])  
*Gets the issuer name of a certificate.*
- ATCA\_STATUS `atcacert_get_issue_date` (const `atcacert_def_t` \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, `atcacert_tm_utc_t` \*timestamp)  
*Gets the issue date from a certificate. Will be parsed according to the date format specified in the certificate definition.*
- ATCA\_STATUS `atcacert_get_expire_date` (const `atcacert_def_t` \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, `atcacert_tm_utc_t` \*timestamp)  
*Gets the expire date from a certificate. Will be parsed according to the date format specified in the certificate definition.*
- ATCA\_STATUS `atcacert_get_cert_sn` (const `atcacert_def_t` \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, uint8\_t \*cert\_sn, size\_t \*cert\_sn\_size)  
*Gets the certificate serial number from a certificate.*
- ATCA\_STATUS `atcacert_get_auth_key_id` (const `atcacert_def_t` \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, uint8\_t auth\_key\_id[20])  
*Gets the authority key ID from a certificate.*
- int `atcacert_calc_expire_years` (const `atcacert_def_t` \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, int issue\_tm\_year, uint8\_t \*expire\_years)
- ATCA\_STATUS `atcacert_der_enc_length` (size\_t length, uint8\_t \*der\_length, size\_t \*der\_length\_size)  
*Encode a length in DER format.*
- ATCA\_STATUS `atcacert_der_dec_length` (const uint8\_t \*der\_length, size\_t \*der\_length\_size, size\_t \*length)  
*Decode a DER format length.*
- ATCA\_STATUS `atcacert_der_adjust_length` (uint8\_t \*der\_length, size\_t \*der\_length\_size, int delta\_length, size\_t \*new\_length)
- ATCA\_STATUS `atcacert_der_enc_integer` (const uint8\_t \*int\_data, size\_t int\_data\_size, uint8\_t is\_unsigned, uint8\_t \*der\_int, size\_t \*der\_int\_size)  
*Encode an ASN.1 integer in DER format, including tag and length fields.*
- ATCA\_STATUS `atcacert_der_dec_integer` (const uint8\_t \*der\_int, size\_t \*der\_int\_size, uint8\_t \*int\_data, size\_t \*int\_data\_size)  
*Decode an ASN.1 DER encoded integer.*
- ATCA\_STATUS `atcacert_der_enc_ecdsa_sig_value` (const uint8\_t raw\_sig[64], uint8\_t \*der\_sig, size\_t \*der\_sig\_size)  
*Formats a raw ECDSA P256 signature in the DER encoding found in X.509 certificates.*
- ATCA\_STATUS `atcacert_der_dec_ecdsa_sig_value` (const uint8\_t \*der\_sig, size\_t \*der\_sig\_size, uint8\_t raw\_sig[64])  
*Parses an ECDSA P256 signature in the DER encoding as found in X.509 certificates.*
- ATCA\_STATUS `atcacert_verify_cert_hw` (const `atcacert_def_t` \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, const uint8\_t ca\_public\_key[64])  
*Verify a certificate against its certificate authority's public key using the host's ATECC device for crypto functions.*
- ATCA\_STATUS `atcacert_gen_challenge_hw` (uint8\_t challenge[32])  
*Generate a random challenge to be sent to the client using the RNG on the host's ATECC device.*
- ATCA\_STATUS `atcacert_verify_response_hw` (const uint8\_t device\_public\_key[64], const uint8\_t challenge[32], const uint8\_t response[64])

## 19.6 Certificate manipulation methods (atcacert\_)

---

*Verify a client's response to a challenge using the host's ATECC device for crypto functions.*

- ATCA\_STATUS [atcacert\\_verify\\_cert\\_sw](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, const uint8\_t ca\_public\_key[64])

*Verify a certificate against its certificate authority's public key using software crypto functions. The function is currently not implemented.*

- ATCA\_STATUS [atcacert\\_gen\\_challenge\\_sw](#) (uint8\_t challenge[32])

*Generate a random challenge to be sent to the client using a software PRNG. The function is currently not implemented.*

- ATCA\_STATUS [atcacert\\_verify\\_response\\_sw](#) (const uint8\_t device\_public\_key[64], const uint8\_t challenge[32], const uint8\_t response[64])

*Verify a client's response to a challenge using software crypto functions. The function is currently not implemented.*

### Variables

- const size\_t [ATCACERT\\_DATE\\_FORMAT\\_SIZES](#) [5]

### 19.6.1 Detailed Description

These methods provide convenient ways to perform certification I/O with CryptoAuth chips and perform certificate manipulation in memory.

### 19.6.2 Macro Definition Documentation

#### 19.6.2.1 ATCACERT\_E\_BAD\_CERT

```
#define ATCACERT_E_BAD_CERT 10
```

Certificate structure is bad in some way.

#### 19.6.2.2 ATCACERT\_E\_BAD\_PARAMS

```
#define ATCACERT_E_BAD_PARAMS ATCA\_BAD\_PARAM
```

Invalid/bad parameter passed to function.

#### 19.6.2.3 ATCACERT\_E\_BUFFER\_TOO\_SMALL

```
#define ATCACERT_E_BUFFER_TOO_SMALL ATCA\_SMALL\_BUFFER
```

Supplied buffer for output is too small to hold the result.



#### 19.6.2.4 ATCACERT\_E\_DECODING\_ERROR

```
#define ATCACERT_E_DECODING_ERROR 4
```

Data being decoded/parsed has an invalid format.

#### 19.6.2.5 ATCACERT\_E\_ELEM\_MISSING

```
#define ATCACERT_E_ELEM_MISSING 8
```

The certificate element isn't defined for the certificate definition.

#### 19.6.2.6 ATCACERT\_E\_ELEM\_OUT\_OF\_BOUNDS

```
#define ATCACERT_E_ELEM_OUT_OF_BOUNDS 9
```

Certificate element is out of bounds for the given certificate.

#### 19.6.2.7 ATCACERT\_E\_ERROR

```
#define ATCACERT_E_ERROR ATCA_GEN_FAIL
```

General error.

#### 19.6.2.8 ATCACERT\_E\_INVALID\_DATE

```
#define ATCACERT_E_INVALID_DATE 5
```

Date is invalid.

#### 19.6.2.9 ATCACERT\_E\_INVALID\_TRANSFORM

```
#define ATCACERT_E_INVALID_TRANSFORM 13
```

Invalid transform passed to function.

#### 19.6.2.10 ATCACERT\_E\_SUCCESS

```
#define ATCACERT_E_SUCCESS ATCA_SUCCESS
```

Operation completed successfully.

#### 19.6.2.11 ATCACERT\_E\_UNEXPECTED\_ELEM\_SIZE

```
#define ATCACERT_E_UNEXPECTED_ELEM_SIZE 7
```

A certificate element size was not what was expected.

### 19.6.2.12 ATCACERT\_E\_UNIMPLEMENTED

```
#define ATCACERT_E_UNIMPLEMENTED ATCA_UNIMPLEMENTED
```

Function is unimplemented for the current configuration.

### 19.6.2.13 ATCACERT\_E\_VERIFY\_FAILED

```
#define ATCACERT_E_VERIFY_FAILED 12
```

Certificate or challenge/response verification failed.

### 19.6.2.14 DATEFMT\_ISO8601\_SEP

```
#define DATEFMT_ISO8601_SEP (0U)
```

ISO8601 full date YYYY-MM-DDThh:mm:ssZ.

Date formats.

## 19.6.3 Typedef Documentation

### 19.6.3.1 atcacert\_build\_state\_t

```
typedef struct atcacert_build_state_s atcacert_build_state_t
```

Tracks the state of a certificate as it's being rebuilt from device information.

### 19.6.3.2 atcacert\_cert\_element\_t

```
typedef struct ATCA_PACKED atcacert_cert_element_s atcacert_cert_element_t
```

Defines a generic dynamic element for a certificate including the device and template locations.

### 19.6.3.3 atcacert\_cert\_loc\_t

```
typedef struct ATCA_PACKED atcacert_cert_loc_s atcacert_cert_loc_t
```

Defines a chunk of data in a certificate template.

### 19.6.3.4 atcacert\_cert\_sn\_src\_t

```
typedef enum atcacert_cert_sn_src_e atcacert_cert_sn_src_t
```

Sources for the certificate serial number.

### 19.6.3.5 atccert\_cert\_type\_t

```
typedef enum atccert_cert_type_e atccert_cert_type_t
```

Types of certificates.

### 19.6.3.6 atccert\_def\_t

```
typedef struct atccert_def_s atccert_def_t
```

Defines a certificate and all the pieces to work with it.

If any of the standard certificate elements (std\_cert\_elements) are not a part of the certificate definition, set their count to 0 to indicate their absence.

### 19.6.3.7 atccert\_device\_loc\_t

```
typedef struct ATCA_PACKED atccert_device_loc_s atccert_device_loc_t
```

Defines a chunk of data in an ATECC device.

### 19.6.3.8 atccert\_device\_zone\_t

```
typedef enum atccert_device_zone_e atccert_device_zone_t
```

ATECC device zones. The values match the Zone Encodings as specified in the datasheet.

### 19.6.3.9 atccert\_std\_cert\_element\_t

```
typedef enum atccert_std_cert_element_e atccert_std_cert_element_t
```

Standard dynamic certificate elements.

### 19.6.3.10 atccert\_tm\_utc\_t

```
typedef struct atccert_tm_utc_s atccert_tm_utc_t
```

Holds a broken-down date in UTC. Mimics atccert\_tm\_utc\_t from time.h.

## 19.6.4 Enumeration Type Documentation

### 19.6.4.1 atccert\_cert\_sn\_src\_e

```
enum atccert_cert_sn_src_e
```

Sources for the certificate serial number.

## 19.6 Certificate manipulation methods (atcacert\_)

### Enumerator

SNSRC_STORED	Cert serial is stored on the device.
SNSRC_STORED_DYNAMIC	Cert serial is stored on the device with the first byte being the DER size (X509 certs only).
SNSRC_DEVICE_SN	Cert serial number is 0x40(MSB) + 9-byte device serial number. Only applies to device certificates.
SNSRC_SIGNER_ID	Cert serial number is 0x40(MSB) + 2-byte signer ID. Only applies to signer certificates.
SNSRC_PUB_KEY_HASH	Cert serial number is the SHA256(Subject public key + Encoded dates), with uppermost 2 bits set to 01.
SNSRC_DEVICE_SN_HASH	Cert serial number is the SHA256(Device SN + Encoded dates), with uppermost 2 bits set to 01. Only applies to device certificates.
SNSRC_PUB_KEY_HASH_POS	Deprecated, don't use. Cert serial number is the SHA256(Subject public key + Encoded dates), with MSBit set to 0 to ensure it's positive.
SNSRC_DEVICE_SN_HASH_POS	Deprecated, don't use. Cert serial number is the SHA256(Device SN + Encoded dates), with MSBit set to 0 to ensure it's positive. Only applies to device certificates.
SNSRC_PUB_KEY_HASH_RAW	Deprecated, don't use. Cert serial number is the SHA256(Subject public key + Encoded dates).
SNSRC_DEVICE_SN_HASH_RAW	Deprecated, don't use. Cert serial number is the SHA256(Device SN + Encoded dates). Only applies to device certificates.

### 19.6.4.2 atcacert\_cert\_type\_e

enum atcacert\_cert\_type\_e

Types of certificates.

### Enumerator

CERTTYPE_X509	Standard X509 certificate.
CERTTYPE_CUSTOM	Custom format.
CERTTYPE_X509_FULL_STORED	Full Stored X509 Certificate.

### 19.6.4.3 atcacert\_device\_zone\_e

enum atcacert\_device\_zone\_e

ATECC device zones. The values match the Zone Encodings as specified in the datasheet.

### Enumerator

DEVZONE_CONFIG	Configuration zone.
DEVZONE_OTP	One Time Programmable zone.
DEVZONE_DATA	Data zone (slots).
DEVZONE_GENKEY	Data zone - Generate Pubkey (slots).
DEVZONE_NONE	Special value used to indicate there is no device location.

19.6.4.4 atcacert\_std\_cert\_element\_e

enum atcacert\_std\_cert\_element\_e

Standard dynamic certificate elements.

Enumerator

STDCERT_NUM_ELEMENTS	Special item to give the number of elements in this enum.
----------------------	---

19.6.4.5 atcacert\_transform\_e

enum atcacert\_transform\_e

How to transform the data from the device to the certificate.

Enumerator

TF_NONE	No transform, data is used byte for byte.
TF_REVERSE	Reverse the bytes (e.g. change endianness)
TF_BIN2HEX_UC	Convert raw binary into ASCII hex, uppercase.
TF_BIN2HEX_LC	Convert raw binary into ASCII hex, lowercase.
TF_HEX2BIN_UC	Convert ASCII hex, uppercase to binary.
TF_HEX2BIN_LC	Convert ASCII hex, lowercase to binary.
TF_BIN2HEX_SPACE_UC	Convert raw binary into ASCII hex, uppercase space between bytes.
TF_BIN2HEX_SPACE_LC	Convert raw binary into ASCII hex, lowercase space between bytes.
TF_HEX2BIN_SPACE_UC	Convert ASCII hex, uppercase with spaces between bytes to binary.
TF_HEX2BIN_SPACE_LC	Convert ASCII hex, lowercase with spaces between bytes to binary.

19.6.5 Function Documentation

19.6.5.1 atcacert\_calc\_expire\_years()

```
int atcacert_calc_expire_years (
    const atcacert_def_t * cert_def,
    const uint8_t * cert,
    size_t cert_size,
    int issue_tm_year,
    uint8_t * expire_years )
```

## 19.6 Certificate manipulation methods (atcacert\_)

---

### Parameters

in	<i>cert_def</i>	Certificate definition to find a max size for.
in	<i>cert</i>	Certificate to get element from.
in	<i>cert_size</i>	Size of the certificate (cert) in bytes.
in	<i>issue_tm_year</i>	issue year.
out	<i>expire_years</i>	expire years.

### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 19.6.5.2 atcacert\_create\_csr()

```
ATCA_STATUS atcacert_create_csr (
    const atcacert_def_t * csr_def,
    uint8_t * csr,
    size_t * csr_size )
```

Creates a CSR specified by the CSR definition from the ATECC508A device. This process involves reading the dynamic CSR data from the device and combining it with the template found in the CSR definition, then signing it. Return the CSR in der format.

### Parameters

in	<i>csr_def</i>	CSR definition describing where to find the dynamic CSR information on the device and how to incorporate it into the template.
out	<i>csr</i>	Buffer to receive the CSR.
in, out	<i>csr_size</i>	As input, the size of the CSR buffer in bytes. As output, the size of the CSR returned in cert in bytes.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.6.5.3 atcacert\_create\_csr\_pem()

```
ATCA_STATUS atcacert_create_csr_pem (
    const atcacert_def_t * csr_def,
    char * csr,
    size_t * csr_size )
```

Creates a CSR specified by the CSR definition from the ATECC508A device. This process involves reading the dynamic CSR data from the device and combining it with the template found in the CSR definition, then signing it. Return the CSR in der format.

Parameters

in	<i>csr_def</i>	CSR definition describing where to find the dynamic CSR information on the device and how to incorporate it into the template.
out	<i>csr</i>	Buffer to received the CSR formatted as PEM.
in, out	<i>csr_size</i>	As input, the size of the CSR buffer in bytes. As output, the size of the CSR as PEM returned in cert in bytes.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.6.5.4 atcacert\_date\_cmp()

```
int atcacert_date_cmp (
    const atcacert_tm_utc_t * timestamp1,
    const atcacert_tm_utc_t * timestamp2 )
```

Compare two dates.

Dates are not checked for validity before comparing.

Parameters

in	<i>timestamp1</i>	First date to compare.
in	<i>timestamp2</i>	Second date to compare.

Returns

-1 if timestamp1 is before timestamp2, 0 if they are equal, 1 if they are timestamp1 is after timestamp2.  
ATCACERT\_E\_BAD\_PARAMS if either input is NULL.

19.6.5.5 atcacert\_date\_dec()

```
ATCA_STATUS atcacert_date_dec (
    atcacert_date_format_t format,
    const uint8_t * formatted_date,
    size_t formatted_date_size,
    atcacert_tm_utc_t * timestamp )
```

Parse a formatted timestamp according to the specified format.

Parameters

in	<i>format</i>	Format to parse the formatted date as.
in	<i>formatted_date</i>	Formatted date to be parsed.
in	<i>formatted_date_size</i>	Size of the formatted date in bytes.
out	<i>timestamp</i>	Parsed timestamp is returned here.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.6.5.6 atcacert\_date\_dec\_compcert()

```
ATCA_STATUS atcacert_date_dec_compcert (
    const uint8_t enc_dates[3],
    atcacert_date_format_t expire_date_format,
    atcacert_tm_utc_t * issue_date,
    atcacert_tm_utc_t * expire_date )
```

Decode the issue and expire dates from the format used by the compressed certificate.

Parameters

in	<i>enc_dates</i>	Encoded date from the compressed certificate. 3 bytes.
in	<i>expire_date_format</i>	Expire date format. Only used to determine max date when no expiration date is specified by the encoded date.
out	<i>issue_date</i>	Decoded issue date is returned here.
out	<i>expire_date</i>	Decoded expire date is returned here. If there is no expiration date, the expire date will be set to a maximum value for the given <i>expire_date_format</i> .

Returns

0 on success

19.6.5.7 atcacert\_date\_dec\_compcert\_ext()

```
ATCA_STATUS atcacert_date_dec_compcert_ext (
    const uint8_t comp_cert[72u],
    atcacert_date_format_t expire_date_format,
    atcacert_tm_utc_t * issue_date,
    atcacert_tm_utc_t * expire_date )
```

Decode the issue and expire dates from the format used by the compressed certificate.

Supports extended dates if the format version field is 1

Parameters

in, out	<i>comp_cert</i>	Compressed certificate (72 bytes) where the encoded dates will be set. Format version (In comp_cert byte 70([3:0]) must be set to 1 to use extended dates.
in	<i>expire_date_format</i>	Expire date format. Only used to determine max date when no expiration date is specified by the encoded date.
out	<i>issue_date</i>	Decoded issue date is returned here.
out	<i>expire_date</i>	Decoded expire date is returned here. If there is no expiration date, the expire date will be set to a maximum value for the given <i>expire_date_format</i> .



Returns

0 on success

19.6.5.8 atcacert\_date\_enc()

```
ATCA_STATUS atcacert_date_enc (
    atcacert_date_format_t format,
    const atcacert_tm_utc_t * timestamp,
    uint8_t * formatted_date,
    size_t * formatted_date_size )
```

Format a timestamp according to the format type.

Parameters

in	<i>format</i>	Format to use.
in	<i>timestamp</i>	Timestamp to format.
out	<i>formatted_date</i>	Formatted date will be returned in this buffer.
in, out	<i>formatted_date_size</i>	As input, the size of the formatted_date buffer. As output, the size of the returned formatted_date.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.6.5.9 atcacert\_date\_enc\_compcert()

```
ATCA_STATUS atcacert_date_enc_compcert (
    const atcacert_tm_utc_t * issue_date,
    uint8_t expire_years,
    uint8_t enc_dates[3] )
```

Encode the issue and expire dates in the format used by the compressed certificate.

Parameters

in	<i>issue_date</i>	Issue date to encode. Note that minutes and seconds will be ignored.
in	<i>expire_years</i>	Expire date is expressed as a number of years past the issue date. 0 should be used if there is no expire date.
out	<i>enc_dates</i>	Encoded dates for use in the compressed certificate is returned here. 3 bytes.

Returns

0 on success

## 19.6 Certificate manipulation methods (atcacert\_)

### 19.6.5.10 atcacert\_date\_enc\_compcert\_ext()

```
ATCA_STATUS atcacert_date_enc_compcert_ext (
    const atcacert_tm_utc_t * issue_date,
    uint8_t expire_years,
    uint8_t comp_cert[72u] )
```

Encode the issue and expire dates in the format used by the compressed certificate.

Supports extended dates if the format version field is set appropriately (currently 1).

#### Parameters

in	<i>issue_date</i>	Issue date to encode. Note that minutes and seconds will be ignored.
in	<i>expire_years</i>	Expire date is expressed as a number of years past the issue date. 0 should be used if there is no expire date.
in, out	<i>comp_cert</i>	Compressed certificate (72 bytes) where the encoded dates will be set. Format version must be set appropriately.

#### Returns

0 on success

### 19.6.5.11 atcacert\_date\_from\_asn1\_tag()

```
atcacert_date_format_t atcacert_date_from_asn1_tag (
    const uint8_t tag )
```

Convert the asn1 tag for the supported time formats into the local time format.

#### Returns

DATEFMT\_RFC5280\_UTC, DATEFMT\_RFC5280\_GEN, or DATEFMT\_INVALID

### 19.6.5.12 atcacert\_date\_get\_max\_date()

```
ATCA_STATUS atcacert_date_get_max_date (
    atcacert_date_format_t format,
    atcacert_tm_utc_t * timestamp )
```

Return the maximum date available for the given format.

#### Parameters

in	<i>format</i>	Format to get the max date for.
out	<i>timestamp</i>	Max date is returned here.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.6.5.13 atcacert\_der\_dec\_ecdsa\_sig\_value()

```
ATCA_STATUS atcacert_der_dec_ecdsa_sig_value (
    const uint8_t * der_sig,
    size_t * der_sig_size,
    uint8_t raw_sig[64] )
```

Parses an ECDSA P256 signature in the DER encoding as found in X.509 certificates.

This will parse the DER encoding of the signatureValue field as found in an X.509 certificate (RFC 5280). x509\_sig should include the tag, length, and value. The value of the signatureValue is the DER encoding of the ECDSA-Sig-Value as specified by RFC 5480 and SECG SEC1.

Parameters

in	der_sig	X.509 format signature (TLV of signatureValue) to be parsed.
in, out	der_sig_size	As input, size of the der_sig buffer in bytes. As output, size of the DER x.509 signature parsed from the buffer.
out	raw_sig	Parsed P256 ECDSA signature will be returned in this buffer. Formatted as R and S integers concatenated together. 64 bytes.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.6.5.14 atcacert\_der\_dec\_integer()

```
ATCA_STATUS atcacert_der_dec_integer (
    const uint8_t * der_int,
    size_t * der_int_size,
    uint8_t * int_data,
    size_t * int_data_size )
```

Decode an ASN.1 DER encoded integer.

X.680 ( <http://www.itu.int/rec/T-REC-X.680/en>) section 19.8, for tag value X.690 ( <http://www.itu.int/rec/T-REC-X.690/en>) section 8.3, for encoding

Parameters

in	der_int	DER encoded ASN.1 integer, including the tag and length fields.
in, out	der_int_size	As input, the size of the der_int buffer in bytes. As output, the size of the DER integer decoded in bytes.
out	int_data	Decode integer is returned in this buffer in a signed big-endian format.
in, out	int_data_size	As input, the size of int_data in bytes. As output, the size of the decoded integer in bytes.

## 19.6 Certificate manipulation methods (atcacert\_)

### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 19.6.5.15 atcacert\_der\_dec\_length()

```
ATCA_STATUS atcacert_der_dec_length (
    const uint8_t * der_length,
    size_t * der_length_size,
    size_t * length )
```

Decode a DER format length.

X.690 ( <http://www.itu.int/rec/T-REC-X.690/en>) section 8.1.3, for encoding

### Parameters

in	<i>der_length</i>	DER encoded length.
in, out	<i>der_length_size</i>	As input, the size of the der_length buffer in bytes. As output, the size of the DER encoded length that was decoded.
out	<i>length</i>	Decoded length is returned here.

### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 19.6.5.16 atcacert\_der\_enc\_ecdsa\_sig\_value()

```
ATCA_STATUS atcacert_der_enc_ecdsa_sig_value (
    const uint8_t raw_sig[64],
    uint8_t * der_sig,
    size_t * der_sig_size )
```

Formats a raw ECDSA P256 signature in the DER encoding found in X.509 certificates.

This will return the DER encoding of the signatureValue field as found in an X.509 certificate (RFC 5280). This include the tag, length, and value. The value of the signatureValue is the DER encoding of the ECDSA-Sig-Value as specified by RFC 5480 and SECG SEC1.

### Parameters

in	<i>raw_sig</i>	P256 ECDSA signature to be formatted. Input format is R and S integers concatenated together. 64 bytes.
out	<i>der_sig</i>	X.509 format signature (TLV of signatureValue) will be returned in this buffer.
in, out	<i>der_sig_size</i>	As input, the size of the x509_sig buffer in bytes. As output, the size of the returned X.509 signature in bytes.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.6.5.17 atcacert\_der\_enc\_integer()

```
ATCA_STATUS atcacert_der_enc_integer (
    const uint8_t * int_data,
    size_t int_data_size,
    uint8_t is_unsigned,
    uint8_t * der_int,
    size_t * der_int_size )
```

Encode an ASN.1 integer in DER format, including tag and length fields.

X.680 ( <http://www.itu.int/rec/T-REC-X.680/en>) section 19.8, for tag value X.690 ( <http://www.itu.int/rec/T-REC-X.690/en>) section 8.3, for encoding

Parameters

in	<i>int_data</i>	Raw integer in big-endian format.
in	<i>int_data_size</i>	Size of the raw integer in bytes.
in	<i>is_unsigned</i>	Indicate whether the input integer should be treated as unsigned.
out	<i>der_int</i>	DER encoded integer is returned in this buffer.
in, out	<i>der_int_size</i>	As input, the size of the der_int buffer in bytes. As output, the size of the DER integer returned in bytes.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.6.5.18 atcacert\_der\_enc\_length()

```
ATCA_STATUS atcacert_der_enc_length (
    size_t length,
    uint8_t * der_length,
    size_t * der_length_size )
```

Encode a length in DER format.

X.690 ( <http://www.itu.int/rec/T-REC-X.690/en>) section 8.1.3, for encoding

Parameters

in	<i>length</i>	Length to be encoded.
out	<i>der_length</i>	DER encoded length will returned in this buffer.
in, out	<i>der_length_size</i>	As input, size of der_length buffer in bytes. As output, the size of the DER length encoding in bytes.

### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

#### 19.6.5.19 atcacert\_gen\_challenge\_hw()

```
ATCA_STATUS atcacert_gen_challenge_hw (
    uint8_t challenge[32] )
```

Generate a random challenge to be sent to the client using the RNG on the host's ATECC device.

### Parameters

out	<i>challenge</i>	Random challenge is return here. 32 bytes.
-----	------------------	--

### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

#### 19.6.5.20 atcacert\_gen\_challenge\_sw()

```
ATCA_STATUS atcacert_gen_challenge_sw (
    uint8_t challenge[32] )
```

Generate a random challenge to be sent to the client using a software PRNG. The function is currently not implemented.

### Parameters

out	<i>challenge</i>	Random challenge is return here. 32 bytes.
-----	------------------	--

### Returns

ATCA\_UNIMPLEMENTED , as the function is currently not implemented.

#### 19.6.5.21 atcacert\_get\_auth\_key\_id()

```
ATCA_STATUS atcacert_get_auth_key_id (
    const atcacert_def_t * cert_def,
    const uint8_t * cert,
    size_t cert_size,
    uint8_t auth_key_id[20] )
```

Gets the authority key ID from a certificate.

Parameters

in	<i>cert_def</i>	Certificate definition for the certificate.
in	<i>cert</i>	Certificate to get element from.
in	<i>cert_size</i>	Size of the certificate (cert) in bytes.
out	<i>auth_key↔ _id</i>	Authority key ID is returned in this buffer. 20 bytes.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.6.5.22 atcacert\_get\_cert\_sn()

```
ATCA_STATUS atcacert_get_cert_sn (
    const atcacert_def_t * cert_def,
    const uint8_t * cert,
    size_t cert_size,
    uint8_t * cert_sn,
    size_t * cert_sn_size )
```

Gets the certificate serial number from a certificate.

Parameters

in	<i>cert_def</i>	Certificate definition for the certificate.
in	<i>cert</i>	Certificate to get element from.
in	<i>cert_size</i>	Size of the certificate (cert) in bytes.
out	<i>cert_sn</i>	Certificate SN will be returned in this buffer.
in, out	<i>cert_sn_size</i>	As input, the size of the cert_sn buffer. As output, the size of the certificate SN (cert_sn) in bytes.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.6.5.23 atcacert\_get\_expire\_date()

```
ATCA_STATUS atcacert_get_expire_date (
    const atcacert_def_t * cert_def,
    const uint8_t * cert,
    size_t cert_size,
    atcacert_tm_utc_t * timestamp )
```

Gets the expire date from a certificate. Will be parsed according to the date format specified in the certificate definition.

## 19.6 Certificate manipulation methods (atcacert\_)

---

### Parameters

in	<i>cert_def</i>	Certificate definition for the certificate.
in	<i>cert</i>	Certificate to get element from.
in	<i>cert_size</i>	Size of the certificate (cert) in bytes.
out	<i>timestamp</i>	Expire date is returned in this structure.

### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

#### 19.6.5.24 atcacert\_get\_issue\_date()

```
ATCA_STATUS atcacert_get_issue_date (
    const atcacert_def_t * cert_def,
    const uint8_t * cert,
    size_t cert_size,
    atcacert_tm_utc_t * timestamp )
```

Gets the issue date from a certificate. Will be parsed according to the date format specified in the certificate definition.

### Parameters

in	<i>cert_def</i>	Certificate definition for the certificate.
in	<i>cert</i>	Certificate to get element from.
in	<i>cert_size</i>	Size of the certificate (cert) in bytes.
out	<i>timestamp</i>	Issue date is returned in this structure.

### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

#### 19.6.5.25 atcacert\_get\_issuer()

```
ATCA_STATUS atcacert_get_issuer (
    const atcacert_def_t * cert_def,
    const uint8_t * cert,
    size_t cert_size,
    uint8_t cert_issuer[128] )
```

Gets the issuer name of a certificate.



Parameters

in	<i>cert_def</i>	Certificate definition for the certificate.
in	<i>cert</i>	Certificate to get element from.
in	<i>cert_size</i>	Size of the certificate (cert) in bytes.
out	<i>cert_issuer</i>	Certificate's issuer is returned in this buffer.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.6.5.26 atcacert\_get\_response()

```
ATCA_STATUS atcacert_get_response (
    uint8_t device_private_key_slot,
    const uint8_t challenge[32],
    uint8_t response[64] )
```

Calculates the response to a challenge sent from the host.

The challenge-response protocol is an ECDSA Sign and Verify. This performs the ECDSA Sign on the challenge and returns the signature as the response.

Parameters

in	<i>device_private_key_slot</i>	Slot number for the device's private key. This must be the same slot used to generate the public key included in the device's certificate.
in	<i>challenge</i>	Challenge to generate the response for. Must be 32 bytes.
out	<i>response</i>	Response will be returned in this buffer. 64 bytes.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.6.5.27 atcacert\_get\_subj\_key\_id()

```
ATCA_STATUS atcacert_get_subj_key_id (
    const atcacert_def_t * cert_def,
    const uint8_t * cert,
    size_t cert_size,
    uint8_t subj_key_id[20] )
```

Gets the subject key ID from a certificate.

## 19.6 Certificate manipulation methods (atcacert\_)

---

### Parameters

in	<i>cert_def</i>	Certificate definition for the certificate.
in	<i>cert</i>	Certificate to get element from.
in	<i>cert_size</i>	Size of the certificate (cert) in bytes.
out	<i>subj_key↔ _id</i>	Subject key ID is returned in this buffer. 20 bytes.

### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 19.6.5.28 atcacert\_get\_subj\_public\_key()

```
ATCA_STATUS atcacert_get_subj_public_key (
    const atcacert_def_t * cert_def,
    const uint8_t * cert,
    size_t cert_size,
    uint8_t subj_public_key[64] )
```

Gets the subject public key from a certificate.

### Parameters

in	<i>cert_def</i>	Certificate definition for the certificate.
in	<i>cert</i>	Certificate to get element from.
in	<i>cert_size</i>	Size of the certificate (cert) in bytes.
out	<i>subj_public_key</i>	Subject public key is returned in this buffer. Formatted at X and Y integers concatenated together. 64 bytes.

### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 19.6.5.29 atcacert\_get\_subject()

```
ATCA_STATUS atcacert_get_subject (
    const atcacert_def_t * cert_def,
    const uint8_t * cert,
    size_t cert_size,
    cal_buffer * cert_subj_buf )
```

Gets the subject name from a certificate.

Parameters

in	<i>cert_def</i>	Certificate definition for the certificate.
in	<i>cert</i>	Certificate to get element from.
in	<i>cert_size</i>	Size of the certificate (cert) in bytes.
out	<i>subject</i>	Subject name is returned in this buffer.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.6.5.30 atcacert\_read\_cert()

```
ATCA_STATUS atcacert_read_cert (
    const atcacert_def_t * cert_def,
    const uint8_t ca_public_key[64],
    uint8_t * cert,
    size_t * cert_size )
```

Reads the certificate specified by the certificate definition from the ATECC508A device.

This process involves reading the dynamic cert data from the device and combining it with the template found in the certificate definition.

Parameters

in	<i>cert_def</i>	Certificate definition describing where to find the dynamic certificate information on the device and how to incorporate it into the template.
in	<i>ca_public_key</i>	The ECC P256 public key of the certificate authority that signed this certificate. Formatted as the 32 byte X and Y integers concatenated together (64 bytes total). Set to NULL if the authority key id is not needed, set properly in the cert_def template, or stored on the device as specied in the cert_def cert_elements.
out	<i>cert</i>	Buffer to received the certificate.
in, out	<i>cert_size</i>	As input, the size of the cert buffer in bytes. As output, the size of the certificate returned in cert in bytes.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.6.5.31 atcacert\_read\_cert\_ext()

```
ATCA_STATUS atcacert_read_cert_ext (
    ATCADevice device,
```

## 19.6 Certificate manipulation methods (atcacert\_)

```
const atcacert_def_t * cert_def,  
const uint8_t ca_public_key[64],  
uint8_t * cert,  
size_t * cert_size )
```

Reads the certificate specified by the certificate definition from the ATECC508A device.

This process involves reading the dynamic cert data from the device and combining it with the template found in the certificate definition.

### Parameters

in	<i>device</i>	Device context
in	<i>cert_def</i>	Certificate definition describing where to find the dynamic certificate information on the device and how to incorporate it into the template.
in	<i>ca_public_key</i>	The ECC P256 public key of the certificate authority that signed this certificate. Formatted as the 32 byte X and Y integers concatenated together (64 bytes total). Set to NULL if the authority key id is not needed, set properly in the cert_def template, or stored on the device as specified in the cert_def cert_elements.
out	<i>cert</i>	Buffer to received the certificate.
in, out	<i>cert_size</i>	As input, the size of the cert buffer in bytes. As output, the size of the certificate returned in cert in bytes.

### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 19.6.5.32 atcacert\_read\_cert\_size()

```
ATCA_STATUS atcacert_read_cert_size (   
    const atcacert_def_t * cert_def,  
    size_t * cert_size )
```

Return the actual certificate size in bytes for a given cert def. Certificate can be variable size, so this gives the absolute buffer size when reading the certificates.

### Parameters

in	<i>cert_def</i>	Certificate definition to find a max size for.
out	<i>cert_size</i>	Certificate size will be returned here in bytes.

### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.6.5.33 atcacert\_read\_cert\_size\_ext()

```
ATCA_STATUS atcacert_read_cert_size_ext (
    ATCADevice device,
    const atcacert_def_t * cert_def,
    size_t * cert_size )
```

Return the actual certificate size in bytes for a given cert def. Certificate can be variable size, so this gives the absolute buffer size when reading the certificates.

Parameters

in	<i>device</i>	Device context
in	<i>cert_def</i>	Certificate definition to find a max size for.
out	<i>cert_size</i>	Certificate size will be returned here in bytes.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.6.5.34 atcacert\_read\_device\_loc()

```
ATCA_STATUS atcacert_read_device_loc (
    const atcacert_device_loc_t * device_loc,
    uint8_t * data )
```

Read the data from a device location.

Parameters

in	<i>device_loc</i>	Device location to read data from.
out	<i>data</i>	Data read is returned here.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.6.5.35 atcacert\_read\_device\_loc\_ext()

```
ATCA_STATUS atcacert_read_device_loc_ext (
    ATCADevice device,
    const atcacert_device_loc_t * device_loc,
    uint8_t * data )
```

Read the data from a device location.

### Parameters

in	<i>device</i>	Device context
in	<i>device_loc</i>	Device location to read data from.
out	<i>data</i>	Data read is returned here.

### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

#### 19.6.5.36 atcacert\_read\_subj\_key\_id()

```
ATCA_STATUS atcacert_read_subj_key_id (
    const atcacert_def_t * cert_def,
    uint8_t subj_key_id[20] )
```

Reads the subject key ID based on a certificate definition.

### Parameters

in	<i>cert_def</i>	Certificate definition
out	<i>subj_key_id</i>	Subject key ID is returned in this buffer. 20 bytes.

### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

#### 19.6.5.37 atcacert\_read\_subj\_key\_id\_ext()

```
ATCA_STATUS atcacert_read_subj_key_id_ext (
    ATCADevice device,
    const atcacert_def_t * cert_def,
    uint8_t subj_key_id[20] )
```

Reads the subject key ID based on a certificate definition.

### Parameters

in	<i>device</i>	Device context
in	<i>cert_def</i>	Certificate definition
out	<i>subj_key_id</i>	Subject key ID is returned in this buffer. 20 bytes.

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.6.5.38 atcacert\_verify\_cert\_hw()

```
ATCA_STATUS atcacert_verify_cert_hw (
    const atcacert_def_t * cert_def,
    const uint8_t * cert,
    size_t cert_size,
    const uint8_t ca_public_key[64] )
```

Verify a certificate against its certificate authority's public key using the host's ATECC device for crypto functions.

Parameters

in	<i>cert_def</i>	Certificate definition describing how to extract the TBS and signature components from the certificate specified.
in	<i>cert</i>	Certificate to verify.
in	<i>cert_size</i>	Size of the certificate (cert) in bytes.
in	<i>ca_public_key</i>	The ECC P256 public key of the certificate authority that signed this certificate. Formatted as the 32 byte X and Y integers concatenated together (64 bytes total).

Returns

ATCACERT\_E\_SUCCESS if the verify succeeds, ATCACERT\_VERIFY\_FAILED or ATCA\_EXECUTION\_ERROR if it fails to verify. ATCA\_EXECUTION\_ERROR may occur when the public key is invalid and doesn't fall on the P256 curve.

19.6.5.39 atcacert\_verify\_cert\_sw()

```
ATCA_STATUS atcacert_verify_cert_sw (
    const atcacert_def_t * cert_def,
    const uint8_t * cert,
    size_t cert_size,
    const uint8_t ca_public_key[64] )
```

Verify a certificate against its certificate authority's public key using software crypto functions. The function is currently not implemented.

Parameters

in	<i>cert_def</i>	Certificate definition describing how to extract the TBS and signature components from the certificate specified.
in	<i>cert</i>	Certificate to verify.
in	<i>cert_size</i>	Size of the certificate (cert) in bytes.
in	<i>ca_public_key</i>	The ECC P256 public key of the certificate authority that signed this certificate. Formatted as the 32 byte X and Y integers concatenated together (64 bytes total).

### Returns

ATCA\_UNIMPLEMENTED , as the function is currently not implemented.

#### 19.6.5.40 atcacert\_verify\_response\_hw()

```
ATCA_STATUS atcacert_verify_response_hw (
    const uint8_t device_public_key[64],
    const uint8_t challenge[32],
    const uint8_t response[64] )
```

Verify a client's response to a challenge using the host's ATECC device for crypto functions.

The challenge-response protocol is an ECDSA Sign and Verify. This performs an ECDSA verify on the response returned by the client, verifying the client has the private key counter-part to the public key returned in its certificate.

### Parameters

in	<i>device_public_key</i>	Device public key as read from its certificate. Formatted as the X and Y integers concatenated together. 64 bytes.
in	<i>challenge</i>	Challenge that was sent to the client. 32 bytes.
in	<i>response</i>	Response returned from the client to be verified. 64 bytes.

### Returns

ATCACERT\_E\_SUCCESS if the verify succeeds, ATCACERT\_VERIFY\_FAILED or ATCA\_EXECUTION\_ERROR if it fails to verify. ATCA\_EXECUTION\_ERROR may occur when the public key is invalid and doesn't fall on the P256 curve.

#### 19.6.5.41 atcacert\_verify\_response\_sw()

```
ATCA_STATUS atcacert_verify_response_sw (
    const uint8_t device_public_key[64],
    const uint8_t challenge[32],
    const uint8_t response[64] )
```

Verify a client's response to a challenge using software crypto functions. The function is currently not implemented.

The challenge-response protocol is an ECDSA Sign and Verify. This performs an ECDSA verify on the response returned by the client, verifying the client has the private key counter-part to the public key returned in its certificate.

### Parameters

in	<i>device_public_key</i>	Device public key as read from its certificate. Formatted as the X and Y integers concatenated together. 64 bytes.
in	<i>challenge</i>	Challenge that was sent to the client. 32 bytes.
in	<i>response</i>	Response returned from the client to be verified. 64 bytes.



Returns

ATCA\_UNIMPLEMENTED , as the function is currently not implemented.

19.6.5.42 atcacert\_write\_cert()

```
ATCA_STATUS atcacert_write_cert (
    const atcacert_def_t * cert_def,
    const uint8_t * cert,
    size_t cert_size )
```

Take a full certificate and write it to the ATECC508A device according to the certificate definition.

Parameters

in	<i>cert_def</i>	Certificate definition describing where the dynamic certificate information is and how to store it on the device.
in	<i>cert</i>	Full certificate to be stored.
in	<i>cert_size</i>	Size of the full certificate in bytes.
in	<i>device</i>	Device context

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

19.6.5.43 atcacert\_write\_cert\_ext()

```
ATCA_STATUS atcacert_write_cert_ext (
    ATCADevice device,
    const atcacert_def_t * cert_def,
    const uint8_t * cert,
    size_t cert_size )
```

Take a full certificate and write it to the ATECC508A device according to the certificate definition.

Parameters

in	<i>device</i>	Device context
in	<i>cert_def</i>	Certificate definition describing where the dynamic certificate information is and how to store it on the device.
in	<i>cert</i>	Full certificate to be stored.
in	<i>cert_size</i>	Size of the full certificate in bytes.
in	<i>device</i>	Device context

### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

## 19.7 Basic Crypto API methods for CryptoAuth Devices (calib\_)

These methods provide a simple API to CryptoAuth chips.

### 19.7.0.1 calib directory - Purpose

The purpose of this directory is to contain the files implementing the APIs for a basic interface to the core CryptoAuthLib library.

High-level functions like these make it very convenient to use the library when standard configurations and defaults are in play. They are the easiest to use when developing examples or trying to understand the "flow" of an authentication operation without getting overwhelmed by the details.

This makes simple jobs easy and if you need more sophistication and power, you can employ the full power of the CryptoAuthLib object model.

See the Doxygen documentation in `cryptoauthlib/docs` for details on the API of the calib commands.

### Data Structures

- struct [atca\\_sha256\\_ctx](#)
- struct [atsha204a\\_config\\_s](#)
- struct [atecc508a\\_config\\_s](#)
- struct [atecc608\\_config\\_s](#)

### Macros

- #define **ATCA\_AES\_ENABLE\_EN\_SHIFT** (0)
- #define **ATCA\_AES\_ENABLE\_EN\_MASK** (0x01u << ATCA\_AES\_ENABLE\_EN\_SHIFT)
- #define **ATCA\_I2C\_ENABLE\_EN\_SHIFT** (0)
- #define **ATCA\_I2C\_ENABLE\_EN\_MASK** (0x01u << ATCA\_I2C\_ENABLE\_EN\_SHIFT)
- #define **ATCA\_COUNTER\_MATCH\_EN\_SHIFT** (0)
- #define **ATCA\_COUNTER\_MATCH\_EN\_MASK** (0x01u << ATCA\_COUNTER\_MATCH\_EN\_SHIFT)
- #define **ATCA\_COUNTER\_MATCH\_KEY\_SHIFT** (4)
- #define **ATCA\_COUNTER\_MATCH\_KEY\_MASK** (0x0Fu << ATCA\_COUNTER\_MATCH\_KEY\_SHIFT)
- #define **ATCA\_COUNTER\_MATCH\_KEY(v)** (ATCA\_COUNTER\_MATCH\_KEY\_MASK & (v << ATCA\_COUNTER\_MATCH\_KEY\_SHIFT))
- #define **ATCA\_CHIP\_MODE\_I2C\_EXTRA\_SHIFT** (0)
- #define **ATCA\_CHIP\_MODE\_I2C\_EXTRA\_MASK** (0x01u << ATCA\_CHIP\_MODE\_I2C\_EXTRA\_SHIFT)
- #define **ATCA\_CHIP\_MODE\_TTL\_EN\_SHIFT** (1)
- #define **ATCA\_CHIP\_MODE\_TTL\_EN\_MASK** (0x01u << ATCA\_CHIP\_MODE\_TTL\_EN\_SHIFT)
- #define **ATCA\_CHIP\_MODE\_WDG\_LONG\_SHIFT** (2)
- #define **ATCA\_CHIP\_MODE\_WDG\_LONG\_MASK** (0x01u << ATCA\_CHIP\_MODE\_WDG\_LONG\_SHIFT)
- #define **ATCA\_CHIP\_MODE\_CLK\_DIV\_SHIFT** (3)
- #define **ATCA\_CHIP\_MODE\_CLK\_DIV\_MASK** (0x1Fu << ATCA\_CHIP\_MODE\_CLK\_DIV\_SHIFT)
- #define **ATCA\_CHIP\_MODE\_CLK\_DIV(v)** (ATCA\_CHIP\_MODE\_CLK\_DIV\_MASK & (v << ATCA\_CHIP\_MODE\_CLK\_DIV\_SHIFT))

- #define **ATCA\_SLOT\_CONFIG\_READKEY\_SHIFT** (0)
- #define **ATCA\_SLOT\_CONFIG\_READKEY\_MASK** (0x0Fu << ATCA\_SLOT\_CONFIG\_READKEY\_SHIFT)
- #define **ATCA\_SLOT\_CONFIG\_READKEY(v)** (ATCA\_SLOT\_CONFIG\_READKEY\_MASK & (v << ATCA\_SLOT\_CONFIG\_READKEY\_SHIFT))
- #define **ATCA\_SLOT\_CONFIG\_NOMAC\_SHIFT** (4)
- #define **ATCA\_SLOT\_CONFIG\_NOMAC\_MASK** (0x01u << ATCA\_SLOT\_CONFIG\_NOMAC\_SHIFT)
- #define **ATCA\_SLOT\_CONFIG\_LIMITED\_USE\_SHIFT** (5)
- #define **ATCA\_SLOT\_CONFIG\_LIMITED\_USE\_MASK** (0x01u << ATCA\_SLOT\_CONFIG\_LIMITED\_USE\_SHIFT)
- #define **ATCA\_SLOT\_CONFIG\_ENC\_READ\_SHIFT** (6)
- #define **ATCA\_SLOT\_CONFIG\_ENC\_READ\_MASK** (0x01u << ATCA\_SLOT\_CONFIG\_ENC\_READ\_SHIFT)
- #define **ATCA\_SLOT\_CONFIG\_IS\_SECRET\_SHIFT** (7)
- #define **ATCA\_SLOT\_CONFIG\_IS\_SECRET\_MASK** (0x01u << ATCA\_SLOT\_CONFIG\_IS\_SECRET\_SHIFT)
- #define **ATCA\_SLOT\_CONFIG\_WRITE\_KEY\_SHIFT** (8)
- #define **ATCA\_SLOT\_CONFIG\_WRITE\_KEY\_MASK** ((uint32\_t)0x0Fu << ATCA\_SLOT\_CONFIG\_WRITE\_KEY\_SHIFT)
- #define **ATCA\_SLOT\_CONFIG\_WRITE\_KEY(v)** (ATCA\_SLOT\_CONFIG\_WRITE\_KEY\_MASK & (v << ATCA\_SLOT\_CONFIG\_WRITE\_KEY\_SHIFT))
- #define **ATCA\_SLOT\_CONFIG\_WRITE\_CONFIG\_SHIFT** (12)
- #define **ATCA\_SLOT\_CONFIG\_WRITE\_CONFIG\_MASK** (((uint32\_t)0x0Fu << ATCA\_SLOT\_CONFIG\_WRITE\_CONFIG\_SHIFT))
- #define **ATCA\_SLOT\_CONFIG\_WRITE\_CONFIG(v)** ((ATCA\_SLOT\_CONFIG\_WRITE\_CONFIG\_MASK & ((uint32\_t)(v) << ATCA\_SLOT\_CONFIG\_WRITE\_CONFIG\_SHIFT)))
- #define **ATCA\_SLOT\_CONFIG\_EXT\_SIG\_SHIFT** (0)
- #define **ATCA\_SLOT\_CONFIG\_EXT\_SIG\_MASK** (0x01u << ATCA\_SLOT\_CONFIG\_EXT\_SIG\_SHIFT)
- #define **ATCA\_SLOT\_CONFIG\_INT\_SIG\_SHIFT** (1)
- #define **ATCA\_SLOT\_CONFIG\_INT\_SIG\_MASK** (0x01u << ATCA\_SLOT\_CONFIG\_INT\_SIG\_SHIFT)
- #define **ATCA\_SLOT\_CONFIG\_ECDH\_SHIFT** (2)
- #define **ATCA\_SLOT\_CONFIG\_ECDH\_MASK** (0x01u << ATCA\_SLOT\_CONFIG\_ECDH\_SHIFT)
- #define **ATCA\_SLOT\_CONFIG\_WRITE\_ECDH\_SHIFT** (3)
- #define **ATCA\_SLOT\_CONFIG\_WRITE\_ECDH\_MASK** (0x01u << ATCA\_SLOT\_CONFIG\_WRITE\_ECDH\_SHIFT)
- #define **ATCA\_SLOT\_CONFIG\_GEN\_KEY\_SHIFT** (8)
- #define **ATCA\_SLOT\_CONFIG\_GEN\_KEY\_MASK** (0x01u << ATCA\_SLOT\_CONFIG\_GEN\_KEY\_SHIFT)
- #define **ATCA\_SLOT\_CONFIG\_PRIV\_WRITE\_SHIFT** (9)
- #define **ATCA\_SLOT\_CONFIG\_PRIV\_WRITE\_MASK** (0x01u << ATCA\_SLOT\_CONFIG\_PRIV\_WRITE\_SHIFT)
- #define **ATCA\_USE\_LOCK\_ENABLE\_SHIFT** (0)
- #define **ATCA\_USE\_LOCK\_ENABLE\_MASK** (0x0Fu << ATCA\_USE\_LOCK\_ENABLE\_SHIFT)
- #define **ATCA\_USE\_LOCK\_KEY\_SHIFT** (4)
- #define **ATCA\_USE\_LOCK\_KEY\_MASK** (0x0Fu << ATCA\_USE\_LOCK\_KEY\_SHIFT)
- #define **ATCA\_VOL\_KEY\_PERM\_SLOT\_SHIFT** (0)
- #define **ATCA\_VOL\_KEY\_PERM\_SLOT\_MASK** (0x0Fu << ATCA\_VOL\_KEY\_PERM\_SLOT\_SHIFT)
- #define **ATCA\_VOL\_KEY\_PERM\_SLOT(v)** (ATCA\_VOL\_KEY\_PERM\_SLOT\_MASK & (v << ATCA\_VOL\_KEY\_PERM\_SLOT\_SHIFT))
- #define **ATCA\_VOL\_KEY\_PERM\_EN\_SHIFT** (7)
- #define **ATCA\_VOL\_KEY\_PERM\_EN\_MASK** (0x01u << ATCA\_VOL\_KEY\_PERM\_EN\_SHIFT)
- #define **ATCA\_SECURE\_BOOT\_MODE\_SHIFT** (0)
- #define **ATCA\_SECURE\_BOOT\_MODE\_MASK** (0x03u << ATCA\_SECURE\_BOOT\_MODE\_SHIFT)
- #define **ATCA\_SECURE\_BOOT\_MODE(v)** (ATCA\_SECURE\_BOOT\_MODE\_MASK & (v << ATCA\_SECURE\_BOOT\_MODE\_SHIFT))
- #define **ATCA\_SECURE\_BOOT\_PERSIST\_EN\_SHIFT** (3)
- #define **ATCA\_SECURE\_BOOT\_PERSIST\_EN\_MASK** (0x01u << ATCA\_SECURE\_BOOT\_PERSIST\_EN\_SHIFT)

- `#define ATCA_SECURE_BOOT_RAND_NONCE_SHIFT (4)`
- `#define ATCA_SECURE_BOOT_RAND_NONCE_MASK (0x01u << ATCA_SECURE_BOOT_RAND_NONCE_SHIFT)`
- `#define ATCA_SECURE_BOOT_DIGEST_SHIFT (8)`
- `#define ATCA_SECURE_BOOT_DIGEST_MASK (0x0Fu << ATCA_SECURE_BOOT_DIGEST_SHIFT)`
- `#define ATCA_SECURE_BOOT_DIGEST(v) (ATCA_SECURE_BOOT_DIGEST_MASK & (v << ATCA_SECURE_BOOT_DIGEST_SHIFT))`
- `#define ATCA_SECURE_BOOT_PUB_KEY_SHIFT (12)`
- `#define ATCA_SECURE_BOOT_PUB_KEY_MASK (0x0Fu << ATCA_SECURE_BOOT_PUB_KEY_SHIFT)`
- `#define ATCA_SECURE_BOOT_PUB_KEY(v) (ATCA_SECURE_BOOT_PUB_KEY_MASK & (v << ATCA_SECURE_BOOT_PUB_KEY_SHIFT))`
- `#define ATCA_SLOT_LOCKED(v) ((0x01 << v) & 0xFFFFu)`
- `#define ATCA_CHIP_OPT_POST_EN_SHIFT (0)`
- `#define ATCA_CHIP_OPT_POST_EN_MASK (0x01u << ATCA_CHIP_OPT_POST_EN_SHIFT)`
- `#define ATCA_CHIP_OPT_IO_PROT_EN_SHIFT (1)`
- `#define ATCA_CHIP_OPT_IO_PROT_EN_MASK (0x01u << ATCA_CHIP_OPT_IO_PROT_EN_SHIFT)`
- `#define ATCA_CHIP_OPT_KDF_AES_EN_SHIFT (2)`
- `#define ATCA_CHIP_OPT_KDF_AES_EN_MASK (0x01u << ATCA_CHIP_OPT_KDF_AES_EN_SHIFT)`
- `#define ATCA_CHIP_OPT_ECDH_PROT_SHIFT (8)`
- `#define ATCA_CHIP_OPT_ECDH_PROT_MASK (0x03u << ATCA_CHIP_OPT_ECDH_PROT_SHIFT)`
- `#define ATCA_CHIP_OPT_ECDH_PROT(v) (ATCA_CHIP_OPT_ECDH_PROT_MASK & (v << ATCA_CHIP_OPT_ECDH_PROT_SHIFT))`
- `#define ATCA_CHIP_OPT_KDF_PROT_SHIFT (10)`
- `#define ATCA_CHIP_OPT_KDF_PROT_MASK (0x03u << ATCA_CHIP_OPT_KDF_PROT_SHIFT)`
- `#define ATCA_CHIP_OPT_KDF_PROT(v) (ATCA_CHIP_OPT_KDF_PROT_MASK & (v << ATCA_CHIP_OPT_KDF_PROT_SHIFT))`
- `#define ATCA_CHIP_OPT_IO_PROT_KEY_SHIFT (12)`
- `#define ATCA_CHIP_OPT_IO_PROT_KEY_MASK ((uint16_t)0x0Fu << ATCA_CHIP_OPT_IO_PROT_KEY_SHIFT)`
- `#define ATCA_CHIP_OPT_IO_PROT_KEY(v) (ATCA_CHIP_OPT_IO_PROT_KEY_MASK & (v << ATCA_CHIP_OPT_IO_PROT_KEY_SHIFT))`
- `#define ATCA_KEY_CONFIG_OFFSET(x) (96UL + (x) * 2u)`
- `#define ATCA_KEY_CONFIG_PRIVATE_SHIFT (0)`
- `#define ATCA_KEY_CONFIG_PRIVATE_MASK (0x01u << ATCA_KEY_CONFIG_PRIVATE_SHIFT)`
- `#define ATCA_KEY_CONFIG_PUB_INFO_SHIFT (1)`
- `#define ATCA_KEY_CONFIG_PUB_INFO_MASK (0x01u << ATCA_KEY_CONFIG_PUB_INFO_SHIFT)`
- `#define ATCA_KEY_CONFIG_KEY_TYPE_SHIFT (2)`
- `#define ATCA_KEY_CONFIG_KEY_TYPE_MASK ((0x07u << ATCA_KEY_CONFIG_KEY_TYPE_SHIFT))`
- `#define ATCA_KEY_CONFIG_KEY_TYPE(v) ((ATCA_KEY_CONFIG_KEY_TYPE_MASK & ((v) << ATCA_KEY_CONFIG_KEY_TYPE_SHIFT)))`
- `#define ATCA_KEY_CONFIG_LOCKABLE_SHIFT (5)`
- `#define ATCA_KEY_CONFIG_LOCKABLE_MASK (0x01u << ATCA_KEY_CONFIG_LOCKABLE_SHIFT)`
- `#define ATCA_KEY_CONFIG_REQ_RANDOM_SHIFT (6)`
- `#define ATCA_KEY_CONFIG_REQ_RANDOM_MASK (0x01u << ATCA_KEY_CONFIG_REQ_RANDOM_SHIFT)`
- `#define ATCA_KEY_CONFIG_REQ_AUTH_SHIFT (7)`
- `#define ATCA_KEY_CONFIG_REQ_AUTH_MASK (0x01u << ATCA_KEY_CONFIG_REQ_AUTH_SHIFT)`
- `#define ATCA_KEY_CONFIG_AUTH_KEY_SHIFT (8)`
- `#define ATCA_KEY_CONFIG_AUTH_KEY_MASK (0x0Fu << ATCA_KEY_CONFIG_AUTH_KEY_SHIFT)`
- `#define ATCA_KEY_CONFIG_AUTH_KEY(v) (ATCA_KEY_CONFIG_AUTH_KEY_MASK & (v << ATCA_KEY_CONFIG_AUTH_KEY_SHIFT))`
- `#define ATCA_KEY_CONFIG_PERSIST_DIS_SHIFT (12)`
- `#define ATCA_KEY_CONFIG_PERSIST_DIS_MASK (0x01u << ATCA_KEY_CONFIG_PERSIST_DIS_SHIFT)`

- #define **ATCA\_KEY\_CONFIG\_RFU\_SHIFT** (13)
- #define **ATCA\_KEY\_CONFIG\_RFU\_MASK** (0x01u << ATCA\_KEY\_CONFIG\_RFU\_SHIFT)
- #define **ATCA\_KEY\_CONFIG\_X509\_ID\_SHIFT** (14)
- #define **ATCA\_KEY\_CONFIG\_X509\_ID\_MASK** (0x03u << ATCA\_KEY\_CONFIG\_X509\_ID\_SHIFT)
- #define **ATCA\_KEY\_CONFIG\_X509\_ID(v)** (ATCA\_KEY\_CONFIG\_X509\_ID\_MASK & (v << ATCA\_KEY\_CONFIG\_X509\_ID\_SHIFT))

## Typedefs

- typedef struct [atca\\_sha256\\_ctx](#) **atca\_sha256\_ctx\_t**
- typedef [atca\\_sha256\\_ctx\\_t](#) **atca\_hmac\_sha256\_ctx\_t**
- typedef struct ATCA\_PACKED [atsha204a\\_config\\_s](#) **atsha204a\_config\_t**
- typedef struct ATCA\_PACKED [atecc508a\\_config\\_s](#) **atecc508a\_config\_t**
- typedef struct ATCA\_PACKED [atecc608\\_config\\_s](#) **atecc608\_config\_t**

## Functions

- ATCA\_STATUS [calib\\_wakeup\\_i2c](#) (ATCADevice device)  
*basic API methods are all prefixed with atcab\_ (CryptoAuthLib Basic) the fundamental premise of the basic API is it is based on a single interface instance and that instance is global, so all basic API commands assume that one global device is the one to operate on.*
- ATCA\_STATUS [calib\\_wakeup](#) (ATCADevice device)  
*wakeup the CryptoAuth device*
- ATCA\_STATUS [calib\\_idle](#) (ATCADevice device)  
*idle the CryptoAuth device*
- ATCA\_STATUS [calib\\_sleep](#) (ATCADevice device)  
*invoke sleep on the CryptoAuth device*
- ATCA\_STATUS [calib\\_exit](#) (ATCADevice device)  
*common cleanup code which idles the device after any operation*
- ATCA\_STATUS [calib\\_get\\_addr](#) (uint8\_t zone, uint16\_t slot, uint8\_t block, uint8\_t offset, uint16\_t \*addr)  
*Compute the address given the zone, slot, block, and offset.*
- ATCA\_STATUS [calib\\_get\\_zone\\_size](#) (ATCADevice device, uint8\_t zone, uint16\_t slot, size\_t \*size)  
*Gets the size of the specified zone in bytes.*
- ATCA\_STATUS [calib\\_ca2\\_get\\_addr](#) (uint8\_t zone, uint16\_t slot, uint8\_t block, uint8\_t offset, uint16\_t \*addr)  
*Compute the address given the zone, slot, block, and offset for the device.*
- ATCA\_STATUS **calib\_is\_locked** (ATCADevice device, uint8\_t zone, bool \*is\_locked)
- ATCA\_STATUS **calib\_is\_slot\_locked** (ATCADevice device, uint16\_t slot, bool \*is\_locked)
- ATCA\_STATUS [calib\\_ca2\\_is\\_locked](#) (ATCADevice device, uint8\_t zone, bool \*is\_locked)  
*Use Info command to check config/data is locked or not.*
- ATCA\_STATUS [calib\\_ca2\\_is\\_data\\_locked](#) (ATCADevice device, bool \*is\_locked)  
*Use Info command to check ECC204 Data zone lock status.*
- ATCA\_STATUS [calib\\_ca2\\_is\\_config\\_locked](#) (ATCADevice device, bool \*is\_locked)  
*Executes Read command, which reads the configuration zone to see if the specified slot is locked.*
- ATCADeviceType **calib\_get\_devicetype** (uint8\_t revision[4])  
*Parse the revision field to get the device type.*
- ATCADeviceType **calib\_get\_devicetype\_with\_device\_id** (uint8\_t device\_id, uint8\_t device\_revision)
- ATCA\_STATUS [calib\\_info\\_base](#) (ATCADevice device, uint8\_t mode, uint16\_t param2, uint8\_t \*out\_data)  
*Issues an Info command, which return internal device information and can control GPIO and the persistent latch.*
- ATCA\_STATUS [calib\\_info](#) (ATCADevice device, uint8\_t \*revision)  
*Use the Info command to get the device revision (DevRev).*
- ATCA\_STATUS [calib\\_info\\_privkey\\_valid](#) (ATCADevice device, uint16\_t key\_id, uint8\_t \*is\_valid)

Use Info command to check ECC Private key stored in key slot is valid or not.

- ATCA\_STATUS [calib\\_info\\_lock\\_status](#) (ATCADevice device, uint16\_t param2, uint8\_t \*is\_locked)

Use Info command to ECC204,TA010 config/data zone lock status.

- ATCA\_STATUS [calib\\_info\\_chip\\_status](#) (ATCADevice device, uint8\_t \*chip\_status)

Use Info command to get ECC204,TA010,SHA10x chip status.

### 19.7.1 Detailed Description

These methods provide a simple API to CryptoAuth chips.

### 19.7.2 Function Documentation

#### 19.7.2.1 calib\_ca2\_get\_addr()

```
ATCA_STATUS calib_ca2_get_addr (
    uint8_t zone,
    uint16_t slot,
    uint8_t block,
    uint8_t offset,
    uint16_t * addr )
```

Compute the address given the zone, slot, block, and offset for the device.

##### Parameters

in	zone	Zone to get address from. Config(1) or Data(0) which requires a slot.
in	slot	Slot Id number for data zone and zero for other zones.
in	block	Block number within the data zone .
in	offset	Aalways zero.
out	addr	Pointer to the address of data or configuration zone.

##### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.7.2.2 calib\_ca2\_is\_config\_locked()

```
ATCA_STATUS calib_ca2_is_config_locked (
    ATCADevice device,
    bool * is_locked )
```

Executes Read command, which reads the configuration zone to see if the specified slot is locked.

Parameters

in	<i>device</i>	Device context pointer
in	<i>slot</i>	Slot to query for locked (slot 0-15)
out	<i>is_locked</i>	Lock state returned here. True if locked.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Use Info command to check ECC204 Config zone lock status

Parameters

in	<i>device</i>	Device context pointer
out	<i>is_locked</i>	return lock status

Returns

ATCA\_SUCCESS on success, otherwise an error code

19.7.2.3 calib\_ca2\_is\_data\_locked()

```
ATCA_STATUS calib_ca2_is_data_locked (
    ATCADevice device,
    bool * is_locked )
```

Use Info command to check ECC204 Data zone lock status.

Parameters

in	<i>device</i>	Device context pointer
out	<i>is_locked</i>	return lock status

Returns

ATCA\_SUCCESS on success, otherwise an error code

19.7.2.4 calib\_ca2\_is\_locked()

```
ATCA_STATUS calib_ca2_is_locked (
    ATCADevice device,
    uint8_t zone,
    bool * is_locked )
```

Use Info command to check config/data is locked or not.

### Parameters

in	<i>device</i>	Device context pointer
in	<i>zone</i>	Config/Data zone
out	<i>is_locked</i>	return lock status here

### Returns

ATCA\_SUCCESS on success, otherwise an error code

#### 19.7.2.5 calib\_exit()

```
ATCA_STATUS calib_exit (  
    ATCADevice device )
```

common cleanup code which idles the device after any operation

### Parameters

in	<i>device</i>	Device context pointer
----	---------------	------------------------

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.7.2.6 calib\_get\_addr()

```
ATCA_STATUS calib_get_addr (  
    uint8_t zone,  
    uint16_t slot,  
    uint8_t block,  
    uint8_t offset,  
    uint16_t * addr )
```

Compute the address given the zone, slot, block, and offset.

### Parameters

in	<i>zone</i>	Zone to get address from. Config(0), OTP(1), or Data(2) which requires a slot.
in	<i>slot</i>	Slot Id number for data zone and zero for other zones.
in	<i>block</i>	Block number within the data or configuration or OTP zone .
in	<i>offset</i>	Offset Number within the block of data or configuration or OTP zone.
out	<i>addr</i>	Pointer to the address of data or configuration or OTP zone.



Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.7.2.7 calib\_get\_zone\_size()

```
ATCA_STATUS calib_get_zone_size (
    ATCADevice device,
    uint8_t zone,
    uint16_t slot,
    size_t * size )
```

Gets the size of the specified zone in bytes.

Parameters

in	device	Device context pointer
in	zone	Zone to get size information from. Config(0), OTP(1), or Data(2) which requires a slot.
in	slot	If zone is Data(2), the slot to query for size.
out	size	Zone size is returned here.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.7.2.8 calib\_idle()

```
ATCA_STATUS calib_idle (
    ATCADevice device )
```

idle the CryptoAuth device

Parameters

in	device	Device context pointer
----	--------	------------------------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.7.2.9 calib\_info()

```
ATCA_STATUS calib_info (
    ATCADevice device,
    uint8_t * revision )
```

Use the Info command to get the device revision (DevRev).

### Parameters

in	<i>device</i>	Device context pointer
out	<i>revision</i>	Device revision is returned here (4 bytes).

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.7.2.10 calib\_info\_base()

```
ATCA_STATUS calib_info_base (
    ATCADevice device,
    uint8_t mode,
    uint16_t param2,
    uint8_t * out_data )
```

Issues an Info command, which return internal device information and can control GPIO and the persistent latch.

### Parameters

in	<i>device</i>	Device context pointer
in	<i>mode</i>	Selects which mode to be used for info command.
in	<i>param2</i>	Selects the particular fields for the mode.
out	<i>out_data</i>	Response from info command (4 bytes). Can be set to NULL if not required.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.7.2.11 calib\_info\_chip\_status()

```
ATCA_STATUS calib_info_chip_status (
    ATCADevice device,
    uint8_t * chip_status )
```

Use Info command to get ECC204,TA010,SHA10x chip status.

### Parameters

in	<i>device</i>	Device context pointer
out	<i>chip_status</i>	return chip status here

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.7.2.12 calib\_info\_lock\_status()

```
ATCA_STATUS calib_info_lock_status (
    ATCADevice device,
    uint16_t param2,
    uint8_t * is_locked )
```

Use Info command to ECC204,TA010 config/data zone lock status.

Parameters

in	<i>device</i>	Device context pointer
in	<i>param2</i>	selects the zone and slot
out	<i>is_locked</i>	return lock status here

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.7.2.13 calib\_info\_privkey\_valid()

```
ATCA_STATUS calib_info_privkey_valid (
    ATCADevice device,
    uint16_t key_id,
    uint8_t * is_valid )
```

Use Info command to check ECC Private key stored in key slot is valid or not.

Parameters

in	<i>device</i>	Device context pointer
in	<i>key_id</i>	ECC private key slot id For ECC204,TA010 key_id is 0x00
out	<i>is_valid</i>	return private key is valid or invalid

Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.7.2.14 calib\_sleep()

```
ATCA_STATUS calib_sleep (
    ATCADevice device )
```

invoke sleep on the CryptoAuth device

#### Parameters

in	<i>device</i>	Device context pointer
----	---------------	------------------------

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.7.2.15 calib\_wakeup()

```
ATCA_STATUS calib_wakeup (
    ATCADevice device )
```

wakeup the CryptoAuth device

#### Parameters

in	<i>device</i>	Device context pointer
----	---------------	------------------------

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.7.2.16 calib\_wakeup\_i2c()

```
ATCA_STATUS calib_wakeup_i2c (
    ATCADevice device )
```

basic API methods are all prefixed with atcab\_ (CryptoAuthLib Basic) the fundamental premise of the basic API is it is based on a single interface instance and that instance is global, so all basic API commands assume that one global device is the one to operate on.

Drive the SDA pin low for wake up Set i2c device addr as 0U to drive SDA low

I2C general call should not interpreted as an addr write

Set the i2c device address

## 19.8 Software crypto methods (atcac\_)

These methods provide a software implementation of various crypto algorithms.

### 19.8.0.1 crypto directory - Purpose

This directory contains software implementations of cryptographic functions. The functions at the base level are wrappers that will point to the final implementations of the software crypto functions.

### Functions

- ATCA\_STATUS **atcac\_sw\_sha1** (const uint8\_t \*data, size\_t data\_size, uint8\_t digest[(20U)])
- ATCA\_STATUS **atcac\_sw\_sha2\_256** (const uint8\_t \*data, size\_t data\_size, uint8\_t digest[(32U)])
- ATCA\_STATUS **atcac\_sha256\_hmac\_ctr\_iteration** (struct [atcac\\_hmac\\_ctx](#) \*ctx, uint8\_t iteration, uint16\_t length, const uint8\_t \*label, size\_t label\_len, const uint8\_t \*data, size\_t data\_len, uint8\_t digest[(32U)])
- ATCA\_STATUS **atcac\_sha256\_hmac\_counter** (uint8\_t \*key, size\_t key\_len, const uint8\_t \*label, size\_t label\_len, const uint8\_t \*data, size\_t data\_len, uint8\_t \*digest, size\_t diglen)

### 19.8.1 Detailed Description

These methods provide a software implementation of various crypto algorithms.

## 19.9 Hardware abstraction layer (hal\_)

These methods define the hardware abstraction layer for communicating with a CryptoAuth device.

### 19.9.0.1 HAL Directory - Purpose

This directory contains all the Hardware Abstraction Layer (HAL) files used to adapt the upper levels of atca-ng and abstractions to physical hardware.

HAL contains physical implementations for I2C, SWI, SPI, UART and timers for specific hardware platforms.

**Include just those HAL files you require based on platform type.**

### 19.9.1 Cryptoauthlib HAL Architecture

Cryptoauthlib has several intermediate conceptual layers

1. The highest layer of cryptoauthlib (outside of integration APIS) that may be used with an application is the `atcab_` api functions. These are general purpose functions that present a simple and consistent crypto interface to the application regardless of the device being used.
2. `calib_`, `talib_` APIs are the library functions behind `atcab_` ones that generate the correct command packets and process the received responses. Device specific logic is handled by the library here
3. `hal_` these functions perform the transmit/recieve of data for a given interface. These are split into sublayers
  - The HAL layer is the first hal layer that presents the interface expected by the higher level library. When using a native driver and no further interpretation is required this layer is all that is required.
  - The PHY layer if for hals that perform an interpretation or additional protocol logic. In this situation the HAL performs protocol interpretation while the phy performs the physical communication

**19.9.1.0.1 HAL and PHY Requirements** The hal and phy layers have the same construction. A hal or phy must have the following functions and their signatures

- `ATCA_STATUS hal_<name>init(ATCAIface iface, ATCAIfaceCfg *cfg);`
- `ATCA_STATUS hal_<name>post_init(ATCAIface iface);`
- `ATCA_STATUS hal_<name>send(ATCAIface iface, uint8_t address, uint8_t *txdata, int txlength);`
- `ATCA_STATUS hal_<name>receive(ATCAIface iface, uint8_t address, uint8_t *rxdata, uint16_t *rxlength);`
- `ATCA_STATUS hal_<name>control(ATCAIface iface, uint8_t option, void* param, size_t paramlen);`
- `ATCA_STATUS hal_<name>_release(void *hal_data);`

If the hal is a native driver no phy is required. See the tables below for which hal is required to be ported based on a configured interface

### 19.9.2 CryptoAuthLib Supported HAL Layers

Device Interface	Physical Interface	HAL	PHY
i2c	i2c	hal_i2c	
	gpio	hal_i2c_gpio	hal_gpio
spi	spi	hal_spi	
swi	uart	hal_swi	hal_uart
	gpio	hal_swi_gpio	hal_gpio
any	uart	kit	hal_uart
	hid	kit	hal_hid
	any (user provided)	kit_bridge	

#### 19.9.2.1 Microchip Harmony 3 for all PIC32 & ARM products - Use the Harmony 3 Configurator to generate and configure projects

Obtain library and configure using [Harmony 3](#)

Interface	Files	API	Notes
I2C	<a href="#">hal_i2c_harmony.c</a>	plib.↔ h	For all Harmony 3 based projects
SPI	<a href="#">hal_spi_harmony.c</a>	plib.↔ h	
UART	<a href="#">hal_uart_harmony.c</a>	plib.↔ h	

#### 19.9.2.2 Microchip 8 & 16 bit products - AVR, PIC16/18, PIC24/DSPIC

Obtain library and integration through [Microchip Code Configurator](#)

#### 19.9.2.3 OS & RTOS integrations

Use [CMake](#) to configure the library in Linux, Windows, and MacOS environments

OS	Interface	Files	API	Notes
Linux	I2C	<a href="#">hal_linux_i2c_userspace.c/h</a>	i2c-dev	
Linux	SPI	<a href="#">hal_linux_spi_userspace.c/h</a>	spidev	
Linux/Mac		<a href="#">hal_linux.c</a>		For all Linux/Mac projects
Windows		<a href="#">hal_windows.c</a>		For all Windows projects
All	kit-hid	<a href="#">hal_all_platforms_kit_hidapi.c/h</a>	hidapi	Works for Windows, Linux, and Mac
freeRTOS		<a href="#">hal_freertos.c</a>		freeRTOS common routines

#### 19.9.2.4 Legacy Support - [Atmel START](https://www.microchip.com/start) for AVR, ARM based processors (SAM)

Interface	Files	API	Notes
	<a href="#">hal_timer_start.c</a>	START	Timer implementation
I2C	<a href="#">hal_i2c_start.c/h</a>	START	
SWI	<a href="#">swi_uart_start.c/h</a>	START	SWI using UART

#### 19.9.2.5 Legacy Support - ASF3 for ARM Cortex-m0 & Cortex-m based processors (SAM)

SAM Micros	Interface	Files	API	Notes
cortex-m0	I2C	<a href="#">hal_sam0_i2c_asf.c/h</a>	ASF3	SAMD21, SAMB11, etc
cortex-m3/4/7	I2C	<a href="#">hal_sam_i2c_asf.c/h</a>	ASF3	SAM4S, SAMG55, SAMV71, etc
all		<a href="#">hal_sam_timer_asf.c</a>	ASF3	Common timer hal for all platforms

## Data Structures

- struct [atca\\_hal\\_kit\\_phy\\_t](#)
- struct [atca\\_hal\\_shm\\_t](#)
- struct [i2c\\_start\\_instance](#)
- struct [atca\\_i2c\\_host\\_s](#)
- struct [i2c\\_sam\\_instance](#)
- struct [atcal2Cmaster](#)

*this is the hal\_data for ATCA HAL for ASF SERCOM*

- struct [atcaSWImaster](#)

*this is the hal\_data for ATCA HAL for ASF SERCOM*

## Macros

- #define **ATCA\_POLLING\_INIT\_TIME\_MSEC** 1
- #define **ATCA\_POLLING\_FREQUENCY\_TIME\_MSEC** 2
- #define **ATCA\_POLLING\_MAX\_TIME\_MSEC** 2500
- #define **ATCA\_HAL\_CONTROL\_WAKE** (0U)  
*Execute the hardware specific wake - generally only for kits.*
- #define **ATCA\_HAL\_CONTROL\_IDLE** (1U)  
*Execute the hardware specific idle - generally only for kits.*
- #define **ATCA\_HAL\_CONTROL\_SLEEP** (2U)  
*Execute the hardware specific sleep - generally only for kits.*
- #define **ATCA\_HAL\_CONTROL\_RESET** (3U)

*Execute the hardware specific reset - generally only for kits.*

- **#define ATCA\_HAL\_CONTROL\_SELECT** (4U)  
*Select the device - assert CS, open device, etc.*
- **#define ATCA\_HAL\_CONTROL\_DESELECT** (5U)  
*Select the device - de-assert CS, release device, etc.*
- **#define ATCA\_HAL\_CHANGE\_BAUD** (6U)  
*Change the datarate of the phy.*
- **#define ATCA\_HAL\_FLUSH\_BUFFER** (7U)  
*If the phy has a buffer make sure all bytes are transmitted.*
- **#define ATCA\_HAL\_CONTROL\_DIRECTION** (8U)  
*Set the PIN mode (in vs out)*
- **#define MAX\_I2C\_BUSES** 3
- **#define KIT\_MAX\_SCAN\_COUNT** 8
- **#define KIT\_MAX\_TX\_BUF** 32
- **#define KIT\_TX\_WRAP\_SIZE** (10)
- **#define KIT\_MSG\_SIZE** (32u)
- **#define KIT\_RX\_WRAP\_SIZE** (KIT\_MSG\_SIZE + 6u)
- **#define MAX\_SWI\_BUSES** 6
- **#define RECEIVE\_MODE** 0
- **#define TRANSMIT\_MODE** 1
- **#define RX\_DELAY** 10
- **#define TX\_DELAY** 90
- **#define DEBUG\_PIN\_1** EXT2\_PIN\_5
- **#define DEBUG\_PIN\_2** EXT2\_PIN\_6
- **#define MAX\_SWI\_BUSES** 6
- **#define RECEIVE\_MODE** 0
- **#define TRANSMIT\_MODE** 1
- **#define RX\_DELAY** 10
- **#define TX\_DELAY** 93

## Typedefs

- **typedef void \* hal\_mutex\_t**  
*Generic mutex type definition for most systems.*
- **typedef void(\* start\_change\_baudrate)** (ATCAIface iface, uint32\_t speed)
- **typedef struct i2c\_start\_instance i2c\_start\_instance\_t**
- **typedef struct atca\_i2c\_host\_s atca\_i2c\_host\_t**
- **typedef void(\* sam\_change\_baudrate)** (ATCAIface iface, uint32\_t speed)
- **typedef struct i2c\_sam\_instance i2c\_sam\_instance\_t**
- **typedef struct atcal2Cmaster ATCAI2CMaster\_t**  
*this is the hal\_data for ATCA HAL for ASF SERCOM*
- **typedef struct atcaswimaster ATCASWIMaster\_t**  
*this is the hal\_data for ATCA HAL for ASF SERCOM*
- **typedef struct atcaswimaster ATCASWIMaster\_t**  
*this is the hal\_data for ATCA HAL for ASF SERCOM*



## Functions

- ATCA\_STATUS [hal\\_iface\\_init](#) (ATCAIfaceCfg \*cfg, ATCAHAL\_t \*\*hal, ATCAHAL\_t \*\*phy)  
*Standard HAL API for ATCA to initialize a physical interface.*
- ATCA\_STATUS [hal\\_iface\\_release](#) (ATCAIfaceType iface\_type, void \*hal\_data)  
*releases a physical interface, HAL knows how to interpret hal\_data*
- ATCA\_STATUS [hal\\_check\\_wake](#) (const uint8\_t \*response, int response\_size)  
*Utility function for hal\_wake to check the reply.*
- void [atca\\_delay\\_ms](#) (uint32\_t ms)  
*Timer API for legacy implementations.*
- void [atca\\_delay\\_us](#) (uint32\_t delay)  
*This function delays for a number of microseconds.*
- void [hal\\_delay\\_ms](#) (uint32\_t delay)  
*Timer API implemented at the HAL level.*
- void [hal\\_delay\\_us](#) (uint32\_t delay)  
*This function delays for a number of microseconds.*
- ATCA\_STATUS [hal\\_create\\_mutex](#) (void \*\*ppMutex, const char \*pName)  
*Optional hal interfaces.*
- ATCA\_STATUS [hal\\_init\\_mutex](#) (void \*pMutex, bool shared)
- ATCA\_STATUS [hal\\_destroy\\_mutex](#) (void \*pMutex)
- ATCA\_STATUS [hal\\_lock\\_mutex](#) (void \*pMutex)
- ATCA\_STATUS [hal\\_unlock\\_mutex](#) (void \*pMutex)
- ATCA\_STATUS [hal\\_alloc\\_shared](#) (void \*\*pShared, size\_t size, const char \*pName, bool \*initialized)
- ATCA\_STATUS [hal\\_free\\_shared](#) (void \*pShared, size\_t size)
- ATCA\_STATUS [hal\\_iface\\_register\\_hal](#) (ATCAIfaceType iface\_type, ATCAHAL\_t \*hal, ATCAHAL\_t \*\*old\_hal, ATCAHAL\_t \*phy, ATCAHAL\_t \*\*old\_phy)  
*Register/Replace a HAL with a.*
- uint8\_t [hal\\_is\\_command\\_word](#) (uint8\_t word\_address)  
*Utility function for hal\_wake to check the reply.*
- ATCA\_STATUS [hal\\_kit\\_hid\\_init](#) (ATCAIface iface, ATCAIfaceCfg \*cfg)  
*HAL implementation of Kit USB HID init.*
- ATCA\_STATUS [hal\\_kit\\_hid\\_post\\_init](#) (ATCAIface iface)  
*HAL implementation of Kit HID post init.*
- ATCA\_STATUS [hal\\_kit\\_hid\\_send](#) (ATCAIface iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*HAL implementation of kit protocol send over USB HID.*
- ATCA\_STATUS [hal\\_kit\\_hid\\_receive](#) (ATCAIface iface, uint8\_t word\_address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*HAL implementation of send over USB HID.*
- ATCA\_STATUS [hal\\_kit\\_hid\\_control](#) (ATCAIface iface, uint8\_t option, void \*param, size\_t paramlen)  
*Perform control operations for the kit protocol.*
- ATCA\_STATUS [hal\\_kit\\_hid\\_release](#) (void \*hal\_data)  
*Close the physical port for HID.*
- void \* [hal\\_malloc](#) (size\_t size)
- void [hal\\_free](#) (void \*ptr)
- void [hal\\_rtos\\_delay\\_ms](#) (uint32\_t delay)  
*This function delays for a number of milliseconds.*
- ATCA\_STATUS [hal\\_i2c\\_discover\\_buses](#) (int i2c\_buses[], int max\_buses)  
*discover i2c buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-prior knowledge*
- ATCA\_STATUS [hal\\_i2c\\_discover\\_devices](#) (int bus\_num, ATCAIfaceCfg cfg[], int \*found)  
*discover any CryptoAuth devices on a given logical bus number*
- ATCA\_STATUS [hal\\_i2c\\_init](#) (ATCAIface iface, ATCAIfaceCfg \*cfg)

*hal\_i2c\_init* manages requests to initialize a physical interface. it manages use counts so when an interface has released the physical layer, it will disable the interface for some other use. You can have multiple ATCAIFace instances using the same bus, and you can have multiple ATCAIFace instances on multiple i2c buses, so *hal\_i2c\_init* manages these things and ATCAIFace is abstracted from the physical details.

- ATCA\_STATUS [hal\\_i2c\\_post\\_init](#) (ATCAIFace iface)  
HAL implementation of I2C post init.
- ATCA\_STATUS [hal\\_i2c\\_send](#) (ATCAIFace iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
HAL implementation of I2C send over START.
- ATCA\_STATUS [hal\\_i2c\\_receive](#) (ATCAIFace iface, uint8\_t address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
HAL implementation of I2C receive function for START I2C.
- ATCA\_STATUS [change\\_i2c\\_speed](#) (ATCAIFace iface, uint32\_t speed)  
method to change the bus speed of I2C
- ATCA\_STATUS [hal\\_i2c\\_control](#) (ATCAIFace iface, uint8\_t option, void \*param, size\_t paramlen)  
Perform control operations for the kit protocol.
- ATCA\_STATUS [hal\\_i2c\\_release](#) (void \*hal\_data)  
manages reference count on given bus and releases resource if no more references exist
- ATCA\_STATUS [hal\\_i2c\\_init](#) (void \*hal, ATCAIFaceCfg \*cfg)  
*hal\_i2c\_init* manages requests to initialize a physical interface. it manages use counts so when an interface has released the physical layer, it will disable the interface for some other use. You can have multiple ATCAIFace instances using the same bus, and you can have multiple ATCAIFace instances on multiple i2c buses, so *hal\_i2c\_init* manages these things and ATCAIFace is abstracted from the physical details.
- ATCA\_STATUS [hal\\_i2c\\_wake](#) (ATCAIFace iface)  
wake up CryptoAuth device using I2C bus
- ATCA\_STATUS [hal\\_i2c\\_idle](#) (ATCAIFace iface)  
idle CryptoAuth device using I2C bus
- ATCA\_STATUS [hal\\_i2c\\_sleep](#) (ATCAIFace iface)  
sleep CryptoAuth device using I2C bus
- ATCA\_STATUS [hal\\_kit\\_attach\\_phy](#) (ATCAIFaceCfg \*cfg, atca\_hal\_kit\_phy\_t \*phy)  
Helper function that connects a physical layer context structure that will be used by the kit protocol bridge.
- ATCA\_STATUS [hal\\_kit\\_init](#) (ATCAIFace iface, ATCAIFaceCfg \*cfg)  
HAL implementation of Kit USB HID init.
- ATCA\_STATUS [hal\\_kit\\_post\\_init](#) (ATCAIFace iface)  
HAL implementation of Kit HID post init.
- ATCA\_STATUS [hal\\_kit\\_send](#) (ATCAIFace iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
HAL implementation of kit protocol send over USB HID.
- ATCA\_STATUS [hal\\_kit\\_receive](#) (ATCAIFace iface, uint8\_t word\_address, uint8\_t \*rxdata, uint16\_t \*rxsize)  
HAL implementation of send over USB HID.
- ATCA\_STATUS [hal\\_kit\\_control](#) (ATCAIFace iface, uint8\_t option, void \*param, size\_t paramlen)  
Kit Protocol Control.
- ATCA\_STATUS [hal\\_kit\\_release](#) (void \*hal\_data)  
Close the physical port for HID.
- ATCA\_STATUS [hal\\_check\\_pid](#) (hal\_pid\_t pid)  
Check if the pid exists in the system.
- void [atca\\_delay\\_10us](#) (uint32\_t delay)  
This function delays for a number of tens of microseconds.
- ATCA\_STATUS [hal\\_spi\\_discover\\_buses](#) (int spi\_buses[], int max\_buses)  
discover spi buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-priori knowledge
- ATCA\_STATUS [hal\\_spi\\_discover\\_devices](#) (int bus\_num, ATCAIFaceCfg cfg[], int \*found)  
discover any TA10x devices on a given logical bus number
- ATCA\_STATUS [hal\\_spi\\_init](#) (ATCAIFace iface, ATCAIFaceCfg \*cfg)  
initialize an SPI interface using given config

- ATCA\_STATUS [hal\\_spi\\_post\\_init](#) (ATCAIface iface)  
*HAL implementation of SPI post init.*
- ATCA\_STATUS [hal\\_spi\\_select](#) (ATCAIface iface)  
*HAL implementation to assert the device chip select.*
- ATCA\_STATUS [hal\\_spi\\_deselect](#) (ATCAIface iface)  
*HAL implementation to deassert the device chip select.*
- ATCA\_STATUS [hal\\_spi\\_send](#) (ATCAIface iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*HAL implementation of SPI send over Harmony.*
- ATCA\_STATUS [hal\\_spi\\_receive](#) (ATCAIface iface, uint8\_t word\_address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*HAL implementation of SPI receive function for HARMONY SPI.*
- ATCA\_STATUS [hal\\_spi\\_control](#) (ATCAIface iface, uint8\_t option, void \*param, size\_t paramlen)  
*Perform control operations for the kit protocol.*
- ATCA\_STATUS [hal\\_spi\\_release](#) (void \*hal\_data)  
*manages reference count on given bus and releases resource if no more references exist*
- ATCA\_STATUS [hal\\_swi\\_init](#) (ATCAIface iface, ATCAIfaceCfg \*cfg)  
*initialize an SWI interface using given config*
- ATCA\_STATUS [hal\\_swi\\_post\\_init](#) (ATCAIface iface)  
*HAL implementation of SWI post init.*
- ATCA\_STATUS [hal\\_swi\\_send](#) (ATCAIface iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*HAL implementation of SWI send command over UART.*
- ATCA\_STATUS [hal\\_swi\\_receive](#) (ATCAIface iface, uint8\_t word\_address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*HAL implementation of SWI receive function over UART.*
- ATCA\_STATUS [hal\\_swi\\_wake](#) (ATCAIface iface)  
*Send Wake flag via SWI.*
- ATCA\_STATUS [hal\\_swi\\_sleep](#) (ATCAIface iface)  
*Send Sleep flag via SWI.*
- ATCA\_STATUS [hal\\_swi\\_idle](#) (ATCAIface iface)  
*Send Idle flag via SWI.*
- ATCA\_STATUS [hal\\_swi\\_control](#) (ATCAIface iface, uint8\_t option, void \*param, size\_t paramlen)  
*Perform control operations for the kit protocol.*
- ATCA\_STATUS [hal\\_swi\\_release](#) (void \*hal\_data)  
*manages reference count on given bus and releases resource if no more references exist*
- const char \* [kit\\_id\\_from\\_devtype](#) (ATCADeviceType devtype)
- const char \* [kit\\_interface\\_from\\_kittype](#) (ATCAKitType kittype)
- const char \* [kit\\_interface](#) (ATCAKitType kittype)
- ATCA\_STATUS [kit\\_init](#) (ATCAIface iface, ATCAIfaceCfg \*cfg)
- ATCA\_STATUS [kit\\_post\\_init](#) (ATCAIface iface)
- ATCA\_STATUS [kit\\_send](#) (ATCAIface iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)
- ATCA\_STATUS [kit\\_receive](#) (ATCAIface iface, uint8\_t word\_address, uint8\_t \*rxdata, uint16\_t \*rxsize)
- ATCA\_STATUS [kit\\_control](#) (ATCAIface iface, uint8\_t option, void \*param, size\_t paramlen)
- ATCA\_STATUS [kit\\_release](#) (void \*hal\_data)
- ATCA\_STATUS [kit\\_wrap\\_cmd](#) (ATCAIface iface, uint8\_t word\_address, const uint8\_t \*txdata, int txlen, char \*pkitcmd, int \*nkitcmd)
- ATCA\_STATUS [kit\\_parse\\_rsp](#) (const char \*pkitbuf, int nkitbuf, uint8\_t \*kitstatus, uint8\_t \*rxdata, int \*datasize)
- ATCA\_STATUS [kit\\_wake](#) (ATCAIface iface)
- ATCA\_STATUS [kit\\_idle](#) (ATCAIface iface)
- ATCA\_STATUS [kit\\_sleep](#) (ATCAIface iface)
- ATCA\_STATUS [kit\\_phy\\_send](#) (ATCAIface iface, uint8\_t \*txdata, int txlength)
- ATCA\_STATUS [kit\\_phy\\_receive](#) (ATCAIface iface, uint8\_t \*rxdata, int \*rxsize)
- ATCA\_STATUS [swi\\_uart\\_init](#) (ATCASWIMaster\_t \*instance)  
*Implementation of SWI UART init.*

- ATCA\_STATUS [swi\\_uart\\_deinit](#) ([ATCASWIMaster\\_t](#) \*instance)  
*Implementation of SWI UART deinit.*
- void [swi\\_uart\\_setbaud](#) ([ATCASWIMaster\\_t](#) \*instance, uint32\_t baudrate)  
*implementation of SWI UART change baudrate.*
- void [swi\\_uart\\_mode](#) ([ATCASWIMaster\\_t](#) \*instance, uint8\_t mode)  
*implementation of SWI UART change mode.*
- void [swi\\_uart\\_discover\\_buses](#) (int swi\_uart\_buses[], int max\_buses)  
*discover UART buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-priori knowledge*
- ATCA\_STATUS [swi\\_uart\\_send\\_byte](#) ([ATCASWIMaster\\_t](#) \*instance, uint8\_t data)  
*HAL implementation of SWI UART send byte over ASF. This function send one byte over UART.*
- ATCA\_STATUS [swi\\_uart\\_receive\\_byte](#) ([ATCASWIMaster\\_t](#) \*instance, uint8\_t \*data)  
*HAL implementation of SWI UART receive bytes over ASF. This function receive one byte over UART.*

### Variables

- struct port\_config **pin\_conf**

### 19.9.3 Detailed Description

These methods define the hardware abstraction layer for communicating with a CryptoAuth device.

These methods define the hardware abstraction layer for communicating with a CryptoAuth device using SWI Interface.

These methods define the hardware abstraction layer for communicating with a TA10x device.

< Uncomment when debugging

These methods define the hardware abstraction layer for communicating with a CryptoAuth device using I2C driver of ASF.

### 19.9.4 Macro Definition Documentation

#### 19.9.4.1 MAX\_SWI\_BUSES [1/2]

```
#define MAX_SWI_BUSES 6
```

- this HAL implementation assumes you've included the ASF SERCOM UART libraries in your project, otherwise, the HAL layer will not compile because the ASF UART drivers are a dependency \*

19.9.4.2 MAX\_SWI\_BUSES [2/2]

```
#define MAX_SWI_BUSES 6
```

- this HAL implementation assumes you've included the ASF SERCOM UART libraries in your project, otherwise, the HAL layer will not compile because the ASF UART drivers are a dependency \*

19.9.5 Function Documentation

19.9.5.1 atca\_delay\_10us()

```
void atca_delay_10us (
    uint32_t delay )
```

This function delays for a number of tens of microseconds.

Parameters

in	<i>delay</i>	number of 0.01 milliseconds to delay
----	--------------	--------------------------------------

Parameters

in	<i>delay</i>	number of 0.01 milliseconds to delay
----	--------------	--------------------------------------

19.9.5.2 atca\_delay\_ms()

```
void atca_delay_ms (
    uint32_t delay )
```

Timer API for legacy implementations.

This function delays for a number of milliseconds.

You can override this function if you like to do something else in your system while delaying.

Parameters

in	<i>delay</i>	number of milliseconds to delay
----	--------------	---------------------------------

You can override this function if you like to do something else in your system while delaying.

### Parameters

in	<i>delay</i>	number of milliseconds to delay
----	--------------	---------------------------------

### 19.9.5.3 atca\_delay\_us()

```
void atca_delay_us (
    uint32_t delay )
```

This function delays for a number of microseconds.

### Parameters

in	<i>delay</i>	number of 0.001 milliseconds to delay
----	--------------	---------------------------------------

### Parameters

in	<i>delay</i>	number of microseconds to delay
----	--------------	---------------------------------

### Parameters

in	<i>delay</i>	number of 0.001 milliseconds to delay
----	--------------	---------------------------------------

### 19.9.5.4 change\_i2c\_speed()

```
ATCA_STATUS change_i2c_speed (
    ATCAIface iface,
    uint32_t speed )
```

method to change the bus speed of I2C

method to change the bus speed of I2C

### Parameters

in	<i>iface</i>	interface on which to change bus speed
in	<i>speed</i>	baud rate (typically 100000 or 400000)
in	<i>iface</i>	interface on which to change bus speed
in	<i>speed</i>	baud rate (typically 100000 or 400000)

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.9.5.5 hal\_check\_wake()

```
ATCA_STATUS hal_check_wake (
    const uint8_t * response,
    int response_size )
```

Utility function for hal\_wake to check the reply.

Parameters

in	<i>response</i>	Wake response to be checked.
in	<i>response_size</i>	Size of the response to check.

Returns

ATCA\_SUCCESS for expected wake, ATCA\_STATUS\_SELFTEST\_ERROR if the power on self test failed, ATCA\_WAKE\_FAILED for other failures.

19.9.5.6 hal\_create\_mutex()

```
ATCA_STATUS hal_create_mutex (
    void ** ppMutex,
    const char * pName )
```

Optional hal interfaces.

Application callback for creating a mutex object.

Parameters

in, out	<i>ppMutex</i>	location to receive ptr to mutex
in, out	<i>pName</i>	String used to identify the mutex
	<i>[IN/OUT]</i>	ppMutex location to receive ptr to mutex
	<i>[IN]</i>	pName Name of the mutex for systems using named objects

19.9.5.7 hal\_delay\_ms()

```
void hal_delay_ms (
    uint32_t delay )
```

Timer API implemented at the HAL level.

This function delays for a number of milliseconds.

### Parameters

in	<i>delay</i>	number of milliseconds to delay
----	--------------	---------------------------------

You can override this function if you like to do something else in your system while delaying.

### Parameters

in	<i>delay</i>	number of milliseconds to delay
----	--------------	---------------------------------

### 19.9.5.8 hal\_delay\_us()

```
void hal_delay_us (
    uint32_t delay )
```

This function delays for a number of microseconds.

### Parameters

in	<i>delay</i>	number of microseconds to delay
----	--------------	---------------------------------

### Parameters

in	<i>delay</i>	number of microseconds to delay
----	--------------	---------------------------------

### 19.9.5.9 hal\_i2c\_control()

```
ATCA_STATUS hal_i2c_control (
    ATCAIface iface,
    uint8_t option,
    void * param,
    size_t paramlen )
```

Perform control operations for the kit protocol.

### Parameters

in	<i>iface</i>	Interface to interact with.
in	<i>option</i>	Control parameter identifier
in	<i>param</i>	Optional pointer to parameter value
in	<i>paramlen</i>	Length of the parameter



Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.9.5.10 hal\_i2c\_discover\_buses()

```
ATCA_STATUS hal_i2c_discover_buses (
    int i2c_buses[],
    int max_buses )
```

discover i2c buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-prior knowledge

This HAL implementation assumes you've included the ASF TWI libraries in your project, otherwise, the HAL layer will not compile because the ASF TWI drivers are a dependency.

logical to physical bus mapping structure

discover i2c buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-priori knowledge

Parameters

in	<i>i2c_buses</i>	- an array of logical bus numbers
in	<i>max_buses</i>	- maximum number of buses the app wants to attempt to discover

Returns

ATCA\_SUCCESS

discover i2c buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-priori knowledge

Parameters

in	<i>i2c_buses</i>	- an array of logical bus numbers
in	<i>max_buses</i>	- maximum number of buses the app wants to attempt to discover

Returns

ATCA\_SUCCESS

discover i2c buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-priori knowledge

Parameters

in	<i>i2c_buses</i>	- an array of logical bus numbers
in	<i>max_buses</i>	- maximum number of buses the app wants to attempt to discover return ATCA_SUCCESS

### 19.9.5.11 hal\_i2c\_discover\_devices()

```
ATCA_STATUS hal_i2c_discover_devices (
    int bus_num,
    ATCAIfaceCfg cfg[],
    int * found )
```

discover any CryptoAuth devices on a given logical bus number

#### Parameters

in	<i>bus_num</i>	logical bus number on which to look for CryptoAuth devices
out	<i>cfg</i>	pointer to head of an array of interface config structures which get filled in by this method
out	<i>found</i>	number of devices found on this bus

#### Returns

ATCA\_SUCCESS

#### Parameters

in	<i>bus_num</i>	- logical bus number on which to look for CryptoAuth devices
out	<i>cfg[]</i>	- pointer to head of an array of interface config structures which get filled in by this method
out	<i>*found</i>	- number of devices found on this bus

#### Returns

ATCA\_SUCCESS

#### Parameters

in	<i>bus_num</i>	Logical bus number on which to look for CryptoAuth devices
out	<i>cfg</i>	Pointer to head of an array of interface config structures which get filled in by this method
out	<i>found</i>	Number of devices found on this bus

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.9.5.12 hal\_i2c\_idle()

```
ATCA_STATUS hal_i2c_idle (
    ATCAIface iface )
```

idle CryptoAuth device using I2C bus

Parameters

in	<i>iface</i>	interface to logical device to idle
----	--------------	-------------------------------------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>iface</i>	interface to logical device to idle
----	--------------	-------------------------------------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.9.5.13 hal\_i2c\_init() [1/2]

```
ATCA_STATUS hal_i2c_init (
    ATCAIFace iface,
    ATCAIFaceCfg * cfg )
```

hal\_i2c\_init manages requests to initialize a physical interface. it manages use counts so when an interface has released the physical layer, it will disable the interface for some other use. You can have multiple ATCAIFace instances using the same bus, and you can have multiple ATCAIFace instances on multiple i2c buses, so hal\_i2c\_init manages these things and ATCAIFace is abstracted from the physical details.

HAL implementation of I2C init.

- this HAL implementation assumes you've included the START Twi libraries in your project, otherwise, the HAL layer will not compile because the START TWI drivers are a dependency \*

initialize an I2C interface using given config

Parameters

in	<i>hal</i>	- opaque ptr to HAL data
in	<i>cfg</i>	- interface configuration

Returns

ATCA\_SUCCESS on success, otherwise an error code.

this implementation assumes I2C peripheral has been enabled by user. It only initialize an I2C interface using given config.

### Parameters

in	<i>hal</i>	pointer to HAL specific data that is maintained by this HAL
in	<i>cfg</i>	pointer to HAL specific configuration data that is used to initialize this HAL

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.9.5.14 hal\_i2c\_init() [2/2]

```
ATCA_STATUS hal_i2c_init (
    void * hal,
    ATCAIFaceCfg * cfg )
```

hal\_i2c\_init manages requests to initialize a physical interface. it manages use counts so when an interface has released the physical layer, it will disable the interface for some other use. You can have multiple ATCAIFace instances using the same bus, and you can have multiple ATCAIFace instances on multiple i2c buses, so hal\_i2c\_init manages these things and ATCAIFace is abstracted from the physical details.

hal\_i2c\_init manages requests to initialize a physical interface. It manages use counts so when an interface has released the physical layer, it will disable the interface for some other use. You can have multiple ATCAIFace instances using the same bus, and you can have multiple ATCAIFace instances on multiple i2c buses, so hal\_i2c\_init manages these things and ATCAIFace is abstracted from the physical details.

initialize an I2C interface using given config

- this HAL implementation assumes you've included the START Twi libraries in your project, otherwise, the HAL layer will not compile because the START TWI drivers are a dependency \*

initialize an I2C interface using given config

### Parameters

in	<i>hal</i>	- opaque ptr to HAL data
in	<i>cfg</i>	- interface configuration

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

- this HAL implementation assumes you've included the ASF SERCOM I2C libraries in your project, otherwise, the HAL layer will not compile because the ASF I2C drivers are a dependency \*

### Parameters

in	<i>hal</i>	- opaque ptr to HAL data
in	<i>cfg</i>	- interface configuration

Returns

ATCA\_SUCCESS on success, otherwise an error code.

initialize an I2C interface using given config

Parameters

in	<i>hal</i>	- opaque ptr to HAL data
in	<i>cfg</i>	- interface configuration

Returns

ATCA\_SUCCESS on success, otherwise an error code.

- this HAL implementation assumes you've included the ASF Twi libraries in your project, otherwise, the HAL layer will not compile because the ASF TWI drivers are a dependency \*

initialize an I2C interface using given config

Parameters

in	<i>hal</i>	- opaque ptr to HAL data
in	<i>cfg</i>	- interface configuration

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.9.5.15 hal\_i2c\_post\_init()

```
ATCA_STATUS hal_i2c_post_init (
    ATCAIface iface )
```

HAL implementation of I2C post init.

Parameters

in	<i>iface</i>	instance
----	--------------	----------

Returns

ATCA\_SUCCESS

Parameters

in	<i>iface</i>	instance
----	--------------	----------

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### Parameters

in	<i>iface</i>	instance
----	--------------	----------

### Returns

ATCA\_SUCCESS

### 19.9.5.16 hal\_i2c\_receive()

```
ATCA_STATUS hal_i2c_receive (
    ATCAIface iface,
    uint8_t word_address,
    uint8_t * rxdata,
    uint16_t * rxlength )
```

HAL implementation of I2C receive function for START I2C.

HAL implementation of I2C receive function for ASF I2C.

HAL implementation of I2C receive function.

### Parameters

in	<i>iface</i>	Device to interact with.
in	<i>word_address</i>	device transaction type
out	<i>rxdata</i>	Data received will be returned here.
in, out	<i>rxlength</i>	As input, the size of the rxdata buffer. As output, the number of bytes received.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### Parameters

in	<i>iface</i>	Device to interact with.
out	<i>rxdata</i>	Data received will be returned here.
in, out	<i>rxlength</i>	As input, the size of the rxdata buffer. As output, the number of bytes received.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>iface</i>	Device to interact with.
in	<i>address</i>	device address
out	<i>rxdata</i>	Data received will be returned here.
in, out	<i>rxlength</i>	As input, the size of the rxdata buffer. As output, the number of bytes received.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>iface</i>	Device to interact with.
in	<i>word_address</i>	device word address
out	<i>rxdata</i>	Data received will be returned here.
in, out	<i>rxlength</i>	As input, the size of the rxdata buffer. As output, the number of bytes received.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.9.5.17 hal\_i2c\_release()

```
ATCA_STATUS hal_i2c_release (
    void * hal_data )
```

manages reference count on given bus and releases resource if no more refences exist

manages reference count on given bus and releases resource if no more refernces exist

Parameters

in	<i>hal_data</i>	- opaque pointer to hal data structure - known only to the HAL implementation
----	-----------------	---

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>hal_data</i>	- opaque pointer to hal data structure - known only to the HAL implementation return ATCA_SUCCESS
----	-----------------	--

### Parameters

in	<i>hal_data</i>	- opaque pointer to hal data structure - known only to the HAL implementation
----	-----------------	---

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### Parameters

in	<i>hal_data</i>	- opaque pointer to hal data structure - known only to the HAL implementation
----	-----------------	---

### Returns

ATCA\_SUCCESS

### 19.9.5.18 hal\_i2c\_send()

```
ATCA_STATUS hal_i2c_send (
    ATCAIface iface,
    uint8_t word_address,
    uint8_t * txdata,
    int txlength )
```

HAL implementation of I2C send over START.

HAL implementation of I2C send over ASF.

HAL implementation of I2C send.

### Parameters

in	<i>iface</i>	instance
in	<i>word_address</i>	device transaction type
in	<i>txdata</i>	pointer to space to bytes to send
in	<i>txlength</i>	number of bytes to send

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### Parameters

in	<i>iface</i>	instance
in	<i>txdata</i>	pointer to space to bytes to send
in	<i>txlength</i>	number of bytes to send



Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>iface</i>	instance
in	<i>word_address</i>	device word address
in	<i>txdata</i>	pointer to space to bytes to send
in	<i>txlength</i>	number of bytes to send

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>iface</i>	instance
in	<i>word_address</i>	device word address
in	<i>txdata</i>	pointer to space to bytes to send
in	<i>txlength</i>	number of bytes to send

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Add 1 byte for word address

Add 1 byte for word address

19.9.5.19 hal\_i2c\_sleep()

```
ATCA_STATUS hal_i2c_sleep (
    ATCAIface iface )
```

sleep CryptoAuth device using I2C bus

Parameters

in	<i>iface</i>	interface to logical device to sleep
----	--------------	--------------------------------------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>iface</i>	interface to logical device to sleep
----	--------------	--------------------------------------

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.9.5.20 hal\_i2c\_wake()

```
ATCA_STATUS hal_i2c_wake (
    ATCAIface iface )
```

wake up CryptoAuth device using I2C bus

### Parameters

in	<i>iface</i>	interface to logical device to wakeup
----	--------------	---------------------------------------

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### Parameters

in	<i>iface</i>	interface to logical device to wakeup
----	--------------	---------------------------------------

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.9.5.21 hal\_iface\_init()

```
ATCA_STATUS hal_iface_init (
    ATCAIfaceCfg * cfg,
    ATCAHAL_t ** hal,
    ATCAHAL_t ** phy )
```

Standard HAL API for ATCA to initialize a physical interface.

### Parameters

in	<i>cfg</i>	pointer to <a href="#">ATCAIfaceCfg</a> object
in	<i>hal</i>	pointer to <a href="#">ATCAHAL_t</a> intermediate data structure

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.9.5.22 hal\_iface\_register\_hal()

```
ATCA_STATUS hal_iface_register_hal (
    ATCAIfaceType iface_type,
    ATCAHAL_t * hal,
    ATCAHAL_t ** old_hal,
    ATCAHAL_t * phy,
    ATCAHAL_t ** old_phy )
```

Register/Replace a HAL with a.

Parameters

in	<i>iface_type</i>	- the type of physical interface to register
in	<i>hal</i>	pointer to the new <a href="#">ATCAHAL_t</a> structure to register
out	<i>old</i>	pointer to the existing <a href="#">ATCAHAL_t</a> structure

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.9.5.23 hal\_iface\_release()

```
ATCA_STATUS hal_iface_release (
    ATCAIfaceType iface_type,
    void * hal_data )
```

releases a physical interface, HAL knows how to interpret hal\_data

Parameters

in	<i>iface_type</i>	- the type of physical interface to release
in	<i>hal_data</i>	- pointer to opaque hal data maintained by HAL implementation for this interface type

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.9.5.24 hal\_is\_command\_word()

```
uint8_t hal_is_command_word (
    uint8_t word_address )
```

Utility function for hal\_wake to check the reply.

## 19.9 Hardware abstraction layer (hal\_)

---

### Parameters

in	<i>word_address</i>	Command to check
----	---------------------	------------------

### Returns

true if the *word\_address* is considered a command

### 19.9.5.25 hal\_kit\_attach\_phy()

```
ATCA_STATUS hal_kit_attach_phy (
    ATCAIfaceCfg * cfg,
    atca_hal_kit_phy_t * phy )
```

Helper function that connects a physical layer context structure that will be used by the kit protocol bridge.

### Returns

ATCA\_STATUS

### Parameters

<i>cfg</i>	[IN] Interface configuration structure
<i>phy</i>	[IN] Structure with physical layer interface functions and context

### 19.9.5.26 hal\_kit\_control()

```
ATCA_STATUS hal_kit_control (
    ATCAIface iface,
    uint8_t option,
    void * param,
    size_t paramlen )
```

Kit Protocol Control.

### Parameters

in	<i>iface</i>	ATCAIface instance that is the interface object to send the bytes over
in	<i>option</i>	Control option to use

### Returns

ATCA\_STATUS

19.9.5.27 hal\_kit\_hid\_control()

```
ATCA_STATUS hal_kit_hid_control (
    ATCAIface iface,
    uint8_t option,
    void * param,
    size_t paramlen )
```

Perform control operations for the kit protocol.

Parameters

in	<i>iface</i>	Interface to interact with.
in	<i>option</i>	Control parameter identifier
in	<i>param</i>	Optional pointer to parameter value
in	<i>paramlen</i>	Length of the parameter

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.9.5.28 hal\_kit\_hid\_init()

```
ATCA_STATUS hal_kit_hid_init (
    ATCAIface iface,
    ATCAIfaceCfg * cfg )
```

HAL implementation of Kit USB HID init.

Parameters

in	<i>hal</i>	pointer to HAL specific data that is maintained by this HAL
in	<i>cfg</i>	pointer to HAL specific configuration data that is used to initialize this HAL

Returns

ATCA\_STATUS

19.9.5.29 hal\_kit\_hid\_post\_init()

```
ATCA_STATUS hal_kit_hid_post_init (
    ATCAIface iface )
```

HAL implementation of Kit HID post init.

Parameters

in	<i>iface</i>	instance
----	--------------	----------

Returns

ATCA\_STATUS

19.9.5.30 hal\_kit\_hid\_receive()

```
ATCA_STATUS hal_kit_hid_receive (
    ATCAIface iface,
    uint8_t word_address,
    uint8_t * rxdata,
    uint16_t * rxlength )
```

HAL implementation of send over USB HID.

Parameters

in	<i>iface</i>	instance
in	<i>word_address</i>	determine device transaction type
in	<i>rxdata</i>	pointer to space to receive the data
in, out	<i>rxsize</i>	ptr to expected number of receive bytes to request

Returns

ATCA\_STATUS

19.9.5.31 hal\_kit\_hid\_release()

```
ATCA_STATUS hal_kit_hid_release (
    void * hal_data )
```

Close the physical port for HID.

Parameters

in	<i>hal_data</i>	The hardware abstraction data specific to this HAL
----	-----------------	--

Returns

ATCA\_STATUS

19.9.5.32 hal\_kit\_hid\_send()

```
ATCA_STATUS hal_kit_hid_send (
    ATCAIface iface,
    uint8_t word_address,
    uint8_t * txdata,
    int txlength )
```

HAL implementation of kit protocol send over USB HID.

Parameters

in	<i>iface</i>	instance
in	<i>word_address</i>	determine device transaction type
in	<i>txdata</i>	pointer to bytes to send
in	<i>txlength</i>	number of bytes to send

Returns

ATCA\_STATUS

19.9.5.33 hal\_kit\_init()

```
ATCA_STATUS hal_kit_init (
    ATCAIface iface,
    ATCAIfaceCfg * cfg )
```

HAL implementation of Kit USB HID init.

Parameters

in	<i>iface</i>	instance
in	<i>cfg</i>	pointer to HAL specific configuration data that is used to initialize this HAL

Returns

ATCA\_STATUS

19.9.5.34 hal\_kit\_post\_init()

```
ATCA_STATUS hal_kit_post_init (
    ATCAIface iface )
```

HAL implementation of Kit HID post init.

### Parameters

in	<i>iface</i>	instance
----	--------------	----------

### Returns

ATCA\_STATUS

#### 19.9.5.35 hal\_kit\_receive()

```
ATCA_STATUS hal_kit_receive (
    ATCAIface iface,
    uint8_t word_address,
    uint8_t * rxdata,
    uint16_t * rxsize )
```

HAL implementation of send over USB HID.

### Parameters

in	<i>iface</i>	instance
in	<i>word_address</i>	determine device transaction type
in	<i>rxdata</i>	pointer to space to receive the data
in, out	<i>rxsize</i>	ptr to expected number of receive bytes to request

### Returns

ATCA\_STATUS

#### 19.9.5.36 hal\_kit\_release()

```
ATCA_STATUS hal_kit_release (
    void * hal_data )
```

Close the physical port for HID.

### Parameters

in	<i>hal_data</i>	The hardware abstraction data specific to this HAL
----	-----------------	--

### Returns

ATCA\_STATUS



19.9.5.37 hal\_kit\_send()

```
ATCA_STATUS hal_kit_send (
    ATCAIface iface,
    uint8_t word_address,
    uint8_t * txdata,
    int txlength )
```

HAL implementation of kit protocol send over USB HID.

Parameters

in	<i>iface</i>	instance
in	<i>word_address</i>	determine device transaction type
in	<i>txdata</i>	pointer to bytes to send
in	<i>txlength</i>	number of bytes to send

Returns

ATCA\_STATUS

Add 1 byte to txlength for word address

19.9.5.38 hal\_rtos\_delay\_ms()

```
void hal_rtos_delay_ms (
    uint32_t delay )
```

This function delays for a number of milliseconds.

You can override this function if you like to do something else in your system while delaying.

Parameters

in	<i>delay</i>	Number of milliseconds to delay
----	--------------	---------------------------------

19.9.5.39 hal\_spi\_control()

```
ATCA_STATUS hal_spi_control (
    ATCAIface iface,
    uint8_t option,
    void * param,
    size_t paramlen )
```

Perform control operations for the kit protocol.

### Parameters

in	<i>iface</i>	Interface to interact with.
in	<i>option</i>	Control parameter identifier
in	<i>param</i>	Optional pointer to parameter value
in	<i>paramlen</i>	Length of the parameter

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.9.5.40 hal\_spi\_deselect()

```
ATCA_STATUS hal_spi_deselect (
    ATCAIface iface )
```

HAL implementation to deassert the device chip select.

### Parameters

in	<i>iface</i>	Device to interact with.
----	--------------	--------------------------

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.9.5.41 hal\_spi\_discover\_buses()

```
ATCA_STATUS hal_spi_discover_buses (
    int spi_buses[],
    int max_buses )
```

discover spi buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-priori knowledge

### Parameters

in	<i>spi_buses</i>	- an array of logical bus numbers
in	<i>max_buses</i>	- maximum number of buses the app wants to attempt to discover

### Returns

ATCA\_SUCCESS

19.9.5.42 hal\_spi\_discover\_devices()

```
ATCA_STATUS hal_spi_discover_devices (
    int bus_num,
    ATCAInterfaceCfg cfg[],
    int * found )
```

discover any TA10x devices on a given logical bus number

Parameters

in	bus_num	logical bus number on which to look for TA10x devices
out	cfg	pointer to head of an array of interface config structures which get filled in by this method
out	found	number of devices found on this bus

Returns

ATCA\_SUCCESS

19.9.5.43 hal\_spi\_init()

```
ATCA_STATUS hal_spi_init (
    ATCAInterface iface,
    ATCAInterfaceCfg * cfg )
```

initialize an SPI interface using given config

Parameters

in	hal	- opaque ptr to HAL data
in	cfg	- interface configuration

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.9.5.44 hal\_spi\_post\_init()

```
ATCA_STATUS hal_spi_post_init (
    ATCAInterface iface )
```

HAL implementation of SPI post init.

### Parameters

in	<i>iface</i>	instance
----	--------------	----------

### Returns

ATCA\_SUCCESS

#### 19.9.5.45 hal\_spi\_receive()

```
ATCA_STATUS hal_spi_receive (
    ATCAIface iface,
    uint8_t word_address,
    uint8_t * rxdata,
    uint16_t * rxlength )
```

HAL implementation of SPI receive function for HARMONY SPI.

### Parameters

in	<i>iface</i>	Device to interact with.
in	<i>word_address</i>	device transaction type
out	<i>rxdata</i>	Data received will be returned here.
in, out	<i>rxlength</i>	As input, the size of the rxdata buffer. As output, the number of bytes received.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.9.5.46 hal\_spi\_release()

```
ATCA_STATUS hal_spi_release (
    void * hal_data )
```

manages reference count on given bus and releases resource if no more refences exist

### Parameters

in	<i>hal_data</i>	- opaque pointer to hal data structure - known only to the HAL implementation
----	-----------------	---

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.9.5.47 hal\_spi\_select()

```
ATCA_STATUS hal_spi_select (
    ATCAIface iface )
```

HAL implementation to assert the device chip select.

Parameters

in	<i>iface</i>	Device to interact with.
----	--------------	--------------------------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.9.5.48 hal\_spi\_send()

```
ATCA_STATUS hal_spi_send (
    ATCAIface iface,
    uint8_t word_address,
    uint8_t * txdata,
    int txlength )
```

HAL implementation of SPI send over Harmony.

Parameters

in	<i>iface</i>	instance
in	<i>word_address</i>	device transaction type
in	<i>txdata</i>	pointer to space to bytes to send
in	<i>txlength</i>	number of bytes to send

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.9.5.49 hal\_swi\_control()

```
ATCA_STATUS hal_swi_control (
    ATCAIface iface,
    uint8_t option,
    void * param,
    size_t paramlen )
```

Perform control operations for the kit protocol.

### Parameters

in	<i>iface</i>	Interface to interact with.
in	<i>option</i>	Control parameter identifier
in	<i>param</i>	Optional pointer to parameter value
in	<i>paramlen</i>	Length of the parameter

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.9.5.50 hal\_swi\_idle()

```
ATCA_STATUS hal_swi_idle (
    ATCAIface iface )
```

Send Idle flag via SWI.

### Parameters

in	<i>iface</i>	interface of the logical device to idle
----	--------------	---

### Returns

ATCA\_SUCCESS

#### 19.9.5.51 hal\_swi\_init()

```
ATCA_STATUS hal_swi_init (
    ATCAIface iface,
    ATCAIfaceCfg * cfg )
```

initialize an SWI interface using given config

### Parameters

in	<i>hal</i>	- opaque ptr to HAL data
in	<i>cfg</i>	- interface configuration

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.9.5.52 hal\_swi\_post\_init()

```
ATCA_STATUS hal_swi_post_init (
    ATCAIface iface )
```

HAL implementation of SWI post init.

Parameters

in	iface	instance
----	-------	----------

Returns

ATCA\_SUCCESS

19.9.5.53 hal\_swi\_receive()

```
ATCA_STATUS hal_swi_receive (
    ATCAIface iface,
    uint8_t word_address,
    uint8_t * rxdata,
    uint16_t * rxlength )
```

HAL implementation of SWI receive function over UART.

Parameters

in	iface	Device to interact with.
in	word_address	device transaction type
out	rxdata	Data received will be returned here.
in, out	rxlength	As input, the size of the rxdata buffer. As output, the number of bytes received.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.9.5.54 hal\_swi\_release()

```
ATCA_STATUS hal_swi_release (
    void * hal_data )
```

manages reference count on given bus and releases resource if no more refences exist

### Parameters

in	<i>hal_data</i>	- opaque pointer to hal data structure - known only to the HAL implementation
----	-----------------	---

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 19.9.5.55 hal\_swi\_send()

```
ATCA_STATUS hal_swi_send (  
    ATCAIface iface,  
    uint8_t word_address,  
    uint8_t * txdata,  
    int txlength )
```

HAL implementation of SWI send command over UART.

### Parameters

in	<i>iface</i>	instance
in	<i>word_address</i>	device transaction type
in	<i>txdata</i>	pointer to space to bytes to send
in	<i>txlength</i>	number of bytes to send

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

Send word address

Send data

#### 19.9.5.56 hal\_swi\_sleep()

```
ATCA_STATUS hal_swi_sleep (  
    ATCAIface iface )
```

Send Sleep flag via SWI.

### Parameters

in	<i>iface</i>	interface of the logical device to sleep
----	--------------	--



Returns

ATCA\_SUCCESS

19.9.5.57 hal\_swi\_wake()

```
ATCA_STATUS hal_swi_wake (
    ATCAIface iface )
```

Send Wake flag via SWI.

Parameters

in	iface	interface of the logical device to wake up
----	-------	--

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.9.5.58 kit\_id\_from\_devtype()

```
const char * kit_id_from_devtype (
    ATCADeviceType devtype )
```

Kit Protocol is key

19.9.5.59 kit\_interface()

```
const char * kit_interface (
    ATCAKitType kittype )
```

Kit parser physical interface string

19.9.5.60 kit\_interface\_from\_kittype()

```
const char * kit_interface_from_kittype (
    ATCAKitType kittype )
```

Kit interface from device

19.9.5.61 swi\_uart\_deinit()

```
ATCA_STATUS swi_uart_deinit (
    ATCASMIMaster_t * instance )
```

Implementation of SWI UART deinit.

HAL implementation of SWI UART deinit.

### Parameters

in	<i>instance</i>	instance
----	-----------------	----------

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### Parameters

in	<i>instance</i>	instance
----	-----------------	----------

### Returns

ATCA\_SUCCESS

### 19.9.5.62 swi\_uart\_discover\_buses()

```
void swi_uart_discover_buses (
    int swi_uart_buses[],
    int max_buses )
```

discover UART buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-priori knowledge

### Parameters

in	<i>swi_uart_buses</i>	- an array of logical bus numbers
in	<i>max_buses</i>	- maximum number of buses the app wants to attempt to discover

### 19.9.5.63 swi\_uart\_init()

```
ATCA_STATUS swi_uart_init (
    ATCASWIMaster_t * instance )
```

Implementation of SWI UART init.

HAL implementation of SWI UART init.

- this HAL implementation assumes you've included the ASF SERCOM UART libraries in your project, otherwise, the HAL layer will not compile because the ASF UART drivers are a dependency \*

Parameters

in	<i>instance</i>	instance
----	-----------------	----------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

- this HAL implementation assumes you've included the START SERCOM UART libraries in your project, otherwise, the HAL layer will not compile because the START UART drivers are a dependency \*

Parameters

in	<i>instance</i>	instance
----	-----------------	----------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.9.5.64 swi\_uart\_mode()

```
void swi_uart_mode (
    ATCASWIMaster_t * instance,
    uint8_t mode )
```

implementation of SWI UART change mode.

HAL implementation of SWI UART change mode.

Parameters

in	<i>instance</i>	instance
in	<i>mode</i>	(TRANSMIT_MODE or RECEIVE_MODE)

19.9.5.65 swi\_uart\_receive\_byte()

```
ATCA_STATUS swi_uart_receive_byte (
    ATCASWIMaster_t * instance,
    uint8_t * data )
```

HAL implementation of SWI UART receive bytes over ASF. This function receive one byte over UART.

Parameters

in	<i>instance</i>	instance
out	<i>data</i>	pointer to space to receive the data

## 19.10 Host side crypto methods (atcah\_)

---

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.9.5.66 swi\_uart\_send\_byte()

```
ATCA_STATUS swi_uart_send_byte (
    ATCASWIMaster_t * instance,
    uint8_t data )
```

HAL implementation of SWI UART send byte over ASF. This function send one byte over UART.

### Parameters

in	<i>instance</i>	instance
in	<i>data</i>	number of byte to send

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 19.9.5.67 swi\_uart\_setbaud()

```
void swi_uart_setbaud (
    ATCASWIMaster_t * instance,
    uint32_t baudrate )
```

implementation of SWI UART change baudrate.

HAL implementation of SWI UART change baudrate.

### Parameters

in	<i>instance</i>	instance
in	<i>baudrate</i>	(typically 230400 , 160000 or 115200)
in	<i>instance</i>	instance
in	<i>baudrate</i>	(typically 230400 or 115200)

## 19.10 Host side crypto methods (atcah\_)

Use these functions if your system does not use an ATCADevice as a host but implements the host in firmware. The functions provide host-side cryptographic functionality for an ATECC client device. They are intended to accompany the CryptoAuthLib functions. They can be called directly from an application, or integrated into an API.

## Data Structures

- struct [atca\\_temp\\_key](#)  
*Structure to hold TempKey fields.*
- struct [atca\\_include\\_data\\_in\\_out](#)  
*Input / output parameters for function `atca_include_data()`.*
- struct [atca\\_nonce\\_in\\_out](#)  
*Input/output parameters for function `atca_nonce()`.*
- struct [atca\\_io\\_decrypt\\_in\\_out](#)
- struct [atca\\_verify\\_mac](#)
- struct [atca\\_secureboot\\_enc\\_in\\_out](#)
- struct [atca\\_secureboot\\_mac\\_in\\_out](#)
- struct [atca\\_mac\\_in\\_out](#)  
*Input/output parameters for function `atca_mac()`.*
- struct [atca\\_hmac\\_in\\_out](#)  
*Input/output parameters for function `atca_hmac()`.*
- struct [atca\\_gen\\_dig\\_in\\_out](#)  
*Input/output parameters for function `atcah_gen_dig()`.*
- struct [atca\\_diversified\\_key\\_in\\_out](#)  
*Input/output parameters for function `atcah_gendivkey()`.*
- struct [atca\\_write\\_mac\\_in\\_out](#)  
*Input/output parameters for function `atcah_write_auth_mac()` and `atcah_privwrite_auth_mac()`.*
- struct [atca\\_derive\\_key\\_in\\_out](#)  
*Input/output parameters for function `atcah_derive_key()`.*
- struct [atca\\_derive\\_key\\_mac\\_in\\_out](#)  
*Input/output parameters for function `atcah_derive_key_mac()`.*
- struct [atca\\_decrypt\\_in\\_out](#)  
*Input/output parameters for function `atca_decrypt()`.*
- struct [atca\\_check\\_mac\\_in\\_out](#)  
*Input/output parameters for function `atcah_check_mac()`.*
- struct [atca\\_resp\\_mac\\_in\\_out](#)  
*Input/Output parameters for calculating the output response mac in SHA105 device. Used with the `atcah_gen_↔  
output_resp_mac()` function.*
- struct [atca\\_verify\\_in\\_out](#)  
*Input/output parameters for function `atcah_verify()`.*
- struct [atca\\_gen\\_key\\_in\\_out](#)  
*Input/output parameters for calculating the PubKey digest put into TempKey by the GenKey command with the `atcah_↔  
_gen_key_msg()` function.*
- struct [atca\\_sign\\_internal\\_in\\_out](#)  
*Input/output parameters for calculating the message and digest used by the Sign(internal) command. Used with the `atcah_sign_internal_msg()` function.*
- struct [atca\\_session\\_key\\_in\\_out](#)  
*Input/Output paramters for calculating the session key by the nonce command. Used with the `atcah_gen_session_↔  
_key()` function.*
- struct [atca\\_delete\\_in\\_out](#)  
*Input/Output paramters for calculating the mac.Used with Delete command.*

## Typedefs

- typedef struct [atca\\_temp\\_key](#) **atca\_temp\_key\_t**  
*Structure to hold TempKey fields.*
- typedef struct [atca\\_nonce\\_in\\_out](#) **atca\_nonce\_in\_out\_t**
- typedef struct [atca\\_io\\_decrypt\\_in\\_out](#) **atca\_io\_decrypt\_in\_out\_t**
- typedef struct [atca\\_verify\\_mac](#) **atca\_verify\_mac\_in\_out\_t**
- typedef struct [atca\\_secureboot\\_enc\\_in\\_out](#) **atca\_secureboot\_enc\_in\_out\_t**
- typedef struct [atca\\_secureboot\\_mac\\_in\\_out](#) **atca\_secureboot\_mac\_in\_out\_t**
- typedef struct [atca\\_mac\\_in\\_out](#) **atca\_mac\_in\_out\_t**
- typedef struct [atca\\_gen\\_dig\\_in\\_out](#) **atca\_gen\_dig\_in\_out\_t**  
*Input/output parameters for function `atcah_gen_dig()`.*
- typedef struct [atca\\_diversified\\_key\\_in\\_out](#) **atca\_diversified\_key\_in\_out\_t**  
*Input/output parameters for function `atcah_gendivkey()`.*
- typedef struct [atca\\_write\\_mac\\_in\\_out](#) **atca\_write\_mac\_in\_out\_t**  
*Input/output parameters for function `atcah_write_auth_mac()` and `atcah_privwrite_auth_mac()`.*
- typedef struct [atca\\_check\\_mac\\_in\\_out](#) **atca\_check\_mac\_in\_out\_t**  
*Input/output parameters for function `atcah_check_mac()`.*
- typedef struct [atca\\_resp\\_mac\\_in\\_out](#) **atca\_resp\_mac\_in\_out\_t**  
*Input/Output parameters for calculating the output response mac in SHA105 device. Used with the `atcah_gen_↔  
output_resp_mac()` function.*
- typedef struct [atca\\_verify\\_in\\_out](#) **atca\_verify\_in\_out\_t**
- typedef struct [atca\\_gen\\_key\\_in\\_out](#) **atca\_gen\_key\_in\_out\_t**  
*Input/output parameters for calculating the PubKey digest put into TempKey by the GenKey command with the `atcah_↔  
_gen_key_msg()` function.*
- typedef struct [atca\\_sign\\_internal\\_in\\_out](#) **atca\_sign\_internal\_in\_out\_t**  
*Input/output parameters for calculating the message and digest used by the Sign(internal) command. Used with the `atcah_sign_internal_msg()` function.*
- typedef struct [atca\\_session\\_key\\_in\\_out](#) **atca\_session\_key\_in\_out\_t**  
*Input/Output paramters for calculating the session key by the nonce command. Used with the `atcah_gen_session_↔  
_key()` function.*
- typedef struct [atca\\_delete\\_in\\_out](#) **atca\_delete\_in\_out\_t**  
*Input/Output paramters for calculating the mac.Used with Delete command.*

## Functions

- ATCA\_STATUS **atcah\_nonce** (struct [atca\\_nonce\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_mac** (struct [atca\\_mac\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_check\_mac** (struct [atca\\_check\\_mac\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_hmac** (struct [atca\\_hmac\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_gen\_dig** (struct [atca\\_gen\\_dig\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_gendivkey** (struct [atca\\_diversified\\_key\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_gen\_mac** (struct [atca\\_gen\\_dig\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_write\_auth\_mac** (struct [atca\\_write\\_mac\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_privwrite\_auth\_mac** (struct [atca\\_write\\_mac\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_derive\_key** (struct [atca\\_derive\\_key\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_derive\_key\_mac** (struct [atca\\_derive\\_key\\_mac\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_decrypt** (struct [atca\\_decrypt\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_sha256** (uint32\_t len, const uint8\_t \*message, uint8\_t \*digest)
- uint8\_t \* **atcah\_include\_data** (struct [atca\\_include\\_data\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_gen\_key\_msg** (struct [atca\\_gen\\_key\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_config\_to\_sign\_internal** (ATCADeviceType device\_type, struct [atca\\_sign\\_internal\\_in\\_out](#) \*param, const uint8\_t \*config)

- ATCA\_STATUS **atcah\_sign\_internal\_msg** (ATCADeviceType device\_type, struct [atca\\_sign\\_internal\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_verify\_mac** ([atca\\_verify\\_mac\\_in\\_out\\_t](#) \*param)
- ATCA\_STATUS **atcah\_secureboot\_enc** ([atca\\_secureboot\\_enc\\_in\\_out\\_t](#) \*param)
- ATCA\_STATUS **atcah\_secureboot\_mac** ([atca\\_secureboot\\_mac\\_in\\_out\\_t](#) \*param)
- ATCA\_STATUS **atcah\_encode\_counter\_match** (uint32\_t counter\_value, uint8\_t \*counter\_match\_value)
- ATCA\_STATUS **atcah\_io\_decrypt** (struct [atca\\_io\\_decrypt\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_ecc204\_write\_auth\_mac** (struct [atca\\_write\\_mac\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_gen\_session\_key** ([atca\\_session\\_key\\_in\\_out\\_t](#) \*param)
- ATCA\_STATUS **atcah\_gen\_output\_resp\_mac** (struct [atca\\_resp\\_mac\\_in\\_out](#) \*param)

## Variables

- uint8\_t \* **atca\_include\_data\_in\_out::p\_temp**  
*[out] pointer to output buffer*
- const uint8\_t \* **atca\_include\_data\_in\_out::otp**  
*[in] pointer to one-time-programming data*
- const uint8\_t \* **atca\_include\_data\_in\_out::sn**  
*[in] pointer to serial number data*
- uint8\_t **atca\_nonce\_in\_out::mode**  
*[in] Mode parameter used in Nonce command (Param1).*
- uint16\_t **atca\_nonce\_in\_out::zero**  
*[in] Zero parameter used in Nonce command (Param2).*
- const uint8\_t \* **atca\_nonce\_in\_out::num\_in**  
*[in] Pointer to 20-byte NumIn data used in Nonce command.*
- const uint8\_t \* **atca\_nonce\_in\_out::rand\_out**  
*[in] Pointer to 32-byte RandOut data from Nonce command.*
- struct [atca\\_temp\\_key](#) \* **atca\_nonce\_in\_out::temp\_key**  
*[in,out] Pointer to TempKey structure.*
- uint8\_t **atca\_mac\_in\_out::mode**  
*[in] Mode parameter used in MAC command (Param1).*
- uint16\_t **atca\_mac\_in\_out::key\_id**  
*[in] KeyID parameter used in MAC command (Param2).*
- const uint8\_t \* **atca\_mac\_in\_out::challenge**  
*[in] Pointer to 32-byte Challenge data used in MAC command, depending on mode.*
- const uint8\_t \* **atca\_mac\_in\_out::key**  
*[in] Pointer to 32-byte key used to generate MAC digest.*
- const uint8\_t \* **atca\_mac\_in\_out::otp**  
*[in] Pointer to 11-byte OTP, optionally included in MAC digest, depending on mode.*
- const uint8\_t \* **atca\_mac\_in\_out::sn**  
*[in] Pointer to 9-byte SN, optionally included in MAC digest, depending on mode.*
- uint8\_t \* **atca\_mac\_in\_out::response**  
*[out] Pointer to 32-byte SHA-256 digest (MAC).*
- struct [atca\\_temp\\_key](#) \* **atca\_mac\_in\_out::temp\_key**  
*[in,out] Pointer to TempKey structure.*
- uint8\_t **atca\_hmac\_in\_out::mode**  
*[in] Mode parameter used in HMAC command (Param1).*
- uint16\_t **atca\_hmac\_in\_out::key\_id**  
*[in] KeyID parameter used in HMAC command (Param2).*
- const uint8\_t \* **atca\_hmac\_in\_out::key**  
*[in] Pointer to 32-byte key used to generate HMAC digest.*

- `const uint8_t * atca_hmac_in_out::otp`  
*[in] Pointer to 11-byte OTP, optionally included in HMAC digest, depending on mode.*
- `const uint8_t * atca_hmac_in_out::sn`  
*[in] Pointer to 9-byte SN, optionally included in HMAC digest, depending on mode.*
- `uint8_t * atca_hmac_in_out::response`  
*[out] Pointer to 32-byte SHA-256 HMAC digest.*
- `struct atca_temp_key * atca_hmac_in_out::temp_key`  
*[in,out] Pointer to TempKey structure.*
- `uint8_t * atca_decrypt_in_out::crypto_data`  
*[in,out] Pointer to 32-byte data. Input encrypted data from Read command (Contents field), output decrypted.*
- `struct atca_temp_key * atca_decrypt_in_out::temp_key`  
*[in,out] Pointer to TempKey structure.*
- `uint16_t atca_verify_in_out::curve_type`  
*[in] Curve type used in Verify command (Param2).*
- `const uint8_t * atca_verify_in_out::signature`  
*[in] Pointer to ECDSA signature to be verified*
- `const uint8_t * atca_verify_in_out::public_key`  
*[in] Pointer to the public key to be used for verification*
- `struct atca_temp_key * atca_verify_in_out::temp_key`  
*[in,out] Pointer to TempKey structure.*

## Definitions for ATECC Message Sizes to Calculate a SHA256 Hash

"||" is the concatenation operator. The number in braces is the length of the hash input value in bytes.

- `#define ATCA_MSG_SIZE_NONCE (55)`  
*RandOut{32} || NumIn{20} || OpCode{1} || Mode{1} || LSB of Param2{1}.*
- `#define ATCA_MSG_SIZE_MAC (88)`  
*(Key or TempKey){32} || (Challenge or TempKey){32} || OpCode{1} || Mode{1} || Param2{2} || (OTP0\_7 or 0){8} || (OTP8\_10 or 0){3} || SN8{1} || (SN4\_7 or 0){4} || SN0\_1{2} || (SN2\_3 or 0){2}*
- `#define ATCA_MSG_SIZE_HMAC (88u)`
- `#define ATCA_MSG_SIZE_GEN_DIG (96)`  
*KeyId{32} || OpCode{1} || Param1{1} || Param2{2} || SN8{1} || SN0\_1{2} || 0{25} || TempKey{32}.*
- `#define ATCA_MSG_SIZE_DIVERSIFIED_KEY (96)`  
*ParentKey{32} || OtherData{4} || SN8{1} || SN0\_1{2} || 0{25} || InputData{32}.*
- `#define ATCA_MSG_SIZE_DERIVE_KEY (96)`  
*KeyId{32} || OpCode{1} || Param1{1} || Param2{2} || SN8{1} || SN0\_1{2} || 0{25} || TempKey{32}.*
- `#define ATCA_MSG_SIZE_DERIVE_KEY_MAC (39)`  
*KeyId{32} || OpCode{1} || Param1{1} || Param2{2} || SN8{1} || SN0\_1{2}.*
- `#define ATCA_MSG_SIZE_ENCRYPT_MAC (96)`  
*KeyId{32} || OpCode{1} || Param1{1} || Param2{2} || SN8{1} || SN0\_1{2} || 0{25} || TempKey{32}.*
- `#define ATCA_MSG_SIZE_SESSION_KEY (96)`  
*TransportKey{32} || 0x15{1} || 0x00{1} || KeyId{2} || SN8{1} || SN0\_1{2} || 0{25} || Nonce{32}.*
- `#define ATCA_MSG_SIZE_DELETE_MAC (96)`  
*Hmac/SecretKey{32} || 0x13{1} || 0x00{1} || 0x0000{2} || SN8{1} || SN0\_1{2} || 0{25} || Nonce{32}.*
- `#define ATCA_MSG_SIZE_RESPONSE_MAC (97)`  
*SlotKey{32} || OpCode{1} || Param1{1} || Param2{2} || SN8{1} || SN0\_1{2} || 0{25} || client\_Resp{32} || checkmac←\_result{1}.*
- `#define ATCA_MSG_SIZE_PRIVWRITE_MAC (96)`  
*KeyId{32} || OpCode{1} || Param1{1} || Param2{2} || SN8{1} || SN0\_1{2} || 0{21} || PlainText{36}.*



- `#define ATCA_COMMAND_HEADER_SIZE ( 4)`
- `#define ATCA_GENDIG_ZEROS_SIZE (25)`
- `#define ATCA_GENDIVKEY_ZEROS_SIZE (25)`
- `#define ATCA_WRITE_MAC_ZEROS_SIZE (25)`
- `#define ATCA_DELETE_MAC_ZEROS_SIZE (25)`
- `#define ATCA_RESP_MAC_ZEROS_SIZE (25)`
- `#define ATCA_PRIVWRITE_MAC_ZEROS_SIZE (21)`
- `#define ATCA_PRIVWRITE_PLAIN_TEXT_SIZE (36)`
- `#define ATCA_DERIVE_KEY_ZEROS_SIZE (25)`
- `#define ATCA_HMAC_BLOCK_SIZE (64u)`
- `#define ATCA_ENCRYPTION_KEY_SIZE (64)`

### Definition for TempKey Mode

- `#define MAC_MODE_USE_TEMPKEY_MASK ((uint8_t)0x03)`  
*mode mask for MAC command when using TempKey*

### 19.10.1 Detailed Description

Use these functions if your system does not use an ATCADevice as a host but implements the host in firmware. The functions provide host-side cryptographic functionality for an ATECC client device. They are intended to accompany the CryptoAuthLib functions. They can be called directly from an application, or integrated into an API.

Modern compilers can garbage-collect unused functions. If your compiler does not support this feature, you can just discard this module from your project if you do use an ATECC as a host. Or, if you don't, delete the functions you do not use.

## 19.11 JSON Web Token (JWT) methods (atca\_jwt\_)

Methods for signing and verifying JSON Web Token (JWT) tokens.

Methods for signing and verifying JSON Web Token (JWT) tokens.

## 19.12 mbedTLS Wrapper methods (atca\_mbedtls\_)

These methods are for interfacing cryptoauthlib to mbedtls.

### 19.12.0.1 mbedtls directory - Purpose

This directory contains the interfacing and wrapper functions to integrate mbedtls as the software crypto library as well as provide elliptic curve cryptography (ECC) hardware acceleration.

### Data Structures

- struct [atca\\_mbedtls\\_eckey\\_s](#)

### Typedefs

- typedef struct [atca\\_mbedtls\\_eckey\\_s](#) [atca\\_mbedtls\\_eckey\\_t](#)

### Functions

- int **atca\_mbedtls\_ecdsa\_sign** (const mbedtls\_mpi \*d, mbedtls\_mpi \*r, mbedtls\_mpi \*s, const unsigned char \*buf, size\_t buf\_len)
- int **atca\_mbedtls\_pk\_init\_ext** ([ATCADevice](#) device, mbedtls\_pk\_context \*pkey, const uint16\_t slotid)  
*Initializes an mbedtls pk context for use with EC operations.*
- int **atca\_mbedtls\_pk\_init** (mbedtls\_pk\_context \*pkey, const uint16\_t slotid)  
*Initializes an mbedtls pk context for use with EC operations.*
- int **atca\_mbedtls\_cert\_add** (struct mbedtls\_x509\_crt \*cert, const struct [atcacert\\_def\\_s](#) \*cert\_def)
- int **atca\_mbedtls\_ecdh\_slot\_cb** (void)  
*ECDH Callback to obtain the "slot" used in ECDH operations from the application.*
- int **atca\_mbedtls\_ecdh\_ioprot\_cb** (uint8\_t secret[32])  
*ECDH Callback to obtain the IO Protection secret from the application.*
- struct mbedtls\_x509\_crt \* **atcac\_mbedtls\_new** (void)
- struct [atcac\\_x509\\_ctx](#) \* **atcac\_x509\_ctx\_new** (void)
- void **atcac\_x509\_ctx\_free** (struct [atcac\\_x509\\_ctx](#) \*ctx)

### 19.12.1 Detailed Description

These methods are for interfacing cryptoauthlib to mbedtls.

### 19.12.2 Typedef Documentation

#### 19.12.2.1 [atca\\_mbedtls\\_eckey\\_t](#)

```
typedef struct atca\_mbedtls\_eckey\_s atca\_mbedtls\_eckey\_t
```

Structure to hold metadata - is written into the mbedtls pk structure as the private key bignum value 'd' which otherwise would be unused. Bignums can be any arbitrary length of bytes

### 19.12.3 Function Documentation

#### 19.12.3.1 [atca\\_mbedtls\\_ecdh\\_ioprot\\_cb\(\)](#)

```
int atca\_mbedtls\_ecdh\_ioprot\_cb (  
    uint8_t secret[32] )
```

ECDH Callback to obtain the IO Protection secret from the application.

Parameters

out	<i>secret</i>	32 byte array used to store the secret
-----	---------------	--

Returns

ATCA\_SUCCESS on success, otherwise an error code.

19.12.3.2 atca\_mbedtls\_ecdh\_slot\_cb()

```
int atca_mbedtls_ecdh_slot_cb (  
    void )
```

ECDH Callback to obtain the "slot" used in ECDH operations from the application.

Returns

Slot Number

19.12.3.3 atca\_mbedtls\_pk\_init()

```
int atca_mbedtls_pk_init (  
    mbedtls_pk_context * pkey,  
    const uint16_t slotid )
```

Initializes an mbedtls pk context for use with EC operations.

Parameters

in, out	<i>pkey</i>	ptr to space to receive version string
in	<i>slotid</i>	Associated with this key

Returns

0 on success, otherwise an error code.

19.12.3.4 atca\_mbedtls\_pk\_init\_ext()

```
int atca_mbedtls_pk_init_ext (  
    ATCADevice device,  
    mbedtls_pk_context * pkey,  
    const uint16_t slotid )
```

Initializes an mbedtls pk context for use with EC operations.

### Parameters

in, out	<i>pkey</i>	ptr to space to receive version string
in	<i>slotid</i>	Associated with this key

### Returns

0 on success, otherwise an error code.

## 19.13 Attributes (pkcs11\_attrib\_)

### Data Structures

- struct [pkcs11\\_conf\\_filedata\\_s](#)
- struct [pkcs11\\_mech\\_table\\_e](#)

### Macros

- #define **PKCS11\_CONFIG\_U8\_MAX** 0xFFL
- #define **PKCS11\_CONFIG\_U16\_MAX** 0xFFFFL
- #define **PKCS11\_CONFIG\_U32\_MAX** 0xFFFFFFFFL
- #define **PKCS11\_MECH\_ECC508\_EC\_CAPABILITY** (CKF\_EC\_F\_P | CKF\_EC\_NAMEDCURVE | CKF\_↔  
EC\_UNCOMPRESS)
- #define **TABLE\_SIZE**(x) sizeof(x) / sizeof(x[0])

### Typedefs

- typedef struct [pkcs11\\_conf\\_filedata\\_s](#) **pkcs11\_conf\_filedata**
- typedef struct [pkcs11\\_conf\\_filedata\\_s](#) \* **pkcs11\_conf\_filedata\_ptr**
- typedef struct [pkcs11\\_mech\\_table\\_e](#) **pkcs11\_mech\_table\_e**
- typedef struct [pkcs11\\_mech\\_table\\_e](#) \* **pkcs11\_mech\_table\_ptr**

### Functions

- CK\_RV [pkcs11\\_attrib\\_fill](#) (CK\_ATTRIBUTE\_PTR pAttribute, const void \*pData, const CK\_ULONG ulSize)  
*Perform the nessasary checks and copy data into an attribute structure.*
- CK\_RV **pkcs11\_attrib\_value** (CK\_ATTRIBUTE\_PTR pAttribute, const CK\_ULONG ulValue, const CK\_↔  
ULONG ulSize)  
*Helper function to write a numerical value to an attribute buffer.*
- CK\_RV **pkcs11\_attrib\_false** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#)  
pSession)
- CK\_RV **pkcs11\_attrib\_true** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#)  
pSession)
- CK\_RV **pkcs11\_attrib\_empty** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#)  
pSession)
- CK\_RV **pkcs11\_cert\_load** (pkcs11\_object\_ptr pObject, CK\_ATTRIBUTE\_PTR pAttribute, [ATCADevice](#) de-  
vice)
- CK\_RV **pkcs11\_cert\_x509\_write** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#)  
pSession)

- CK\_RV **pkcs11\_cert\_clear\_session\_cache** ([pkcs11\\_session\\_ctx\\_ptr](#) session\_ctx)
- CK\_RV **pkcs11\_cert\_clear\_object\_cache** (pkcs11\_object\_ptr pObject)
- void **pkcs11\_config\_init\_private** (pkcs11\_object\_ptr pObject, const char \*label, size\_t len)
- void **pkcs11\_config\_init\_public** (pkcs11\_object\_ptr pObject, const char \*label, size\_t len)
- void **pkcs11\_config\_init\_secret** (pkcs11\_object\_ptr pObject, const char \*label, size\_t len, size\_t keylen)
- void **pkcs11\_config\_init\_cert** (pkcs11\_object\_ptr pObject, const char \*label, size\_t len)
- void **pkcs11\_config\_split\_string** (char \*s, char splitter, int \*argc, char \*argv[])
- CK\_RV **pkcs11\_config\_cert** (pkcs11\_lib\_ctx\_ptr pLibCtx, pkcs11\_slot\_ctx\_ptr pSlot, pkcs11\_object\_ptr p↵Object, CK\_ATTRIBUTE\_PTR pLabel)
- CK\_RV **pkcs11\_config\_key** (pkcs11\_lib\_ctx\_ptr pLibCtx, pkcs11\_slot\_ctx\_ptr pSlot, pkcs11\_object\_ptr p↵Object, CK\_ATTRIBUTE\_PTR pLabel)
- CK\_RV **pkcs11\_config\_remove\_object** (pkcs11\_lib\_ctx\_ptr pLibCtx, pkcs11\_slot\_ctx\_ptr pSlot, pkcs11↵\_object\_ptr pObject)
- CK\_RV **pkcs11\_config\_load\_objects** (pkcs11\_slot\_ctx\_ptr slot\_ctx)
- CK\_RV **pkcs11\_config\_load** (pkcs11\_slot\_ctx\_ptr slot\_ctx)
- CK\_RV **pkcs11\_encrypt\_init** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hObject)
- CK\_RV **pkcs11\_encrypt** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulData↵Len, CK\_BYTE\_PTR pEncryptedData, CK\_ULONG\_PTR pulEncryptedDataLen)
- CK\_RV **pkcs11\_encrypt\_update** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pEncryptedData, CK\_ULONG\_PTR pulEncryptedDataLen)
- CK\_RV **pkcs11\_encrypt\_final** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pEncryptedData, CK↵\_ULONG\_PTR pulEncryptedDataLen)

*Finishes a multiple-part encryption operation.*

- CK\_RV **pkcs11\_decrypt\_init** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hObject)
- CK\_RV **pkcs11\_decrypt** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pEncryptedData, CK↵\_ULONG ulEncryptedDataLen, CK\_BYTE\_PTR pData, CK\_ULONG\_PTR pulDataLen)
- CK\_RV **pkcs11\_decrypt\_update** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pEncryptedData, CK\_ULONG ulEncryptedDataLen, CK\_BYTE\_PTR pData, CK\_ULONG\_PTR pulDataLen)
- CK\_RV **pkcs11\_decrypt\_final** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG↵\_PTR pulDataLen)

*Finishes a multiple-part decryption operation.*

- CK\_RV **pkcs11\_find\_init** (CK\_SESSION\_HANDLE hSession, CK\_ATTRIBUTE\_PTR pTemplate, CK↵\_ULONG ulCount)
- CK\_RV **pkcs11\_find\_continue** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE\_PTR ph↵Object, CK\_ULONG ulMaxObjectCount, CK\_ULONG\_PTR pulObjectCount)
- CK\_RV **pkcs11\_find\_finish** (CK\_SESSION\_HANDLE hSession)
- CK\_RV **pkcs11\_find\_get\_attribute** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hObject, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount)
- CK\_RV **pkcs11\_get\_lib\_info** (CK\_INFO\_PTR pInfo)

*Obtains general information about Cryptoki.*

- pkcs11\_lib\_ctx\_ptr **pkcs11\_get\_context** (void)

*Retrieve the current library context.*

- CK\_RV **pkcs11\_lock\_context** (pkcs11\_lib\_ctx\_ptr pContext)
- CK\_RV **pkcs11\_unlock\_context** (pkcs11\_lib\_ctx\_ptr pContext)
- CK\_RV **pkcs11\_lock\_device** (pkcs11\_lib\_ctx\_ptr pContext)
- CK\_RV **pkcs11\_unlock\_device** (pkcs11\_lib\_ctx\_ptr pContext)
- CK\_RV **pkcs11\_lock\_both** (pkcs11\_lib\_ctx\_ptr pContext)
- CK\_RV **pkcs11\_unlock\_both** (pkcs11\_lib\_ctx\_ptr pContext)
- CK\_RV **pkcs11\_init\_check** (pkcs11\_lib\_ctx\_ptr \*ppContext, CK\_BBOOL lock)

*Check if the library is initialized properly.*

- CK\_RV **pkcs11\_init** ([CK\\_C\\_INITIALIZE\\_ARGS](#) const \*pInitArgs)

*Initializes the PKCS11 API Library for Cryptoauthlib.*

- CK\_RV **pkcs11\_deinit** (CK\_VOID\_PTR pReserved)
- const **pkcs11\_ecc\_key\_info\_t** \* **pkcs11\_get\_object\_key\_type** (ATCADevice device\_ctx, pkcs11\_object\_ptr obj\_ptr)
- CK\_RV **pkcs11\_ta\_get\_pubkey** (CK\_VOID\_PTR pObject, cal\_buffer \*key\_buffer, **pkcs11\_session\_ctx\_ptr** session\_ctx)
- CK\_RV **pkcs11\_key\_write** (CK\_VOID\_PTR pSession, CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, const **pkcs11\_ecc\_key\_info\_t** \*ec\_key\_info)
- CK\_RV **pkcs11\_key\_generate** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount, CK\_OBJECT\_HANDLE\_PTR phKey)
- CK\_RV **pkcs11\_key\_generate\_pair** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_ATTRIBUTE\_PTR pPublicKeyTemplate, CK\_ULONG ulPublicKeyAttributeCount, CK\_ATTRIBUTE\_PTR pPrivateKeyTemplate, CK\_ULONG ulPrivateKeyAttributeCount, CK\_OBJECT\_HANDLE\_PTR phPublicKey, CK\_OBJECT\_HANDLE\_PTR phPrivateKey)
- CK\_RV **pkcs11\_key\_derive** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hBaseKey, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount, CK\_OBJECT\_HANDLE\_PTR phKey)
- CK\_RV **pkcs11\_key\_clear\_session\_cache** (**pkcs11\_session\_ctx\_ptr** session\_ctx)
- CK\_RV **pkcs11\_key\_clear\_object\_cache** (pkcs11\_object\_ptr pObject)
- CK\_RV **C\_Initialize** (CK\_VOID\_PTR pInitArgs)
 

*Initializes Cryptoki library NOTES: If pInitArgs is a non-NULL\_PTR is must dereference to a **CK\_C\_INITIALIZE\_ARGS** structure.*
- CK\_RV **C\_Finalize** (CK\_VOID\_PTR pReserved)
 

*Clean up miscellaneous Cryptoki-associated resources.*
- CK\_RV **C\_GetInfo** (CK\_INFO\_PTR pInfo)
 

*Obtains general information about Cryptoki.*
- CK\_RV **C\_GetFunctionList** (CK\_FUNCTION\_LIST\_PTR\_PTR ppFunctionList)
 

*Obtains entry points of Cryptoki library functions.*
- CK\_RV **C\_GetSlotList** (CK\_BBOOL tokenPresent, CK\_SLOT\_ID\_PTR pSlotList, CK\_ULONG\_PTR pulCount)
 

*Obtains a list of slots in the system.*
- CK\_RV **C\_GetSlotInfo** (CK\_SLOT\_ID slotID, CK\_SLOT\_INFO\_PTR pInfo)
 

*Obtains information about a particular slot.*
- CK\_RV **C\_GetTokenInfo** (CK\_SLOT\_ID slotID, CK\_TOKEN\_INFO\_PTR pInfo)
 

*Obtains information about a particular token.*
- CK\_RV **C\_GetMechanismList** (CK\_SLOT\_ID slotID, CK\_MECHANISM\_TYPE\_PTR pMechanismList, CK\_ULONG\_PTR pulCount)
 

*Obtains a list of mechanisms supported by a token (in a slot)*
- CK\_RV **C\_GetMechanismInfo** (CK\_SLOT\_ID slotID, CK\_MECHANISM\_TYPE type, CK\_MECHANISM\_INFO\_PTR pInfo)
 

*Obtains information about a particular mechanism of a token (in a slot)*
- CK\_RV **C\_InitToken** (CK\_SLOT\_ID slotID, CK\_UTF8CHAR\_PTR pPin, CK\_ULONG ulPinLen, CK\_UTF8CHAR\_PTR pLabel)
 

*Initializes a token (in a slot)*
- CK\_RV **C\_InitPIN** (CK\_SESSION\_HANDLE hSession, CK\_UTF8CHAR\_PTR pPin, CK\_ULONG ulPinLen)
 

*Initializes the normal user's PIN.*
- CK\_RV **C\_SetPIN** (CK\_SESSION\_HANDLE hSession, CK\_UTF8CHAR\_PTR pOldPin, CK\_ULONG ulOldLen, CK\_UTF8CHAR\_PTR pNewPin, CK\_ULONG ulNewLen)
 

*Modifies the PIN of the current user.*
- CK\_RV **C\_OpenSession** (CK\_SLOT\_ID slotID, CK\_FLAGS flags, CK\_VOID\_PTR pApplication, CK\_NOTIFY Notify, CK\_SESSION\_HANDLE\_PTR phSession)
 

*Opens a connection between an application and a particular token or sets up an application callback for token insertion.*
- CK\_RV **C\_CloseSession** (CK\_SESSION\_HANDLE hSession)
 

*Close the given session.*

- **CK\_RV C\_CloseAllSessions** (CK\_SLOT\_ID slotID)  
*Close all open sessions.*
- **CK\_RV C\_GetSessionInfo** (CK\_SESSION\_HANDLE hSession, CK\_SESSION\_INFO\_PTR pInfo)  
*Retrieve information about the specified session.*
- **CK\_RV C\_GetOperationState** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pOperationState, CK\_ULONG\_PTR pulOperationStateLen)  
*Obtains the cryptographic operations state of a session.*
- **CK\_RV C\_SetOperationState** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pOperationState, CK\_ULONG ulOperationStateLen, CK\_OBJECT\_HANDLE hEncryptionKey, CK\_OBJECT\_HANDLE hAuthenticationKey)  
*Sets the cryptographic operations state of a session.*
- **CK\_RV C\_Login** (CK\_SESSION\_HANDLE hSession, CK\_USER\_TYPE userType, CK\_UTF8CHAR\_PTR pPin, CK\_ULONG ulPinLen)  
*Login on the token in the specified session.*
- **CK\_RV C\_Logout** (CK\_SESSION\_HANDLE hSession)  
*Log out of the token in the specified session.*
- **CK\_RV C\_CreateObject** (CK\_SESSION\_HANDLE hSession, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount, CK\_OBJECT\_HANDLE\_PTR phObject)  
*Create a new object on the token in the specified session using the given attribute template.*
- **CK\_RV C\_CopyObject** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hObject, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount, CK\_OBJECT\_HANDLE\_PTR phNewObject)  
*Create a copy of the object with the specified handle.*
- **CK\_RV C\_DestroyObject** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hObject)  
*Destroy the specified object.*
- **CK\_RV C\_GetObjectSize** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hObject, CK\_ULONG\_PTR pulSize)  
*Obtains the size of an object in bytes.*
- **CK\_RV C\_GetAttributeValue** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hObject, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount)  
*Obtains an attribute value of an object.*
- **CK\_RV C\_SetAttributeValue** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hObject, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount)  
*Change or set the value of the specified attributes on the specified object.*
- **CK\_RV C\_FindObjectsInit** (CK\_SESSION\_HANDLE hSession, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount)  
*Initializes an object search in the specified session using the specified attribute template as search parameters.*
- **CK\_RV C\_FindObjects** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE\_PTR phObject, CK\_ULONG ulMaxObjectCount, CK\_ULONG\_PTR pulObjectCount)  
*Continue the search for objects in the specified session.*
- **CK\_RV C\_FindObjectsFinal** (CK\_SESSION\_HANDLE hSession)  
*Finishes an object search operation (and cleans up)*
- **CK\_RV C\_EncryptInit** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hKey)  
*Initializes an encryption operation using the specified mechanism and session.*
- **CK\_RV C\_Encrypt** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pEncryptedData, CK\_ULONG\_PTR pulEncryptedDataLen)  
*Perform a single operation encryption operation in the specified session.*
- **CK\_RV C\_EncryptUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ulPartLen, CK\_BYTE\_PTR pEncryptedPart, CK\_ULONG\_PTR pulEncryptedPartLen)  
*Continues a multiple-part encryption operation.*
- **CK\_RV C\_EncryptFinal** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pLastEncryptedPart, CK\_ULONG\_PTR pulLastEncryptedPartLen)  
*Finishes a multiple-part encryption operation.*

- **CK\_RV C\_DecryptInit** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hKey)  
*Initialize decryption using the specified object.*
- **CK\_RV C\_Decrypt** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pEncryptedData, CK\_ULONG ulEncryptedDataLen, CK\_BYTE\_PTR pData, CK\_ULONG\_PTR pulDataLen)  
*Perform a single operation decryption in the given session.*
- **CK\_RV C\_DecryptUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pEncryptedPart, CK\_ULONG ulEncryptedPartLen, CK\_BYTE\_PTR pPart, CK\_ULONG\_PTR pulPartLen)  
*Continues a multiple-part decryption operation.*
- **CK\_RV C\_DecryptFinal** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pLastPart, CK\_ULONG\_PTR pulLastPartLen)  
*Finishes a multiple-part decryption operation.*
- **CK\_RV C\_DigestInit** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism)  
*Initializes a message-digesting operation using the specified mechanism in the specified session.*
- **CK\_RV C\_Digest** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pDigest, CK\_ULONG\_PTR pulDigestLen)  
*Digest the specified data in a one-pass operation and return the resulting digest.*
- **CK\_RV C\_DigestUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ulPartLen)  
*Continues a multiple-part digesting operation.*
- **CK\_RV C\_DigestKey** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hKey)  
*Update a running digest operation by digesting a secret key with the specified handle.*
- **CK\_RV C\_DigestFinal** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pDigest, CK\_ULONG\_PTR pulDigestLen)  
*Finishes a multiple-part digesting operation.*
- **CK\_RV C\_SignInit** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hKey)  
*Initialize a signing operation using the specified key and mechanism.*
- **CK\_RV C\_Sign** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pSignature, CK\_ULONG\_PTR pulSignatureLen)  
*Sign the data in a single pass operation.*
- **CK\_RV C\_SignUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ulPartLen)  
*Continues a multiple-part signature operation.*
- **CK\_RV C\_SignFinal** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pSignature, CK\_ULONG\_PTR pulSignatureLen)  
*Finishes a multiple-part signature operation.*
- **CK\_RV C\_SignRecoverInit** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hKey)  
*Initializes a signature operation, where the data can be recovered from the signature.*
- **CK\_RV C\_SignRecover** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pSignature, CK\_ULONG\_PTR pulSignatureLen)  
*Signs single-part data, where the data can be recovered from the signature.*
- **CK\_RV C\_VerifyInit** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hKey)  
*Initializes a verification operation using the specified key and mechanism.*
- **CK\_RV C\_Verify** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pSignature, CK\_ULONG\_PTR pulSignatureLen)  
*Verifies a signature on single-part data.*
- **CK\_RV C\_VerifyUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ulPartLen)  
*Continues a multiple-part verification operation.*
- **CK\_RV C\_VerifyFinal** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pSignature, CK\_ULONG\_PTR pulSignatureLen)



*Finishes a multiple-part verification operation.*

- CK\_RV **C\_VerifyRecoverInit** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hKey)

*Initializes a verification operation where the data is recovered from the signature.*

- CK\_RV **C\_VerifyRecover** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pSignature, CK\_ULONG ulSignatureLen, CK\_BYTE\_PTR pData, CK\_ULONG\_PTR pulDataLen)

*Verifies a signature on single-part data, where the data is recovered from the signature.*

- CK\_RV **C\_DigestEncryptUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ulPartLen, CK\_BYTE\_PTR pEncryptedPart, CK\_ULONG\_PTR pulEncryptedPartLen)

*Continues simultaneous multiple-part digesting and encryption operations.*

- CK\_RV **C\_DecryptDigestUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pEncryptedPart, CK\_ULONG ulEncryptedPartLen, CK\_BYTE\_PTR pPart, CK\_ULONG\_PTR pulPartLen)

*Continues simultaneous multiple-part decryption and digesting operations.*

- CK\_RV **C\_SignEncryptUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ulPartLen, CK\_BYTE\_PTR pEncryptedPart, CK\_ULONG\_PTR pulEncryptedPartLen)

*Continues simultaneous multiple-part signature and encryption operations.*

- CK\_RV **C\_DecryptVerifyUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pEncryptedPart, CK\_ULONG ulEncryptedPartLen, CK\_BYTE\_PTR pPart, CK\_ULONG\_PTR pulPartLen)

*Continues simultaneous multiple-part decryption and verification operations.*

- CK\_RV **C\_GenerateKey** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_↔ ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount, CK\_OBJECT\_HANDLE\_PTR phKey)

*Generates a secret key using the specified mechanism.*

- CK\_RV **C\_GenerateKeyPair** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_ATTRIBUTE\_PTR pPublicKeyTemplate, CK\_ULONG ulPublicKeyAttributeCount, CK\_ATTRIBUTE\_PTR pPrivateKeyTemplate, CK\_ULONG ulPrivateKeyAttributeCount, CK\_OBJECT\_HANDLE\_PTR phPublicKey, CK\_OBJECT\_HANDLE\_PTR phPrivateKey)

*Generates a public-key/private-key pair using the specified mechanism.*

- CK\_RV **C\_WrapKey** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_↔ OBJECT\_HANDLE hWrappingKey, CK\_OBJECT\_HANDLE hKey, CK\_BYTE\_PTR pWrappedKey, CK\_↔ ULONG\_PTR pulWrappedKeyLen)

*Wraps (encrypts) the specified key using the specified wrapping key and mechanism.*

- CK\_RV **C\_UnwrapKey** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_↔ OBJECT\_HANDLE hUnwrappingKey, CK\_BYTE\_PTR pWrappedKey, CK\_ULONG ulWrappedKeyLen, CK\_↔ \_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulAttributeCount, CK\_OBJECT\_HANDLE\_PTR phKey)

*Unwraps (decrypts) the specified key using the specified unwrapping key.*

- CK\_RV **C\_DeriveKey** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_↔ \_OBJECT\_HANDLE hBaseKey, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulAttributeCount, CK\_↔ OBJECT\_HANDLE\_PTR phKey)

*Derive a key from the specified base key.*

- CK\_RV **C\_SeedRandom** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pSeed, CK\_ULONG ul\_↔ SeedLen)

*Mixes in additional seed material to the random number generator.*

- CK\_RV **C\_GenerateRandom** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR RandomData, CK\_↔ ULONG ulRandomLen)

*Generate the specified amount of random data.*

- CK\_RV **C\_GetFunctionStatus** (CK\_SESSION\_HANDLE hSession)

*Legacy function - see PKCS#11 v2.40.*

- CK\_RV **C\_CancelFunction** (CK\_SESSION\_HANDLE hSession)

*Legacy function.*

- CK\_RV **C\_WaitForSlotEvent** (CK\_FLAGS flags, CK\_SLOT\_ID\_PTR pSlot, CK\_VOID\_PTR pReserved)

*Wait for a slot event (token insertion, removal, etc) on the specified slot to occur.*

- CK\_RV **pkcs11\_mech\_get\_list** (CK\_SLOT\_ID slotID, CK\_MECHANISM\_TYPE\_PTR pMechanismList, CK\_ULONG\_PTR pulCount)

- CK\_RV **pkcs\_mech\_get\_info** (CK\_SLOT\_ID slotID, CK\_MECHANISM\_TYPE type, CK\_MECHANISM\_INFO\_PTR pInfo)
- CK\_RV **pkcs11\_object\_alloc** (CK\_SLOT\_ID slotId, pkcs11\_object\_ptr \*ppObject)
- CK\_RV **pkcs11\_object\_free** (pkcs11\_object\_ptr pObject)
- CK\_RV **pkcs11\_object\_check** (pkcs11\_object\_ptr \*ppObject, CK\_OBJECT\_HANDLE hObject)
- CK\_RV **pkcs11\_object\_get\_handle** (pkcs11\_object\_ptr pObject, CK\_OBJECT\_HANDLE\_PTR phObject)
- CK\_RV **pkcs11\_object\_get\_owner** (pkcs11\_object\_ptr pObject, CK\_SLOT\_ID\_PTR pSlotId)
- CK\_RV **pkcs11\_object\_get\_name** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV **pkcs11\_object\_get\_class** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV **pkcs11\_object\_get\_type** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV **pkcs11\_object\_get\_destroyable** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV **pkcs11\_object\_get\_size** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hObject, CK\_ULONG\_PTR pulSize)
- CK\_RV **pkcs11\_object\_find** (CK\_SLOT\_ID slotId, pkcs11\_object\_ptr \*ppObject, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount)
- CK\_RV **pkcs11\_object\_create** (CK\_SESSION\_HANDLE hSession, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount, CK\_OBJECT\_HANDLE\_PTR phObject)  
*Create a new object on the token in the specified session using the given attribute template.*
- CK\_RV **pkcs11\_object\_destroy** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hObject)  
*Destroy the specified object.*
- CK\_RV **pkcs11\_object\_deinit** (pkcs11\_lib\_ctx\_ptr pContext)
- ATCA\_STATUS **pkcs11\_object\_load\_handle\_info** ([ATCADevice](#) device, pkcs11\_lib\_ctx\_ptr pContext)
- CK\_RV **pkcs11\_object\_is\_private** (pkcs11\_object\_ptr pObject, CK\_BBOOL \*is\_private, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)  
*Checks the attributes of the underlying cryptographic asset to determine if it is a private key - this changes the way the associated public key is referenced.*
- CK\_RV [pkcs11\\_os\\_create\\_mutex](#) (CK\_VOID\_PTR\_PTR ppMutex)  
*Application callback for creating a mutex object.*
- CK\_RV **pkcs11\_os\_destroy\_mutex** (CK\_VOID\_PTR pMutex)
- CK\_RV **pkcs11\_os\_lock\_mutex** (CK\_VOID\_PTR pMutex)
- CK\_RV **pkcs11\_os\_unlock\_mutex** (CK\_VOID\_PTR pMutex)
- CK\_RV **pkcs11\_os\_alloc\_shared\_ctx** (void \*\*ppShared, size\_t size)
- CK\_RV **pkcs11\_os\_free\_shared\_ctx** (void \*pShared, size\_t size)
- [pkcs11\\_session\\_ctx\\_ptr](#) **pkcs11\_get\_session\_context** (CK\_SESSION\_HANDLE hSession)
- CK\_RV **pkcs11\_session\_check** ([pkcs11\\_session\\_ctx\\_ptr](#) \*pSession, CK\_SESSION\_HANDLE hSession)  
*Check if the session is initialized properly.*
- CK\_RV **pkcs11\_reserve\_resource** (pkcs11\_lib\_ctx\_ptr pContext, [pkcs11\\_session\\_ctx\\_ptr](#) pSession, uint8\_t resource)
- CK\_RV **pkcs11\_release\_resource** (pkcs11\_lib\_ctx\_ptr pContext, [pkcs11\\_session\\_ctx\\_ptr](#) pSession, uint8\_t resource)
- CK\_RV **pkcs11\_session\_open** (CK\_SLOT\_ID slotID, CK\_FLAGS flags, CK\_VOID\_PTR pApplication, CK\_NOTIFY\_PTR notify, CK\_SESSION\_HANDLE\_PTR phSession)
- CK\_RV **pkcs11\_session\_close** (CK\_SESSION\_HANDLE hSession)
- CK\_RV [pkcs11\\_session\\_closeall](#) (CK\_SLOT\_ID slotID)  
*Close all sessions for a given slot - not actually all open sessions.*
- CK\_RV **pkcs11\_session\_get\_info** (CK\_SESSION\_HANDLE hSession, CK\_SESSION\_INFO\_PTR pInfo)  
*Obtains information about a particular session.*
- CK\_RV [pkcs11\\_session\\_login](#) (CK\_SESSION\_HANDLE hSession, CK\_USER\_TYPE userType, CK\_UTF8CHAR\_PTR pPin, CK\_ULONG ulPinLen)
- CK\_RV **pkcs11\_session\_logout** (CK\_SESSION\_HANDLE hSession)

- CK\_RV **pkcs11\_signature\_sign\_init** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hKey)  
*Initialize a signing operation using the specified key and mechanism.*
- CK\_RV **pkcs11\_signature\_sign** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pSignature, CK\_ULONG\_PTR pulSignatureLen)  
*Sign the data in a single pass operation.*
- CK\_RV **pkcs11\_signature\_sign\_continue** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ulPartLen)  
*Continues a multiple-part signature operation.*
- CK\_RV **pkcs11\_signature\_sign\_finish** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pSignature, CK\_ULONG\_PTR pulSignatureLen)  
*Finishes a multiple-part signature operation.*
- CK\_RV **pkcs11\_signature\_verify\_init** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hKey)  
*Initializes a verification operation using the specified key and mechanism.*
- CK\_RV **pkcs11\_signature\_verify** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pSignature, CK\_ULONG ulSignatureLen)  
*Verifies a signature on single-part data.*
- CK\_RV **pkcs11\_signature\_verify\_continue** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ulPartLen)  
*Continues a multiple-part verification operation.*
- CK\_RV **pkcs11\_signature\_verify\_finish** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pSignature, CK\_ULONG ulSignatureLen)  
*Finishes a multiple-part verification operation.*
- pkcs11\_slot\_ctx\_ptr **pkcs11\_slot\_get\_context** (pkcs11\_lib\_ctx\_ptr lib\_ctx, CK\_SLOT\_ID slotID)  
*Retrieve the current slot context.*
- pkcs11\_slot\_ctx\_ptr **pkcs11\_slot\_get\_new\_context** (pkcs11\_lib\_ctx\_ptr lib\_ctx)
- CK\_VOID\_PTR **pkcs11\_slot\_initslots** (CK\_ULONG pulCount)
- CK\_RV **pkcs11\_slot\_deinitslots** (pkcs11\_lib\_ctx\_ptr lib\_ctx)
- CK\_RV **pkcs11\_slot\_config** (CK\_SLOT\_ID slotID)
- CK\_RV **pkcs11\_slot\_init** (CK\_SLOT\_ID slotID)  
*This is an internal function that initializes a pkcs11 slot - it must already have the locks in place before being called.*
- CK\_RV **pkcs11\_slot\_get\_list** (CK\_BBOOL tokenPresent, CK\_SLOT\_ID\_PTR pSlotList, CK\_ULONG\_PTR pulCount)
- CK\_RV **pkcs11\_slot\_get\_info** (CK\_SLOT\_ID slotID, CK\_SLOT\_INFO\_PTR pInfo)  
*Obtains information about a particular slot.*
- CK\_RV **pkcs11\_token\_init** (CK\_SLOT\_ID slotID, CK\_UTF8CHAR\_PTR pPin, CK\_ULONG ulPinLen, CK\_UTF8CHAR\_PTR pLabel)
- CK\_RV **pkcs11\_token\_get\_access\_type** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, pkcs11\_session\_ctx\_ptr pSession)
- CK\_RV **pkcs11\_token\_get\_writable** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, pkcs11\_session\_ctx\_ptr pSession)
- CK\_RV **pkcs11\_token\_get\_storage** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, pkcs11\_session\_ctx\_ptr pSession)
- CK\_RV **pkcs11\_token\_get\_info** (CK\_SLOT\_ID slotID, CK\_TOKEN\_INFO\_PTR pInfo)  
*Obtains information about a particular token.*
- CK\_RV **pkcs11\_token\_random** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pRandomData, CK\_ULONG ulRandomLen)  
*Generate the specified amount of random data.*
- CK\_RV **pkcs11\_token\_convert\_pin\_to\_key** (const CK\_UTF8CHAR\_PTR pPin, const CK\_ULONG ulPinLen, const CK\_UTF8CHAR\_PTR pSalt, const CK\_ULONG ulSaltLen, CK\_BYTE\_PTR pKey, CK\_ULONG ulKeyLen, pkcs11\_slot\_ctx\_ptr slot\_ctx)
- CK\_RV **pkcs11\_token\_set\_pin** (CK\_SESSION\_HANDLE hSession, CK\_UTF8CHAR\_PTR pOldPin, CK\_ULONG ulOldLen, CK\_UTF8CHAR\_PTR pNewPin, CK\_ULONG ulNewLen)

- void **pkcs11\_util\_escape\_string** (CK\_UTF8CHAR\_PTR buf, CK\_ULONG buf\_len)
- CK\_RV **pkcs11\_util\_convert\_rv** (ATCA\_STATUS status)
- int **pkcs11\_util\_memset** (void \*dest, size\_t destsz, int ch, size\_t count)

### Variables

- const [pkcs11\\_attrib\\_model](#) **pkcs11\_cert\_x509public\_attributes** []
- const CK\_ULONG **pkcs11\_cert\_x509public\_attributes\_count** = (CK\_ULONG)(sizeof( [pkcs11\\_cert\\_x509public\\_attributes](#) ) / sizeof( [pkcs11\\_cert\\_x509public\\_attributes](#) [0]))
- const [pkcs11\\_attrib\\_model](#) **pkcs11\_cert\_wtlspublic\_attributes** []
- const CK\_ULONG **pkcs11\_cert\_wtlspublic\_attributes\_count** = (CK\_ULONG)(sizeof( [pkcs11\\_cert\\_wtlspublic\\_attributes](#) ) / sizeof( [pkcs11\\_cert\\_wtlspublic\\_attributes](#) [0]))
- const [pkcs11\\_attrib\\_model](#) **pkcs11\_cert\_x509\_attributes** []
- const CK\_ULONG **pkcs11\_cert\_x509\_attributes\_count** = (CK\_ULONG)(sizeof( [pkcs11\\_cert\\_x509\\_attributes](#) ) / sizeof( [pkcs11\\_cert\\_x509\\_attributes](#) [0]))
- const char **pkcs11\_lib\_manufacturer\_id** [] = "Microchip Technology Inc"
- const char **pkcs11\_lib\_description** [] = "Cryptoauthlib PKCS11 Interface"
- CK\_BYTE [pkcs11\\_ec\\_pbkey\\_asn1\\_hdr\\_p256](#) []
- CK\_BYTE [pkcs11\\_x962\\_asn1\\_hdr\\_ec256](#) []
- CK\_BYTE **pkcs11\_key\_ec\_params\_p256** [] = { 0x06, 0x08, 0x2a, 0x86, 0x48, 0xce, 0x3d, 0x03, 0x01, 0x07 }
- CK\_BYTE [pkcs11\\_ec\\_pbkey\\_asn1\\_hdr\\_p224](#) []
- CK\_BYTE [pkcs11\\_x962\\_asn1\\_hdr\\_ec224](#) []
- CK\_BYTE **pkcs11\_key\_ec\_params\_p224** [] = { 0x06, 0x05, 0x2B, 0x81, 0x04, 0x00, 0x21 }
- CK\_BYTE [pkcs11\\_ec\\_pbkey\\_asn1\\_hdr\\_p384](#) []
- CK\_BYTE **pkcs11\_key\_ec\_params\_p384** [] = { 0x06, 0x05, 0x2B, 0x81, 0x04, 0x00, 0x22 }
- CK\_BYTE [pkcs11\\_x962\\_asn1\\_hdr\\_ec384](#) []
- CK\_BYTE [pkcs11\\_ec\\_pbkey\\_asn1\\_hdr\\_p521](#) []
- CK\_BYTE [pkcs11\\_x962\\_asn1\\_hdr\\_ec521](#) []
- CK\_BYTE **pkcs11\_key\_ec\_params\_p521** [] = { 0x06, 0x05, 0x2B, 0x81, 0x04, 0x00, 0x23 }
- const [pkcs11\\_ecc\\_key\\_info\\_t](#) **ec\_key\_data\_table** [4]
- const [pkcs11\\_attrib\\_model](#) **pkcs11\_key\_public\_attributes** []
- const CK\_ULONG **pkcs11\_key\_public\_attributes\_count** = (CK\_ULONG)(sizeof( [pkcs11\\_key\\_public\\_attributes](#) ) / sizeof( [pkcs11\\_key\\_public\\_attributes](#) [0]))
- const [pkcs11\\_attrib\\_model](#) **pkcs11\_key\_private\_attributes** []
- const CK\_ULONG **pkcs11\_key\_private\_attributes\_count** = (CK\_ULONG)(sizeof( [pkcs11\\_key\\_private\\_attributes](#) ) / sizeof( [pkcs11\\_key\\_private\\_attributes](#) [0]))
- const [pkcs11\\_attrib\\_model](#) **pkcs11\_key\_secret\_attributes** []
- const CK\_ULONG **pkcs11\_key\_secret\_attributes\_count** = (CK\_ULONG)(sizeof( [pkcs11\\_key\\_secret\\_attributes](#) ) / sizeof( [pkcs11\\_key\\_secret\\_attributes](#) [0]))
- [pkcs11\\_object\\_cache\\_t](#) **pkcs11\_object\_cache** [PKCS11\_MAX\_OBJECTS\_ALLOWED]
- const [pkcs11\\_attrib\\_model](#) **pkcs11\_object\_monotonic\_attributes** []
- const CK\_ULONG **pkcs11\_object\_monotonic\_attributes\_count** = (CK\_ULONG)(sizeof( [pkcs11\\_object\\_monotonic\\_attributes](#) ) / sizeof( [pkcs11\\_object\\_monotonic\\_attributes](#) [0]))

### 19.13.1 Detailed Description

### 19.13.2 Function Documentation

### 19.13.2.1 pkcs11\_attrib\_fill()

```
CK_RV pkcs11_attrib_fill (
    CK_ATTRIBUTE_PTR pAttribute,
    const void * pData,
    const CK_ULONG ulSize )
```

Perform the nessasary checks and copy data into an attribute structure.

The ulValueLen field is modified to hold the exact length of the specified attribute for the object. In the special case of an attribute whose value is an array of attributes, for example CKA\_WRAP\_TEMPLATE, where it is passed in with pValue not NULL, then if the pValue of elements within the array is NULL\_PTR then the ulValueLen of elements within the array will be set to the required length. If the pValue of elements within the array is not NULL\_PTR, then the ulValueLen element of attributes within the array MUST reflect the space that the corresponding pValue points to, and pValue is filled in if there is sufficient room. Therefore it is important to initialize the contents of a buffer before calling C\_GetAttributeValue to get such an array value. If any ulValueLen within the array isn't large enough, it will be set to CK\_UNAVAILABLE\_INFORMATION and the function will return CKR\_BUFFER\_TOO\_SMALL, as it does if an attribute in the pTemplate argument has ulValueLen too small. Note that any attribute whose value is an array of attributes is identifiable by virtue of the attribute type having the CKF\_ARRAY\_ATTRIBUTE bit set.

### 19.13.2.2 pkcs11\_deinit()

```
CK_RV pkcs11_deinit (
    CK_VOID_PTR pReserved )
```

### 19.13.2.3 pkcs11\_init()

```
CK_RV pkcs11_init (
    CK_C_INITIALIZE_ARGS const * pInitArgs )
```

Initializes the PKCS11 API Library for Cryptoauthlib.

### 19.13.2.4 pkcs11\_os\_create\_mutex()

```
CK_RV pkcs11_os_create_mutex (
    CK_VOID_PTR_PTR ppMutex )
```

Application callback for creating a mutex object.

#### Parameters

in, out	<i>ppMutex</i>	location to receive ptr to mutex
---------	----------------	----------------------------------

### 19.13.2.5 pkcs11\_session\_closeall()

```
CK_RV pkcs11_session_closeall (
    CK_SLOT_ID slotID )
```

Close all sessions for a given slot - not actually all open sessions.

for specified slotid close all sessions related with it.

### 19.13.2.6 pkcs11\_session\_login()

```
CK_RV pkcs11_session_login (
    CK_SESSION_HANDLE hSession,
    CK_USER_TYPE userType,
    CK_UTF8CHAR_PTR pPin,
    CK_ULONG ulPinLen )
```

Reserve the PKCS11\_AUTH\_OP\_0 / PKCS11\_AUTH\_OP\_1 based on availability

Auth operation unavailable return error

### 19.13.2.7 pkcs11\_token\_init()

```
CK_RV pkcs11_token_init (
    CK_SLOT_ID slotID,
    CK_UTF8CHAR_PTR pPin,
    CK_ULONG ulPinLen,
    CK_UTF8CHAR_PTR pLabel )
```

Write the configuration into the device and generate new keys

## 19.13.3 Variable Documentation

### 19.13.3.1 ec\_key\_data\_table

```
const pkcs11_ecc_key_info_t ec_key_data_table[4]
```

Initial value:

```
= {
    { ATCA_KEY_TYPE_ECCP256, (CK_BYTE)ATCA_ECCP256_OID_SIZE, pkcs11_key_ec_params_p256,
      pkcs11_ec_pbkey_asn1_hdr_p256,
      pkcs11_x962_asn1_hdr_ec256, (uint16_t)ATCA_ECCP256_ASN1_HDR_SIZE, ATCA_ECCP256_PUBKEY_SIZE,
      ATCA_ECCP256_MSG_SIZE, ATCA_ECCP256_SIG_SIZE },
    { TA_KEY_TYPE_ECCP224, (CK_BYTE)TA_ECC224_OID_SIZE, pkcs11_key_ec_params_p224,
      pkcs11_ec_pbkey_asn1_hdr_p224,
      pkcs11_x962_asn1_hdr_ec224, (uint16_t)TA_ECC224_ASN1_HDR_SIZE, TA_ECC224_PUB_KEY_SIZE,
      TA_SIGN_P224_MSG_SIZE, TA_SIGN_P224_SIG_SIZE },
    { TA_KEY_TYPE_ECCP384, (CK_BYTE)TA_ECC384_OID_SIZE, pkcs11_key_ec_params_p384,
      pkcs11_ec_pbkey_asn1_hdr_p384,
      pkcs11_x962_asn1_hdr_ec384, (uint16_t)TA_ECC384_ASN1_HDR_SIZE, TA_ECC384_PUB_KEY_SIZE,
      TA_SIGN_P384_MSG_SIZE, TA_SIGN_P384_SIG_SIZE },
    { TA_KEY_TYPE_ECCP521, (CK_BYTE)TA_ECC521_OID_SIZE, pkcs11_key_ec_params_p521,
      pkcs11_ec_pbkey_asn1_hdr_p521,
      pkcs11_x962_asn1_hdr_ec521, (uint16_t)TA_ECC521_ASN1_HDR_SIZE, TA_ECC521_PUB_KEY_SIZE,
      TA_SIGN_P521_MSG_SIZE, TA_SIGN_P521_SIG_SIZE },
}
```

### 19.13.3.2 pkcs11\_cert\_wtlspublic\_attributes

```
const pkcs11_attr_model pkcs11_cert_wtlspublic_attributes[]
```

CKO\_CERTIFICATE (Type: CKC\_WTLS) - WTLS Public Key Certificate Model

### 19.13.3.3 pkcs11\_cert\_x509\_attributes

```
const pkcs11_attr_model pkcs11_cert_x509_attributes[]
```

CKO\_CERTIFICATE (Type: CKC\_X\_509\_ATTR\_CERT) - X509 Attribute Certificate Model

### 19.13.3.4 pkcs11\_cert\_x509public\_attributes

```
const pkcs11_attr_model pkcs11_cert_x509public_attributes[]
```

CKO\_CERTIFICATE (Type: CKC\_X\_509) - X509 Public Key Certificate Model

### 19.13.3.5 pkcs11\_ec\_pbkey\_asn1\_hdr\_p224

```
CK_BYTE pkcs11_ec_pbkey_asn1_hdr_p224[]
```

#### Initial value:

```
= {
    0x30, 0x4e,
    0x30, 0x10,
    0x06, 0x07,
    0x2a, 0x86, 0x48, 0xce, 0x3d, 0x02, 0x01,
    0x06, 0x05, 0x2b, 0x81, 0x04, 0x00, 0x21,
    0x03, 0x3a, 0x00,
    0x04
}
```

ASN.1 Header for SECP224R1 public keys

### 19.13.3.6 pkcs11\_ec\_pbkey\_asn1\_hdr\_p256

```
CK_BYTE pkcs11_ec_pbkey_asn1_hdr_p256[]
```

#### Initial value:

```
= {
    0x30, 0x59,
    0x30, 0x13,
    0x06, 0x07,
    0x2a, 0x86, 0x48, 0xce, 0x3d, 0x02, 0x01,
    0x06, 0x08, 0x2a, 0x86, 0x48, 0xce, 0x3d, 0x03, 0x01, 0x07,
    0x03, 0x42, 0x00,
    0x04
}
```

ASN.1 Header for SECP256R1 public keys

### 19.13.3.7 pkcs11\_ec\_pbkey\_asn1\_hdr\_p384

```
CK_BYTE pkcs11_ec_pbkey_asn1_hdr_p384[ ]
```

#### Initial value:

```
= {  
    0x30, 0x76,  
    0x30, 0x10,  
    0x06, 0x07,  
    0x2a, 0x86, 0x48, 0xce, 0x3d, 0x02, 0x01,  
    0x06, 0x05,  
    0x2b, 0x81, 0x04, 0x00, 0x22,  
    0x03, 0x62, 0x00,  
    0x04  
}
```

ASN.1 Header for SECP384R1 public keys

### 19.13.3.8 pkcs11\_ec\_pbkey\_asn1\_hdr\_p521

```
CK_BYTE pkcs11_ec_pbkey_asn1_hdr_p521[ ]
```

#### Initial value:

```
= {  
    0x30, 0x81, 0x9b,  
    0x30, 0x10,  
    0x06, 0x07,  
    0x2a, 0x86, 0x48, 0xce, 0x3d, 0x02, 0x01,  
    0x06, 0x05,  
    0x2b, 0x81, 0x04, 0x00, 0x23,  
    0x03, 0x81, 0x86, 0x00,  
    0x04  
}
```

ASN.1 Header for SECP521R1 public keys

### 19.13.3.9 pkcs11\_key\_private\_attributes

```
const pkcs11_attrib_model pkcs11_key_private_attributes[ ]
```

CKO\_PRIVATE\_KEY - Private Key Object Base Model

### 19.13.3.10 pkcs11\_key\_public\_attributes

```
const pkcs11_attrib_model pkcs11_key_public_attributes[ ]
```

CKO\_PUBLIC\_KEY - Public Key Object Model

### 19.13.3.11 pkcs11\_key\_secret\_attributes

```
const pkcs11_attrib_model pkcs11_key_secret_attributes[ ]
```

CKO\_SECRET\_KEY - Secret Key Object Base Model



### 19.13.3.12 pkcs11\_object\_monotonic\_attributes

```
const pkcs11_attr_model pkcs11_object_monotonic_attributes[]
```

**Initial value:**

```
= {  
    { 0x00000000UL ,      pkcs11_object_get_class },  
    { 0x00000300UL , pkcs11_object_get_type  },  
    { 0x00000301UL ,  pkcs11_attr_false    },  
    { 0x00000302UL ,      pkcs11_attr_false    },  
    { 0x00000011UL ,          0              },  
}
```

CKA\_CLASS == CKO\_HW\_FEATURE\_TYPE CKA\_HW\_FEATURE\_TYPE == CKH\_MONOTONIC\_COUNTER

### 19.13.3.13 pkcs11\_x962\_asn1\_hdr\_ec224

```
CK_BYTE pkcs11_x962_asn1_hdr_ec224[]
```

**Initial value:**

```
= {  
    0x04, 0x39, 0x04  
}
```

X.962 ASN.1 Header for EC224 public keys

### 19.13.3.14 pkcs11\_x962\_asn1\_hdr\_ec256

```
CK_BYTE pkcs11_x962_asn1_hdr_ec256[]
```

**Initial value:**

```
= {  
    0x04, 0x41, 0x04  
}
```

X.962 ASN.1 Header for EC256 public keys

### 19.13.3.15 pkcs11\_x962\_asn1\_hdr\_ec384

```
CK_BYTE pkcs11_x962_asn1_hdr_ec384[]
```

**Initial value:**

```
= {  
    0x04, 0x61, 0x04  
}
```

X.962 ASN.1 Header for EC384 public keys

### 19.13.3.16 pkcs11\_x962\_asn1\_hdr\_ec521

```
CK_BYTE pkcs11_x962_asn1_hdr_ec521[]
```

**Initial value:**

```
= {  
    0x04, 0x85, 0x04  
}
```

X.962 ASN.1 Header for EC521 public keys

## Chapter 20

# Namespace Documentation

### 20.1 cryptoauthlib Namespace Reference

#### Namespaces

- namespace [atcab](#)
- namespace [atcacert](#)
- namespace [atcaenum](#)
- namespace [atjwt](#)
- namespace [device](#)
- namespace [exceptions](#)
- namespace [iface](#)
- namespace [library](#)
- namespace [sha206\\_api](#)
- namespace [status](#)
- namespace [tng](#)

#### Variables

- **try :**
- `os_lib_definition_file = os.path.join(os.path.dirname(__file__), 'cryptoauth.json')`

#### 20.1.1 Detailed Description

Package Definition

### 20.2 cryptoauthlib.atcab Namespace Reference

#### Data Structures

- class [atca\\_aes\\_cbc\\_ctx](#)
- class [atca\\_aes\\_cbcmac\\_ctx](#)
- class [atca\\_aes\\_ccm\\_ctx](#)
- class [atca\\_aes\\_cmac\\_ctx](#)
- class [atca\\_aes\\_ctr\\_ctx](#)
- class [atca\\_aes\\_gcm\\_ctx](#)
- class [atca\\_hmac\\_sha256\\_ctx](#)
- class [atca\\_sha256\\_ctx](#)

## Functions

- def [atcab\\_init](#) (iface\_cfg)
- def [atcab\\_release](#) ()
- def [atcab\\_get\\_device](#) ()
- def [atcab\\_get\\_device\\_type](#) ()
- def [atcab\\_aes](#) (mode, key\_id, aes\_in, aes\_out)
- def [atcab\\_aes\\_encrypt](#) (key\_id, key\_block, plaintext, ciphertext)
- def [atcab\\_aes\\_decrypt](#) (key\_id, key\_block, ciphertext, plaintext)
- def [atcab\\_aes\\_gfm](#) (hash\_key, inp, output)
- def [atcab\\_aes\\_cbc\\_init](#) (ctx, key\_id, key\_block, iv)
- def [atcab\\_aes\\_cbc\\_encrypt\\_block](#) (ctx, plaintext, ciphertext)
- def [atcab\\_aes\\_cbc\\_decrypt\\_block](#) (ctx, ciphertext, plaintext)
- def [atcab\\_aes\\_cmac\\_init](#) (ctx, key\_id, key\_block)
- def [atcab\\_aes\\_cmac\\_update](#) (ctx, data, data\_size)
- def [atcab\\_aes\\_cmac\\_finish](#) (ctx, cmac, size)
- def [atcab\\_aes\\_ctr\\_init](#) (ctx, key\_id, key\_block, counter\_size, iv)
- def [atcab\\_aes\\_ctr\\_init\\_rand](#) (ctx, key\_id, key\_block, counter\_size, iv)
- def [atcab\\_aes\\_ctr\\_encrypt\\_block](#) (ctx, plaintext, ciphertext)
- def [atcab\\_aes\\_ctr\\_decrypt\\_block](#) (ctx, ciphertext, plaintext)
- def [atcab\\_aes\\_gcm\\_init](#) (ctx, key\_id, key\_block, iv, iv\_size)
- def [atcab\\_aes\\_gcm\\_init\\_rand](#) (ctx, key\_id, key\_block, rand\_size, free\_field, free\_field\_size, iv)
- def [atcab\\_aes\\_gcm\\_aad\\_update](#) (ctx, aad, aad\_size)
- def [atcab\\_aes\\_gcm\\_encrypt\\_update](#) (ctx, plaintext, plaintext\_size, ciphertext)
- def [atcab\\_aes\\_gcm\\_encrypt\\_finish](#) (ctx, tag, tag\_size)
- def [atcab\\_aes\\_gcm\\_decrypt\\_update](#) (ctx, ciphertext, ciphertext\_size, plaintext)
- def [atcab\\_aes\\_gcm\\_decrypt\\_finish](#) (ctx, tag, tag\_size, is\_verified)
- def [atcab\\_aes\\_cbcmac\\_init](#) (ctx, key\_id, key\_block)
- def [atcab\\_aes\\_cbcmac\\_update](#) (ctx, data, data\_size)
- def [atcab\\_aes\\_cbcmac\\_finish](#) (ctx, mac, mac\_size)
- def [atcab\\_aes\\_ccm\\_init](#) (ctx, key\_id, key\_block, iv, iv\_size, aad\_size, text\_size, tag\_size)
- def [atcab\\_aes\\_ccm\\_init\\_rand](#) (ctx, key\_id, key\_block, iv, iv\_size, aad\_size, text\_size, tag\_size)
- def [atcab\\_aes\\_ccm\\_aad\\_update](#) (ctx, aad, aad\_size)
- def [atcab\\_aes\\_ccm\\_aad\\_finish](#) (ctx)
- def [atcab\\_aes\\_ccm\\_encrypt\\_update](#) (ctx, plaintext, plaintext\_size, ciphertext)
- def [atcab\\_aes\\_ccm\\_decrypt\\_update](#) (ctx, ciphertext, ciphertext\_size, plaintext)
- def [atcab\\_aes\\_ccm\\_encrypt\\_finish](#) (ctx, tag, tag\_size)
- def [atcab\\_aes\\_ccm\\_decrypt\\_finish](#) (ctx, tag, is\_verified)
- def [atcab\\_checkmac](#) (mode, key\_id, challenge, response, other\_data)
- def [atcab\\_counter](#) (mode, counter\_id, counter\_value)
- def [atcab\\_counter\\_increment](#) (counter\_id, counter\_value)
- def [atcab\\_counter\\_read](#) (counter\_id, counter\_value)
- def [atcab\\_derivekey](#) (mode, target\_key, mac)
- def [atcab\\_ecdh\\_base](#) (mode, key\_id, public\_key, pms, out\_nonce)
- def [atcab\\_ecdh](#) (key\_id, public\_key, pms)
- def [atcab\\_ecdh\\_enc](#) (key\_id, public\_key, pms, read\_key, read\_key\_id, num\_in=None)
- def [atcab\\_ecdh\\_ioenc](#) (key\_id, public\_key, pms, io\_key)
- def [atcab\\_ecdh\\_tempkey](#) (public\_key, pms)
- def [atcab\\_ecdh\\_tempkey\\_ioenc](#) (public\_key, pms, io\_key)
- def [atcab\\_gendig](#) (zone, key\_id, other\_data, other\_data\_size)
- def [atcab\\_genkey\\_base](#) (mode, key\_id, other\_data, public\_key=None)
- def [atcab\\_genkey](#) (key\_id, public\_key)
- def [atcab\\_get\\_pubkey](#) (key\_id, public\_key)
- def [atcab\\_hmac](#) (mode, key\_id, digest)
- def [atcab\\_info\\_base](#) (mode, param2, out\_data)

- def [atcab\\_info](#) (revision)
- def [atcab\\_info\\_get\\_latch](#) (state)
- def [atcab\\_info\\_set\\_latch](#) (state)
- def [atcab\\_kdf](#) (mode, key\_id, details, message, out\_data, out\_nonce)
- def [atcab\\_lock](#) (mode, summary\_crc)
- def [atcab\\_lock\\_config\\_zone](#) ()
- def [atcab\\_lock\\_config\\_zone\\_crc](#) (summary\_crc)
- def [atcab\\_lock\\_data\\_zone](#) ()
- def [atcab\\_lock\\_data\\_zone\\_crc](#) (summary\_crc)
- def [atcab\\_lock\\_data\\_slot](#) (slot)
- def [atcab\\_mac](#) (mode, key\_id, challenge, digest)
- def [atcab\\_nonce\\_base](#) (mode, zero, num\_in, rand\_out)
- def [atcab\\_nonce](#) (num\_in)
- def [atcab\\_nonce\\_load](#) (target, num\_in, num\_in\_size)
- def [atcab\\_nonce\\_rand](#) (num\_in, rand\_out)
- def [atcab\\_challenge](#) (num\_in)
- def [atcab\\_challenge\\_seed\\_update](#) (num\_in, rand\_out)
- def [atcab\\_priv\\_write](#) (key\_id, priv\_key, write\_key\_id, write\_key, num\_in=None)
- def [atcab\\_random](#) (random\_number)
- def [atcab\\_read\\_zone](#) (zone, slot, block, offset, data, length)
- def [atcab\\_read\\_serial\\_number](#) (serial\_number)
- def [atcab\\_is\\_slot\\_locked](#) (slot, is\_locked)
- def [atcab\\_is\\_locked](#) (zone, is\_locked)
- def [atcab\\_read\\_enc](#) (key\_id, block, data, enc\_key, enc\_key\_id, num\_in=None)
- def [atcab\\_read\\_config\\_zone](#) (config\_data)
- def [atcab\\_cmp\\_config\\_zone](#) (config\_data, same\_config)
- def [atcab\\_read\\_sig](#) (slot, sig)
- def [atcab\\_read\\_pubkey](#) (slot, public\_key)
- def [atcab\\_read\\_bytes\\_zone](#) (zone, slot, offset, data, length)
- def [atcab\\_secureboot](#) (mode, param2, digest, signature, mac)
- def [atcab\\_secureboot\\_mac](#) (mode, digest, signature, num\_in, io\_keys, is\_verified)
- def [atcab\\_selftest](#) (mode, param2, result)
- def [atcab\\_sha\\_base](#) (mode, length, message, data\_out, data\_out\_size)
- def [atcab\\_sha\\_start](#) ()
- def [atcab\\_sha\\_update](#) (message)
- def [atcab\\_sha\\_end](#) (digest, length, message)
- def [atcab\\_sha\\_read\\_context](#) (context, context\_size)
- def [atcab\\_sha\\_write\\_context](#) (context, context\_size)
- def [atcab\\_sha](#) (length, message, digest)
- def [atcab\\_hw\\_sha2\\_256\\_init](#) (ctx)
- def [atcab\\_hw\\_sha2\\_256\\_update](#) (ctx, data, data\_size)
- def [atcab\\_hw\\_sha2\\_256\\_finish](#) (ctx, digest)
- def [atcab\\_hw\\_sha2\\_256](#) (data, data\_size, digest)
- def [atcab\\_sha\\_hmac\\_init](#) (ctx, key\_slot)
- def [atcab\\_sha\\_hmac\\_update](#) (ctx, data, data\_size)
- def [atcab\\_sha\\_hmac\\_finish](#) (ctx, digest, target)
- def [atcab\\_sha\\_hmac](#) (data, data\_size, key\_slot, digest, target)
- def [atcab\\_sign\\_base](#) (mode, key\_id, signature)
- def [atcab\\_sign](#) (key\_id, msg, signature)
- def [atcab\\_sign\\_internal](#) (key\_id, is\_invalidate, is\_full\_sn, signature)
- def [atcab\\_updateextra](#) (mode, new\_value)
- def [atcab\\_verify](#) (mode, key\_id, signature, public\_key, other\_data, mac)
- def [atcab\\_verify\\_extern\\_stored\\_mac](#) (mode, key\_id, message, signature, public\_key, num\_in, io\_key, is\_↵  
verified)
- def [atcab\\_verify\\_extern](#) (message, signature, public\_key, is\_verified)

- def [atcab\\_verify\\_extern\\_mac](#) (message, signature, public\_key, num\_in, io\_key, is\_verified)
- def [atcab\\_verify\\_stored](#) (message, signature, key\_id, is\_verified)
- def [atcab\\_verify\\_stored\\_mac](#) (message, signature, key\_id, num\_in, io\_key, is\_verified)
- def [atcab\\_verify\\_validate](#) (key\_id, signature, other\_data, is\_verified)
- def [atcab\\_verify\\_invalidate](#) (key\_id, signature, other\_data, is\_verified)
- def [atcab\\_write](#) (zone, [address](#), value, mac)
- def [atcab\\_write\\_zone](#) (zone, slot, block, offset, data, length)
- def [atcab\\_write\\_enc](#) (key\_id, block, data, enc\_key, enc\_key\_id, num\_in=None)
- def [atcab\\_write\\_config\\_zone](#) (conf)
- def [atcab\\_write\\_pubkey](#) (slot, public\_key)
- def [atcab\\_write\\_bytes\\_zone](#) (zone, slot, offset\_bytes, data, length)
- def [atcab\\_write\\_config\\_counter](#) (counter\_id, counter\_value)

## 20.2.1 Detailed Description

Dynamic link library loading under ctypes and HAL initialization/release functions

## 20.2.2 Function Documentation

### 20.2.2.1 [atcab\\_aes\(\)](#)

```
def cryptoauthlib.atcab.atcab_aes (
    mode,
    key_id,
    aes_in,
    aes_out )
```

Compute the AES-128 encrypt, decrypt, or GFM calculation.

#### Args:

mode	The mode for the AES command. (int)
key_id	Key location. Can either be a slot number or ATCA_TEMPKEY_KEYID for TempKey. (int)
aes_in	Input data to the AES command (16 bytes). (Can be of type bytearray or bytes)
aes_out	Output data from the AES command is returned here (16 bytes). (Expects bytearray of size 16)

#### Returns:

Status Code

### 20.2.2.2 atcab\_aes\_cbc\_decrypt\_block()

```
def cryptoauthlib.atcab.atcab_aes_cbc_decrypt_block (
    ctx,
    ciphertext,
    plaintext )
```

Decrypt a block of data using CBC mode and a key within the ATECC608. `atcab_aes_cbc_init()` should be called before the first use of this function.

Args:

<code>ctx</code>	AES CBC context.
<code>ciphertext</code>	Ciphertext to be decrypted (16 bytes). (Bytearray or bytes)
<code>plaintext</code>	Decrypted data is returned here (16 bytes). (Bytearray or bytes)

Returns:

Status code

### 20.2.2.3 atcab\_aes\_cbc\_encrypt\_block()

```
def cryptoauthlib.atcab.atcab_aes_cbc_encrypt_block (
    ctx,
    plaintext,
    ciphertext )
```

Encrypt a block of data using CBC mode and a key within the ATECC608. `atcab_aes_cbc_init()` should be called before the first use of this function.

Args:

<code>ctx</code>	AES CBC context.
<code>plaintext</code>	Plaintext to be encrypted (16 bytes). (Bytearray or bytes)
<code>ciphertext</code>	Encrypted data is returned here (16 bytes). (Bytearray or bytes)

Returns:

Status code

### 20.2.2.4 atcab\_aes\_cbc\_init()

```
def cryptoauthlib.atcab.atcab_aes_cbc_init (
    ctx,
    key_id,
    key_block,
    iv )
```

Initialize context for AES CBC operation.

Args:

<code>ctx</code>	AES CBC context to be initialized
<code>key_id</code>	Key location. Can either be a slot number or <code>ATCA_TEMPKEY_KEYID</code> for TempKey.
<code>key_block</code>	Index of the 16-byte block to use within the key location for the actual key.
<code>iv</code>	Initialization vector (16 bytes). Bytearray format

Returns:

Status Code

### 20.2.2.5 `atcab_aes_cbcmac_finish()`

```
def cryptoauthlib.atcab.atcab_aes_cbcmac_finish (
    ctx,
    mac,
    mac_size )
```

Finish a CBC-MAC operation returning the CBC-MAC value. If the data provided to the `atcab_aes_cbcmac_update()` function has incomplete block this function will return an error code.

Args:

<code>ctx</code>	AES-128 CBC-MAC context.
<code>mac</code>	CBC-MAC is returned here.
<code>mac_size</code>	Size of CBC-MAC requested in bytes (max 16 bytes).

Returns:

`ATCA_SUCCESS` on success, otherwise an error code.

### 20.2.2.6 `atcab_aes_cbcmac_init()`

```
def cryptoauthlib.atcab.atcab_aes_cbcmac_init (
    ctx,
    key_id,
    key_block )
```

Initialize context for AES CBC-MAC operation.

Args:

<code>ctx</code>	AES CBC-MAC context to be initialized
<code>key_id</code>	Key location. Can either be a slot number or <code>ATCA_TEMPKEY_KEYID</code> for TempKey.
<code>key_block</code>	Index of the 16-byte block to use within the key location for the actual key.

Returns:

`ATCA_SUCCESS` on success, otherwise an error code.

### 20.2.2.7 atcab\_aes\_cbcmac\_update()

```
def cryptoauthlib.atcab.atcab_aes_cbcmac_update (
    ctx,
    data,
    data_size )
```

Calculate AES CBC-MAC with key stored within ECC608A device.  
atcab\_aes\_cbcmac\_init() should be called before the first use of  
this function.

Args:

ctx	AES CBC-MAC context structure.
data	Data to be added for AES CBC-MAC calculation. Can be bytearray or bytes.
data_size	Data length in bytes.

Returns:

ATCA\_SUCCESS on success, otherwise an error code.

### 20.2.2.8 atcab\_aes\_ccm\_aad\_finish()

```
def cryptoauthlib.atcab.atcab_aes_ccm_aad_finish (
    ctx )
```

Finish processing Additional Authenticated Data (AAD) using CCM mode.

Args:

ctx	AES CCM context
-----	-----------------

### 20.2.2.9 atcab\_aes\_ccm\_aad\_update()

```
def cryptoauthlib.atcab.atcab_aes_ccm_aad_update (
    ctx,
    aad,
    aad_size )
```

Process Additional Authenticated Data (AAD) using CCM mode and a  
key within the ATECC608A device

Args:

ctx	AES CCM context
aad	Additional authenticated data to be added
aad_size	Size of aad in bytes.



### 20.2.2.10 atcab\_aes\_ccm\_decrypt\_finish()

```
def cryptoauthlib.atcab.atcab_aes_ccm_decrypt_finish (
    ctx,
    tag,
    is_verified )
```

Complete a CCM decrypt operation authenticating provided tag.

Args:

ctx	AES CCM context structure.
tag	Authentication tag is returned here.
is_verified	Value is set to true if the tag is authenticated else the value is set to false.

### 20.2.2.11 atcab\_aes\_ccm\_decrypt\_update()

```
def cryptoauthlib.atcab.atcab_aes_ccm_decrypt_update (
    ctx,
    ciphertext,
    ciphertext_size,
    plaintext )
```

Process data using CCM mode and a key within the ATECC608A device. atcab\_aes\_ccm\_init() or atcab\_aes\_ccm\_init\_rand() should be called before the first use of this function.

Args:

ctx	AES CCM context structure.
ciphertext	Data to be processed.
ciphertext_size	Size of the data to be processed.
plaintext	Output data is returned here.

### 20.2.2.12 atcab\_aes\_ccm\_encrypt\_finish()

```
def cryptoauthlib.atcab.atcab_aes_ccm_encrypt_finish (
    ctx,
    tag,
    tag_size )
```

Complete a CCM encrypt operation returning the authentication tag.

Args:

ctx	AES CCM context structure.
tag	Authentication tag is returned here.
tag_size	Tag size in bytes.

### 20.2.2.13 atcab\_aes\_ccm\_encrypt\_update()

```
def cryptoauthlib.atcab.atcab_aes_ccm_encrypt_update (
    ctx,
    plaintext,
    plaintext_size,
    ciphertext )
```

Process data using CCM mode and a key within the ATECC608A device. `atcab_aes_ccm_init()` or `atcab_aes_ccm_init_rand()` should be called before the first use of this function.

Args:

<code>ctx</code>	AES CCM context structure.
<code>plaintext</code>	Data to be processed.
<code>plaintext_size</code>	Size of the data to be processed.
<code>ciphertext</code>	Output data is returned here.

### 20.2.2.14 atcab\_aes\_ccm\_init()

```
def cryptoauthlib.atcab.atcab_aes_ccm_init (
    ctx,
    key_id,
    key_block,
    iv,
    iv_size,
    aad_size,
    text_size,
    tag_size )
```

Initialize context for AES CCM operation with an existing IV, which is common when starting a decrypt operation.

Args:

<code>ctx</code>	AES CCM context to be initialized
<code>key_id</code>	Key location. Can either be a slot number or <code>ATCA_TEMPKEY_KEYID</code> for TempKey.
<code>key_block</code>	Index of the 16-byte block to use within the key location for the actual key.
<code>iv</code>	Nonce to be fed into the AES CCM calculation.
<code>iv_size</code>	Size of iv.
<code>aad_size</code>	Size of Additional authentication data.
<code>text_size</code>	Size of plaintext/ciphertext to be processed.
<code>tag_size</code>	Preferred size of tag.

### 20.2.2.15 atcab\_aes\_ccm\_init\_rand()

```
def cryptoauthlib.atcab.atcab_aes_ccm_init_rand (
    ctx,
    key_id,
    key_block,
    iv,
    iv_size,
    aad_size,
    text_size,
    tag_size )
```

Initialize context for AES CCM operation with a random nonce

Args:

ctx	AES CCM context to be initialized
key_id	Key location. Can either be a slot number or ATCA_TEMPKEY_KEYID for TempKey.
key_block	Index of the 16-byte block to use within the key location for the actual key.
iv	Nonce to be fed into the AES CCM calculation.
iv_size	Size of iv.
aad_size	Size of Additional authentication data.
text_size	Size of plaintext/ciphertext to be processed.
tag_size	Preferred size of tag.

#### 20.2.2.16 atcab\_aes\_cmac\_finish()

```
def cryptoauthlib.atcab.atcab_aes_cmac_finish (
    ctx,
    cmac,
    size )
```

Finish a CMAC operation returning the CMAC value.

Args:

ctx	AES-128 CMAC context.
cmac	CMAC is returned here.
cmac_size	Size of CMAC requested in bytes (max 16 bytes).

Returns:

Status code
-------------

#### 20.2.2.17 atcab\_aes\_cmac\_init()

```
def cryptoauthlib.atcab.atcab_aes_cmac_init (
    ctx,
    key_id,
    key_block )
```

Initialize a CMAC calculation using an AES-128 key in the ATECC608.

Args:

ctx	AES-128 CMAC context.
key_id	Key location. Can either be a slot number or ATCA_TEMPKEY_KEYID for TempKey.
key_block	Index of the 16-byte block to use within the key location for the actual key.

Returns:

Status code
-------------

### 20.2.2.18 atcab\_aes\_cmac\_update()

```
def cryptoauthlib.atcab.atcab_aes_cmac_update (
    ctx,
    data,
    data_size )
```

Add data to an initialized CMAC calculation.

Args:

ctx	AES-128 CMAC context.
data	Data to be added.
data_size	Size of the data to be added in bytes.

Returns:

Status code

### 20.2.2.19 atcab\_aes\_ctr\_decrypt\_block()

```
def cryptoauthlib.atcab.atcab_aes_ctr_decrypt_block (
    ctx,
    ciphertext,
    plaintext )
```

Decrypt a block of data using CTR mode and a key within the ATECC608 device. `atcab_aes_ctr_init()` or `atcab_aes_ctr_init_rand()` should be called before the first use of this function.

Args:

ctx	AES CTR context structure.
ciphertext	Ciphertext to be decrypted (16 bytes).
plaintext	Decrypted data is returned here (16 bytes).

Returns:

Status code

### 20.2.2.20 atcab\_aes\_ctr\_encrypt\_block()

```
def cryptoauthlib.atcab.atcab_aes_ctr_encrypt_block (
    ctx,
    plaintext,
    ciphertext )
```

Encrypt a block of data using CTR mode and a key within the ATECC608 device. `atcab_aes_ctr_init()` or `atcab_aes_ctr_init_rand()` should be called before the first use of this function.

Args:

ctx	AES CTR context structure.
plaintext	Plaintext to be encrypted (16 bytes).
ciphertext	Encrypted data is returned here (16 bytes).

Returns:

Status code

### 20.2.2.21 atcab\_aes\_ctr\_init()

```
def cryptoauthlib.atcab.atcab_aes_ctr_init (
    ctx,
    key_id,
    key_block,
    counter_size,
    iv )
```

Initialize context for AES CTR operation with an existing IV, which is common when start a decrypt operation.

The IV is a combination of nonce (left-field) and big-endian counter (right-field). The counter\_size field sets the size of the counter and the remaining bytes are assumed to be the nonce.

Args:

ctx	AES CTR context to be initialized.
key_id	Key location. Can either be a slot number or ATCA_TEMPKEY_KEYID for TempKey.
key_block	Index of the 16-byte block to use within the key location for the actual key.
counter_size	Size of counter in IV in bytes. 4 bytes is a common size.
iv	Initialization vector (concatenation of nonce and counter) 16 bytes.

Returns:

ATCA\_SUCCESS on success, otherwise an error code.

### 20.2.2.22 atcab\_aes\_ctr\_init\_rand()

```
def cryptoauthlib.atcab.atcab_aes_ctr_init_rand (
    ctx,
    key_id,
    key_block,
    counter_size,
    iv )
```

Initialize context for AES CTR operation with a random nonce and counter set to 0 as the IV, which is common when starting an encrypt operation.

The IV is a combination of nonce (left-field) and big-endian counter (right-field). The counter\_size field sets the size of the counter and the remaining bytes are assumed to be the nonce.

Args:

ctx	AES CTR context to be initialized.
key_id	Key location. Can either be a slot number or ATCA_TEMPKEY_KEYID for TempKey.
key_block	Index of the 16-byte block to use within the key location for the actual key.
counter_size	Size of counter in IV in bytes. 4 bytes is a common size.
iv	Initialization vector (concatenation of nonce and counter) is returned here (16 bytes).

Returns:

ATCA\_SUCCESS on success, otherwise an error code.

### 20.2.2.23 atcab\_aes\_decrypt()

```
def cryptoauthlib.atcab.atcab_aes_decrypt (
    key_id,
    key_block,
    ciphertext,
    plaintext )
```

Perform an AES-128 decrypt operation with a key in the device.

Args:

key_id	Key location. Can either be a slot number or ATCA_TEMPKEY_KEYID for TempKey. (int)
key_block	Index of the 16-byte block to use within the key location for the actual key. (int)
ciphertext	Input ciphertext to be decrypted (16 bytes). (bytearray or bytes)
plaintext	Output plaintext is returned here (16 bytes). (Expects bytearray of size 16)s

Returns:

Status Code

### 20.2.2.24 atcab\_aes\_encrypt()

```
def cryptoauthlib.atcab.atcab_aes_encrypt (
    key_id,
    key_block,
    plaintext,
    ciphertext )
```

Perform an AES-128 encrypt operation with a key in the device.

Args:

key_id	Key location. Can either be a slot number or ATCA_TEMPKEY_KEYID for TempKey. (int)
key_block	Index of the 16-byte block to use within the key location for the actual key. (int)
plaintext	Input plaintext to be encrypted (16 bytes). (Can be of type bytearray or bytes)
ciphertext	Output ciphertext is returned here (16 bytes). (Expects bytearray of size 16)

Returns:

Status Code

### 20.2.2.25 atcab\_aes\_gcm\_aad\_update()

```
def cryptoauthlib.atcab.atcab_aes_gcm_aad_update (
    ctx,
    aad,
    aad_size )
```

Process Additional Authenticated Data (AAD) using GCM mode and a key within the ATECC608 device.

This can be called multiple times. `atcab_aes_gcm_init()` or `atcab_aes_gcm_init_rand()` should be called before the first use of this function. When there is AAD to include, this should be called before `atcab_aes_gcm_encrypt_update()` or `atcab_aes_gcm_decrypt_update()`.

Args:

<code>ctx</code>	AES GCM context
<code>aad</code>	Additional authenticated data to be added
<code>aad_size</code>	Size of aad in bytes

Returns:

ATCA\_SUCCESS on success, otherwise an error code.

#### 20.2.2.26 `atcab_aes_gcm_decrypt_finish()`

```
def cryptoauthlib.atcab.atcab_aes_gcm_decrypt_finish (
    ctx,
    tag,
    tag_size,
    is_verified )
```

Complete a GCM decrypt operation verifying the authentication tag.

Args:

<code>ctx</code>	AES GCM context structure.
<code>tag</code>	Expected authentication tag.
<code>tag_size</code>	Size of tag in bytes (12 to 16 bytes).
<code>is_verified</code>	Returns whether or not the tag verified.

Returns:

ATCA\_SUCCESS on success, otherwise an error code.

#### 20.2.2.27 `atcab_aes_gcm_decrypt_update()`

```
def cryptoauthlib.atcab.atcab_aes_gcm_decrypt_update (
    ctx,
    ciphertext,
    ciphertext_size,
    plaintext )
```

Decrypt data using GCM mode and a key within the ATECC608 device. `atcab_aes_gcm_init()` or `atcab_aes_gcm_init_rand()` should be called before the first use of this function.

Args:

<code>ctx</code>	AES GCM context structure.
<code>ciphertext</code>	Ciphertext to be decrypted.
<code>ciphertext_size</code>	Size of ciphertext in bytes.
<code>plaintext</code>	Decrypted data is returned here.

Returns:

ATCA\_SUCCESS on success, otherwise an error code.

### 20.2.2.28 atcab\_aes\_gcm\_encrypt\_finish()

```
def cryptoauthlib.atcab.atcab_aes_gcm_encrypt_finish (
    ctx,
    tag,
    tag_size )
```

Complete a GCM encrypt operation returning the authentication tag.

Args:

ctx	AES GCM context structure.
tag	Authentication tag is returned here.
tag_size	Tag size in bytes (12 to 16 bytes).

Returns:

ATCA\_SUCCESS on success, otherwise an error code.

### 20.2.2.29 atcab\_aes\_gcm\_encrypt\_update()

```
def cryptoauthlib.atcab.atcab_aes_gcm_encrypt_update (
    ctx,
    plaintext,
    plaintext_size,
    ciphertext )
```

Encrypt data using GCM mode and a key within the ATECC608 device. atcab\_aes\_gcm\_init() or atcab\_aes\_gcm\_init\_rand() should be called before the first use of this function.

Args:

ctx	AES GCM context structure.
plaintext	Plaintext to be encrypted (16 bytes).
plaintext_size	Size of plaintext in bytes.
ciphertext	Encrypted data is returned here.

Returns:

ATCA\_SUCCESS on success, otherwise an error code.

### 20.2.2.30 atcab\_aes\_gcm\_init()

```
def cryptoauthlib.atcab.atcab_aes_gcm_init (
    ctx,
    key_id,
    key_block,
    iv,
    iv_size )
```

Initialize context for AES GCM operation with an existing IV, which is common when starting a decrypt operation.

Args:

ctx	AES GCM context to be initialized.
key_id	Key location. Can either be a slot number or ATCA_TEMPKEY_KEYID for TempKey.
key_block	Index of the 16-byte block to use within the key location for the actual key.
iv	Initialization vector.
iv_size	Size of IV in bytes. Standard is 12 bytes.

Returns:

ATCA\_SUCCESS on success, otherwise an error code.



**20.2.2.31 atcab\_aes\_gcm\_init\_rand()**

```
def cryptoauthlib.atcab.atcab_aes_gcm_init_rand (
    ctx,
    key_id,
    key_block,
    rand_size,
    free_field,
    free_field_size,
    iv )
```

Initialize context for AES GCM operation with a IV composed of a random and optional fixed(free) field, which is common when starting an encrypt operation.

**Args:**

ctx	AES CTR context to be initialized.
key_id	Key location. Can either be a slot number or ATCA_TEMPKEY_KEYID for TempKey.
key_block	Index of the 16-byte block to use within the key location for the actual key.
rand_size	Size of the random field in bytes. Minimum and recommended size is 12 bytes. Max is 32 bytes.
free_field	Fixed data to include in the IV after the random field. Can be NULL if not used.
free_field_size	Size of the free field in bytes.
iv	Initialization vector is returned here. Its size will be rand_size and free_field_size combined.

**Returns:**

ATCA\_SUCCESS on success, otherwise an error code.

**20.2.2.32 atcab\_aes\_gfm()**

```
def cryptoauthlib.atcab.atcab_aes_gfm (
    hash_key,
    inp,
    output )
```

Perform a Galois Field Multiply (GFM) operation.

**Args:**

hash_key	First input value (16 bytes). (bytearray or bytes)
inp	Second input value (16 bytes). (bytearray or bytes)
output	GFM result is returned here (16 bytes). (Expects bytearray of size 16)

**Returns:**

Status Code

### 20.2.2.33 atcab\_challenge()

```
def cryptoauthlib.atcab.atcab_challenge (
    num_in )
```

Execute a Nonce command in pass-through mode to initialize TempKey to a specified value.

Args:

num_in	Data to be loaded into TempKey (32 bytes). (bytearray or bytes)
--------	--

Returns:

Status Code
-------------

### 20.2.2.34 atcab\_challenge\_seed\_update()

```
def cryptoauthlib.atcab.atcab_challenge_seed_update (
    num_in,
    rand_out )
```

Execute a Nonce command to generate a random challenge combining a host nonce (num\_in) and a device random number.

Args:

num_in	Host nonce to be combined with the device random number (20 bytes). (bytearray or bytes)
rand_out	Internally generated 32-byte random number that was used in the nonce/challenge calculation is returned here. Can be NULL if not needed. (Expects bytearray)

Returns:

Status code
-------------

### 20.2.2.35 atcab\_checkmac()

```
def cryptoauthlib.atcab.atcab_checkmac (
    mode,
    key_id,
    challenge,
    response,
    other_data )
```

Compares a MAC response with input values

Args:

mode	Controls which fields within the device are used in the message (int)
key_id	Key location in the CryptoAuth device to use for the MAC (int)
challenge	Challenge data (32 bytes) (bytearray or bytes)
response	MAC response data (32 bytes) (bytearray or bytes)
other_data	OtherData parameter (13 bytes) (bytearray or bytes)

Returns:

Status code
-------------

**20.2.2.36 atcab\_cmp\_config\_zone()**

```
def cryptoauthlib.atcab.atcab_cmp_config_zone (
    config_data,
    same_config )
```

Compares a specified configuration zone with the configuration zone currently on the device.

This only compares the static portions of the configuration zone and skips those that are unique per device (first 16 bytes) and areas that can change after the configuration zone has been locked (e.g. LastKeyUse).

Args:

config_data	Full configuration data to compare the device against. (bytearray or bytes)
same_config	Result is returned here. True if the static portions on the configuration zones are the same. (Expects AtcaReference)

Returns:

Status code

**20.2.2.37 atcab\_counter()**

```
def cryptoauthlib.atcab.atcab_counter (
    mode,
    counter_id,
    counter_value )
```

Compute the Counter functions

Args:

mode	The mode used for the counter (int)
counter_id	The counter to be used (int)
counter_value	Counter value returned from device (AtcaReference expected)

Returns:

Status code

**20.2.2.38 atcab\_counter\_increment()**

```
def cryptoauthlib.atcab.atcab_counter_increment (
    counter_id,
    counter_value )
```

Increments one of the device's monotonic counters

Args:

counter_id	Counter to be incremented (int)
counter_value	New value of the counter is returned here (AtcaReference expected)

Returns:

Status code

### 20.2.2.39 atcab\_counter\_read()

```
def cryptoauthlib.atcab.atcab_counter_read (
    counter_id,
    counter_value )
```

Reads one of the device's monotonic counters

Args:

counter_id	Counter to be read (int)
counter_value	Counter value is returned here (AtcaReference expected)

Returns:

Status code

### 20.2.2.40 atcab\_derivekey()

```
def cryptoauthlib.atcab.atcab_derivekey (
    mode,
    target_key,
    mac )
```

Executes the DeviveKey command for deriving a new key from a nonce (TempKey) and an existing key.

Args:

mode	Bit 2 must match the value in TempKey.SourceFlag (int)
target_key	Key slot to be written (int)
mac	Optional 32 byte MAC used to validate operation. (bytearray or bytes)

Returns:

Status code

### 20.2.2.41 atcab\_ecdh()

```
def cryptoauthlib.atcab.atcab_ecdh (
    key_id,
    public_key,
    pms )
```

ECDH command with a private key in a slot and the premaster secret is returned in the clear.

Args:

key_id	Slot of key for ECDH computation (int)
public_key	Public key input to ECDH calculation. X and Y integers in big-endian format. 64 bytes for P256 key. (bytearray or bytes)
pms	ByteArray - Computed ECDH premaster secret is returned here (32 bytes). (Expects bytearray of size 32)

Returns:

Status code

**20.2.2.42 atcab\_ecdh\_base()**

```
def cryptoauthlib.atcab.atcab_ecdh_base (
    mode,
    key_id,
    public_key,
    pms,
    out_nonce )
```

Base function for generating premaster secret key using ECDH.

**Args:**

mode	Mode to be used for ECDH computation (int)
key_id	Slot of key for ECDH computation (int)
public_key	Public key input to ECDH calculation. X and Y integers in big-endian format. 64 bytes for P256 key. (bytearray or bytes)
pms	ByteArray - Computed ECDH pre-master secret is returned here (32 bytes) if returned directly. Otherwise NULL.
out_nonce	ByteArray - Nonce used to encrypt pre-master secret. NULL if output encryption not used.

**Returns:**

Status code

**20.2.2.43 atcab\_ecdh\_enc()**

```
def cryptoauthlib.atcab.atcab_ecdh_enc (
    key_id,
    public_key,
    pms,
    read_key,
    read_key_id,
    num_in = None )
```

ECDH command with a private key in a slot and the premaster secret is read from the next slot. This function only works for even numbered slots with the proper configuration.

**Args:**

key_id	Slot of key for ECDH computation (int)
public_key	Public key input to ECDH calculation. X and Y integers in big-endian format. 64 bytes for P256 key. (bytearray or bytes)
read_key	Read key for the premaster secret slot (key_id 1) (32 bytes). (bytearray or bytes)
read_key_id	Read key slot for read_key. (int)
pms	ByteArray - Computed ECDH premaster secret is returned here (32 bytes). (Expects bytearray of size 32)
num_in	Bytearray - Host nonce used to calculate nonce (20 bytes)

**Returns:**

Status code

### 20.2.2.44 atcab\_ecdh\_ioenc()

```
def cryptoauthlib.atcab.atcab_ecdh_ioenc (
    key_id,
    public_key,
    pms,
    io_key )
```

ECDH command with a private key in a slot and the premaster secret is returned encrypted using the IO protection key.

Args:

key_id	Slot of key for ECDH computation (int)
public_key	Public key input to ECDH calculation. X and Y integers in big-endian format. 64 bytes for P256 key. (bytearray or bytes)
io_key	IO protection key (32 bytes). (bytearray or bytes)
pms	Computed ECDH premaster secret is returned here (32 bytes). (Expects bytearray of size 32)

Returns:

Status code
-------------

### 20.2.2.45 atcab\_ecdh\_tempkey()

```
def cryptoauthlib.atcab.atcab_ecdh_tempkey (
    public_key,
    pms )
```

ECDH command with a private key in TempKey and the premaster secret is returned in the clear.

Args:

public_key	Public key input to ECDH calculation. X and Y integers in big-endian format. 64 bytes for P256 key. (bytearray or bytes)
pms	Computed ECDH premaster secret is returned here (32 bytes). (Expects bytearray of size 32)

Retuns:

Status code
-------------

### 20.2.2.46 atcab\_ecdh\_tempkey\_ioenc()

```
def cryptoauthlib.atcab.atcab_ecdh_tempkey_ioenc (
    public_key,
    pms,
    io_key )
```

ECDH command with a private key in TempKey and the premaster secret is returned encrypted using the IO protection key.

Args:

<code>public_key</code>	Public key input to ECDH calculation. X and Y integers in big-endian format. 64 bytes for P256 key. (bytearray or bytes)
<code>io_key</code>	IO protection key (32 bytes). (bytearray or bytes)
<code>pms</code>	Computed ECDH premaster secret is returned here (32 bytes). (Expects bytearray of size 32)

Returns:

Status code

#### 20.2.2.47 atcab\_gendig()

```
def cryptoauthlib.atcab.atcab_gendig (
    zone,
    key_id,
    other_data,
    other_data_size )
```

Issues a GenDig command, which performs a SHA256 hash on the source data indicated by zone with the contents of TempKey. See the CryptoAuth datasheet for your chip to see what the values of zone correspond to.

Args:

<code>zone</code>	Designates the source of the data to hash with TempKey. (int)
<code>key_id</code>	Indicates the key, OTP block, or message order for shared nonce mode. (int)
<code>other_data</code>	Four bytes of data for SHA calculation when using a NoMac key, 32 bytes for "Shared Nonce" mode, otherwise ignored (can be NULL). (bytearray or bytes)
<code>other_data_size</code>	Size of other_data in bytes. (int)

Returns:

Status code

#### 20.2.2.48 atcab\_genkey()

```
def cryptoauthlib.atcab.atcab_genkey (
    key_id,
    public_key )
```

Issues GenKey command, which generates a new random private key in slot and returns the public key.

Args:

<code>key_id</code>	Slot number where an ECC private key is configured. Can also be ATCA_TEMPKEY_KEYID to generate a private key in TempKey. (int)
<code>public_key</code>	Public key will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve. Set to NULL if public key isn't required. (Expects bytearray)

Returns:

Status code

### 20.2.2.49 atcab\_genkey\_base()

```
def cryptoauthlib.atcab.atcab_genkey_base (
    mode,
    key_id,
    other_data,
    public_key = None )
```

Issues GenKey command, which can generate a private key, compute a public key, nd/or compute a digest of a public key.

Args:

mode	Mode determines what operations the GenKey command performs. (int)
key_id	Slot to perform the GenKey command on. (int)
other_data	OtherData for PubKey digest calculation. Can be set to NULL otherwise. (bytearray or bytes)
public_key	If the mode indicates a public key will be calculated, it will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve. Set to NULL if public key isn't required. (Expects bytearray of size 64 bytes)

Returns:

Status code

### 20.2.2.50 atcab\_get\_device()

```
def cryptoauthlib.atcab.atcab_get_device (
    void )
```

Return the global device instance

### 20.2.2.51 atcab\_get\_device\_type()

```
def cryptoauthlib.atcab.atcab_get_device_type (
    void )
```

Return the device type of the currently initialized device.



**20.2.2.52 atcab\_get\_pubkey()**

```
def cryptoauthlib.atcab.atcab_get_pubkey (
    key_id,
    public_key )
```

Uses GenKey command to calculate the public key from an existing private key in a slot.

Args:

key_id	Slot number of the private key. (int)
public_key	Public key will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve. Set to NULL if public key isn't required. (Expects bytearray)

Returns:

Status code
-------------

**20.2.2.53 atcab\_hmac()**

```
def cryptoauthlib.atcab.atcab_hmac (
    mode,
    key_id,
    digest )
```

Issues a HMAC command, which computes an HMAC/SHA-256 digest of a key stored in the device, a challenge, and other information on the device.

Args:

mode	Controls which fields within the device are used in the message. (int)
key_id	Which key is to be used to generate the response. Bits 0:3 only are used to select a slot but all 16 bits are used in the HMAC message. (int)
digest	HMAC digest is returned in this buffer (32 bytes). (Expects bytearray)

Returns:

Status code
-------------

**20.2.2.54 atcab\_hw\_sha2\_256()**

```
def cryptoauthlib.atcab.atcab_hw_sha2_256 (
    data,
    data_size,
    digest )
```

Use the SHA command to compute a SHA-256 digest.

Args:

data	Message data to be hashed. (bytearray or bytes)
data_size	Size of data in bytes. (int)
digest	Digest is returned here (32 bytes). (Expects bytearray)

Returns:

Status code
-------------

### 20.2.2.55 atcab\_hw\_sha2\_256\_finish()

```
def cryptoauthlib.atcab.atcab_hw_sha2_256_finish (
    ctx,
    digest )
```

Finish SHA-256 digest for a SHA context for performing a hardware SHA-256 operation on a device.

Args:

ctx	SHA256 context (atca_sha256_ctx)
digest	SHA256 digest is returned here (32 bytes) (Expects bytearray)

Returns:

Status code
-------------

### 20.2.2.56 atcab\_hw\_sha2\_256\_init()

```
def cryptoauthlib.atcab.atcab_hw_sha2_256_init (
    ctx )
```

Initialize a SHA context for performing a hardware SHA-256 operation on a device. Note that only one SHA operation can be run at a time.

Args:

ctx	SHA256 context (atca_sha256_ctx)
-----	----------------------------------

Returns:

Status code
-------------

### 20.2.2.57 atcab\_hw\_sha2\_256\_update()

```
def cryptoauthlib.atcab.atcab_hw_sha2_256_update (
    ctx,
    data,
    data_size )
```

--> Add message data to a SHA context for performing a hardware SHA-256 operation on a device.

Args:

ctx	SHA256 context (atca_sha256_ctx)
data	Message data to be added to hash. (bytearray or bytes)
data_size	Size of data in bytes. (int)

Returns:

Status code
-------------

### 20.2.2.58 atcab\_info()

```
def cryptauthlib.atcab.atcab_info (
    revision )
```

Used to get the device revision number. (DevRev)

Args:

revision	4-byte bytearray receiving the revision number from the device. (Expects bytearray)
----------	---

Returns:

Status code
-------------

### 20.2.2.59 atcab\_info\_base()

```
def cryptauthlib.atcab.atcab_info_base (
    mode,
    param2,
    out_data )
```

Issues an Info command, which return internal device information and can control GPIO and the persistent latch.

Args:

mode	Selects which mode to be used for info command.(int)
param2	Selects the particular fields for the mode.(int)
out_data	Response from info command (4 bytes). Can be set to NULL if not required.(Expects bytearray)

Returns:

Status
--------

### 20.2.2.60 atcab\_info\_get\_latch()

```
def cryptauthlib.atcab.atcab_info_get_latch (
    state )
```

Using the Info command to get the persistent latch current state for an ATECC608 device.

Args:

state	The state is returned here. Set (True) or clear (False). Expects AtcaReference.
-------	---

Returns:

Status code
-------------

### 20.2.2.61 atcab\_info\_set\_latch()

```
def cryptoauthlib.atcab.atcab_info_set_latch (
    state )
```

Use the Info command to set the persistent latch state for an ATECC608 device.

Args:

state	Persistent latch state. Set (True) or clear (False).
-------	--

Returns:

Status code
-------------

### 20.2.2.62 atcab\_init()

```
def cryptoauthlib.atcab.atcab_init (
    iface_cfg )
```

Initialize the communication stack and initializes the ATCK590 kit  
Communication over USB HID and Kit Protocol by default  
raise CryptoException

### 20.2.2.63 atcab\_is\_locked()

```
def cryptoauthlib.atcab.atcab_is_locked (
    zone,
    is_locked )
```

Executes Read command, which reads the configuration zone to see if the specified slot is locked.

Args:

zone	The zone to query for locked (use LOCK_ZONE_CONFIG(0x00) or LOCK_ZONE_DATA(0x01) ). (int)
is_locked	Lock state returned here. True if locked. (Expects AtcaReference)

Returns:

Status code
-------------

**20.2.2.64 atcab\_is\_slot\_locked()**

```
def cryptoauthlib.atcab.atcab_is_slot_locked (
    slot,
    is_locked )
```

Executes Read command, which reads the configuration zone to see if the specified slot is locked.

Args:

slot	Slot to query for locked (slot 0-15) (int)
is_locked	Lock state returned here. True if locked. (Expects AtcaReference)

Returns:

Status code

**20.2.2.65 atcab\_kdf()**

```
def cryptoauthlib.atcab.atcab_kdf (
    mode,
    key_id,
    details,
    message,
    out_data,
    out_nonce )
```

Executes the KDF command, which derives a new key in PRF, AES, or HKDF modes. Generally this function combines a source key with an input string and creates a result key/digest/array.

Args:

mode	Mode determines KDF algorithm (PRF,AES,HKDF), source key location, and target key locations. (int)
key_id	Source and target key slots if locations are in the EEPROM. Source key slot is the LSB and target key slot is the MSB. (int)
details	Further information about the computation, depending on the algorithm. (int)
message	Input value from system (up to 128 bytes). Actual size of message is 16 bytes for AES algorithm or is encoded in the MSB of the details parameter for other algorithms. (bytearray or bytes)
out_data	Output of the KDF function is returned here. If the result remains in the device, this can be NULL. (Expects bytearray)
out_nonce	If the output is encrypted, a 32 byte random nonce generated by the device is returned here. If output encryption is not used, this can be NULL. (Expects bytearray)

Returns:

Status code

### 20.2.2.66 atcab\_lock()

```
def cryptoauthlib.atcab.atcab_lock (
    mode,
    summary_crc )
```

The Lock command prevents future modifications of the Configuration and/or Data and OTP zones. If the device is so configured, then this command can be used to lock individual data slots. This command fails if the designated area is already locked.

Args:

mode	Zone, and/or slot, and summary check (bit 7). (int)
summary_crc	CRC of the config or data zones. Ignored for slot locks or when mode bit 7 is set. (int)

Returns:

Status code
-------------

### 20.2.2.67 atcab\_lock\_config\_zone()

```
def cryptoauthlib.atcab.atcab_lock_config_zone (
    void )
```

Unconditionally (no CRC required) lock the config zone.

Args:

None
------

Returns:

Status code
-------------

### 20.2.2.68 atcab\_lock\_config\_zone\_crc()

```
def cryptoauthlib.atcab.atcab_lock_config_zone_crc (
    summary_crc )
```

Lock the config zone with summary CRC.

The CRC is calculated over the entire config zone contents. 88 bytes for ATSHA devices, 128 bytes for ATECC devices. Lock will fail if the provided CRC doesn't match the internally calculated one.

Args:

summary_crc	Expected CRC over the config zone. (int)
-------------	--

Returns:

Status code
-------------

### 20.2.2.69 atcab\_lock\_data\_slot()

```
def cryptoauthlib.atcab.atcab_lock_data_slot (
    slot )
```

Lock an individual slot in the data zone on an ATECC device. Not available for ATSHA devices. Slot must be configured to be slot lockable (KeyConfig.Lockable=1).

Args:

slot	Slot to be locked in data zone. (int)
------	---------------------------------------

Returns:

Status code
-------------

### 20.2.2.70 atcab\_lock\_data\_zone()

```
def cryptoauthlib.atcab.atcab_lock_data_zone (
    void )
```

Unconditionally (no CRC required) lock the data zone (slots and OTP).

ConfigZone must be locked and DataZone must be unlocked for the zone to be successfully locked.

Args:

None
------

Returns:

Status code
-------------

### 20.2.2.71 atcab\_lock\_data\_zone\_crc()

```
def cryptoauthlib.atcab.atcab_lock_data_zone_crc (
    summary_crc )
```

Lock the data zone (slots and OTP) with summary CRC.

The CRC is calculated over the concatenated contents of all the slots and OTP at the end. Private keys (KeyConfig.Private=1) are skipped. Lock will fail if the provided CRC doesn't match the internally calculated one.

Args:

summary_crc	Expected CRC over the config zone. (int)
-------------	--

Returns:

Status code
-------------

### 20.2.2.72 atcab\_mac()

```
def cryptoauthlib.atcab.atcab_mac (
    mode,
    key_id,
    challenge,
    digest )
```

Executes MAC command, which computes a SHA-256 digest of a key stored in the device, a challenge, and other information on the device.

Args:

mode	Controls which fields within the device are used in the message (int)
key_id	Key in the CryptoAuth device to use for the MAC (int)
challenge	Challenge message (32 bytes). May be NULL if mode indicates a challenge isn't required. (bytearray or bytes)
digest	MAC response is returned here (32 bytes). (Expects bytearray)

Returns:

Status code

### 20.2.2.73 atcab\_nonce()

```
def cryptoauthlib.atcab.atcab_nonce (
    num_in )
```

Execute a Nonce command in pass-through mode to initialize TempKey to a specified value.

Args:

num_in	Data to be loaded into TempKey (32 bytes). (bytearray or bytes)
--------	---

Returns:

None

### 20.2.2.74 atcab\_nonce\_base()

```
def cryptoauthlib.atcab.atcab_nonce_base (
    mode,
    zero,
    num_in,
    rand_out )
```



Executes Nonce command, which loads a random or fixed nonce/data into the device for use by subsequent commands.

Args:

mode	Controls the mechanism of the internal RNG or fixed write. (int)
zero	Param2, normally 0, but can be used to indicate a nonce calculation mode (bit 15). (int)
num_in	Input value to either be included in the nonce calculation in random modes (20 bytes) or to be written directly (32 bytes or 64 bytes(ATECC608)) in pass-through mode. (bytearray or bytes)
rand_out	If using a random mode, the internally generated 32-byte random number that was used in the nonce calculation is returned here. Can be NULL if not needed. (Expects bytearray)

Returns:

Status code

### 20.2.2.75 atcab\_nonce\_load()

```
def cryptoauthlib.atcab.atcab_nonce_load (
    target,
    num_in,
    num_in_size )
```

Execute a Nonce command in pass-through mode to load one of the device's internal buffers with a fixed value.

For the ATECC608, available targets are TempKey (32 or 64 bytes), Message Digest Buffer (32 or 64 bytes), or the Alternate Key Buffer (32 bytes). For all other devices, only TempKey (32 bytes) is available.

Args:

target	Target device buffer to load. Can be NONCE_MODE_TARGET_TEMPKEY, NONCE_MODE_TARGET_MSGDIGBUF, or NONCE_MODE_TARGET_ALTKEYBUF. (int)
num_in	Data to load into the buffer. (bytearray or bytes)
num_in_size	Size of num_in in bytes. Can be 32 or 64 bytes depending on device and target. (int)

Returns:

Status code

### 20.2.2.76 atcab\_nonce\_rand()

```
def cryptoauthlib.atcab.atcab_nonce_rand (
    num_in,
    rand_out )
```

## 20.2 cryptoauthlib.atcab Namespace Reference

---

Execute a Nonce command to generate a random nonce combining a host nonce (num\_in) and a device random number.

Args:

num_in	Host nonce to be combined with the device random number (20 bytes). (bytearray or bytes)
rand_out	Internally generated 32-byte random number that was used in the nonce/challenge calculation is returned here. Can be NULL if not needed. (Expects bytearray)

Returns:

Status code

### 20.2.2.77 atcab\_priv\_write()

```
def cryptoauthlib.atcab.atcab_priv_write (
    key_id,
    priv_key,
    write_key_id,
    write_key,
    num_in = None )
```

Executes PrivWrite command, to write externally generated ECC private keys into the device.

Args:

key_id	Slot to write the external private key into. (int)
priv_key	External private key (36 bytes) to be written. The first 4 bytes should be zero for P256 curve. (bytearray or bytes)
write_key_id	Write key slot. Ignored if write_key is NULL. (int)
write_key	Write key (32 bytes). If NULL, perform an unencrypted PrivWrite, which is only available when the data zone is unlocked. (bytearray or bytes)
num_in	Bytearray - Host nonce used to calculate nonce (20 bytes)

Returns:

Status code

### 20.2.2.78 atcab\_random()

```
def cryptoauthlib.atcab.atcab_random (
    random_number )
```

Generates a 32 byte random number. Note that if the configuration zone isn't locked yet (LockConfig) then it will return a 0xFFFF0000 repeating pattern instead.

Args:

random_number	Random number is returned here (expects bytearray)
---------------	--

Returns:

Status code

**20.2.2.79 atcab\_read\_bytes\_zone()**

```
def cryptoauthlib.atcab.atcab_read_bytes_zone (
    zone,
    slot,
    offset,
    data,
    length )
```

Used to read an arbitrary number of bytes from any zone configured for clear reads.

This function will issue the Read command as many times as is required to read the requested data.

**Args:**

zone	Zone to read data from. Option are ATCA_ZONE_CONFIG(0), ATCA_ZONE_OTP(1), or ATCA_ZONE_DATA(2). (int)
slot	Slot number to read from if zone is ATCA_ZONE_DATA(2). Ignored for all other zones. (int)
offset	Byte offset within the zone to read from. (int)
length	Number of bytes to read starting from the offset. (int)
data	Read data is returned here. (Expects bytearray)

**Returns:**

Status code

**20.2.2.80 atcab\_read\_config\_zone()**

```
def cryptoauthlib.atcab.atcab_read_config_zone (
    config_data )
```

Executes Read command to read the complete device configuration zone.

**Args:**

config_data	Configuration zone data is returned here. 88 bytes for ATSHA devices, 128 bytes for ATECC devices. (Expects bytearray)
-------------	--

**Returns:**

Status code

**20.2.2.81 atcab\_read\_enc()**

```
def cryptoauthlib.atcab.atcab_read_enc (
    key_id,
    block,
    data,
    enc_key,
    enc_key_id,
    num_in = None )
```

## 20.2 cryptoauthlib.atcab Namespace Reference

---

Executes Read command on a slot configured for encrypted reads and decrypts the data to return it as plaintext.

Data zone must be locked for this command to succeed. Can only read 32 byte blocks.

Args:

key_id	The slot ID to read from. (int)
block	Index of the 32 byte block within the slot to read. (int)
enc_key	32 byte ReadKey for the slot being read. (bytearray or bytes)
enc_key_id	KeyID of the ReadKey being used. (int)
data	Decrypted (plaintext) data from the read is returned here (32 bytes). (Expects bytearray)
num_in	Bytearray - Host nonce used to calculate nonce (20 byte)

Returns:

Status code
-------------

### 20.2.2.82 atcab\_read\_pubkey()

```
def cryptoauthlib.atcab.atcab_read_pubkey (
    slot,
    public_key )
```

Executes Read command to read an ECC P256 public key from a slot configured for clear reads.

This function assumes the public key is stored using the ECC public key format specified in the datasheet.

Args:

slot	Slot number to read from. Only slots 8 to 15 are large enough for a public key. (int)
public_key	Public key is returned here (64 bytes). Format will be the 32 byte X and Y big-endian integers concatenated. (Expects bytearray)

Returns:

Status code
-------------

### 20.2.2.83 atcab\_read\_serial\_number()

```
def cryptoauthlib.atcab.atcab_read_serial_number (
    serial_number )
```

Executes Read command, which reads the 9 byte serial number of the device from the config zone.

Args:

serial_number	9 byte serial number is returned here. (Expects bytearray)
---------------	--

Returns:

Status code
-------------

**20.2.2.84 atcab\_read\_sig()**

```
def cryptoauthlib.atcab.atcab_read_sig (
    slot,
    sig )
```

Executes Read command to read a 64 byte ECDSA P256 signature from a slot configured for clear reads.

Args:

slot	Slot number to read from. Only slots 8 to 15 are large enough for a signature. (int)
sig	Signature will be returned here (64 bytes). Format will be the 32 byte R and S big-endian integers concatenated. (Expects bytearray)

Returns:

Status code
-------------

**20.2.2.85 atcab\_read\_zone()**

```
def cryptoauthlib.atcab.atcab_read_zone (
    zone,
    slot,
    block,
    offset,
    data,
    length )
```

Executes Read command, which reads either 4 or 32 bytes of data from a given slot, configuration zone, or the OTP zone.

When reading a slot or OTP, data zone must be locked and the slot configuration must not be secret for a slot to be successfully read.

Args:

zone	Zone to be read from device. Options are ATCA_ZONE_CONFIG, ATCA_ZONE_OTP, or ATCA_ZONE_DATA. (int)
slot	Slot number for data zone and ignored for other zones. (int)
block	32 byte block index within the zone. (int)
offset	4 byte work index within the block. Ignored for 32 byte reads. (Expects bytearray)
length	Length of the data to be read. Must be either 4 or 32.
data	Read data is returned here. (Expects bytearray)

Returns:

Status code
-------------

**20.2.2.86 atcab\_release()**

```
def cryptoauthlib.atcab.atcab_release (
    void )
```

Release the kit and the communication stack  
raise CryptoException

### 20.2.2.87 atcab\_secureboot()

```
def cryptoauthlib.atcab.atcab_secureboot (
    mode,
    param2,
    digest,
    signature,
    mac )
```

Executes Secure Boot command, which provides support for secure boot of an external MCU or MPU.

Args:

mode	Mode determines what operations the SecureBoot command performs. (int)
param2	Not used, must be 0. (int)
digest	Digest of the code to be verified (32 bytes). (bytearray or bytes)
signature	Signature of the code to be verified (64 bytes). Can be NULL when using the FullStore mode. (bytearray or bytes)
mac	Validating MAC will be returned here (32 bytes). Can be NULL if not required. (Expects bytearray)

Return:

Status code

### 20.2.2.88 atcab\_secureboot\_mac()

```
def cryptoauthlib.atcab.atcab_secureboot_mac (
    mode,
    digest,
    signature,
    num_in,
    io_keys,
    is_verified )
```

Executes Secure Boot command with encrypted digest and validated MAC response using the IO protection key.

Args:

mode	Mode determines what operations the SecureBoot command performs. (int)
digest	Digest of the code to be verified (32 bytes). This is the plaintext digest (not encrypted). (bytearray or bytes)
signature	Signature of the code to be verified (64 bytes). Can be NULL when using the FullStore mode. (bytearray or bytes)
num_in	Host nonce (20 bytes). (bytearray or bytes)
io_key	IO protection key (32 bytes). (bytearray or bytes)
is_verified	Verify result is returned here. (Expects AtcaReference)

Returns:

Status code

**20.2.2.89 atcab\_selftest()**

```
def cryptoauthlib.atcab.atcab_selftest (
    mode,
    param2,
    result )
```

Executes the SelfTest command, which performs a test of one or more of the cryptographic engines within the ATECC608 chip.

Args:

mode	Functions to test. Can be a bit field combining any of the following: SELFTEST_MODE_RNG, SELFTEST_MODE_ECDSA_VERIFY, SELFTEST_MODE_ECDSA_SIGN, SELFTEST_MODE_ECDH, SELFTEST_MODE_AES, SELFTEST_MODE_SHA, SELFTEST_MODE_ALL. (int)
param2	Currently unused, should be 0. (int)
result	Results are returned here as a bit field. (Expects AtcaReference)

Returns:

Status code
-------------

**20.2.2.90 atcab\_sha()**

```
def cryptoauthlib.atcab.atcab_sha (
    length,
    message,
    digest )
```

Use the SHA command to compute a SHA-256 digest.

Args:

length	Size of message parameter in bytes. (int)
message	Message data to be hashed. (bytearray or bytes)
digest	Digest is returned here (32 bytes). (Expects bytearray)

Returns:

Status code
-------------

**20.2.2.91 atcab\_sha\_base()**

```
def cryptoauthlib.atcab.atcab_sha_base (
    mode,
    length,
    message,
    data_out,
    data_out_size )
```

## 20.2 cryptoauthlib.atcab Namespace Reference

---

Executes SHA command, which computes a SHA-256 or HMAC/SHA-256 digest for general purpose use by the host system.

Only the Start(0) and Compute(1) modes are available for ATSHA devices.

### Args:

mode	SHA command mode Start(0), Update/Compute(1), End(2), Public(3), HMACstart(4), HMACend(5), Read_Context(6), or Write_Context(7). Also message digest target location for the ATECC608. (int)
length	Number of bytes in the message parameter or KeySlot for the HMAC key if Mode is HMACstart(4) or Public(3). (int)
message	Message bytes to be hashed or Write_Context if restoring a context on the ATECC608. Can be NULL if not required by the mode. (bytearray or bytes)
data_out	Data returned by the command (digest or context). (Expects bytearray)
data_out_size	As input, the size of the data_out buffer. As output, the number of bytes returned in data_out. (Expects AtcaReference)

### Returns:

Status code

### 20.2.2.92 atcab\_sha\_end()

```
def cryptoauthlib.atcab.atcab_sha_end (  
    digest,  
    length,  
    message )
```

Executes SHA command to complete SHA-256 or HMAC/SHA-256 operation.

### Args:

length	Length of any remaining data to include in hash. Max 64 bytes. (int)
message	Remaining data to include in hash. NULL if length is 0. (bytearray or bytes)
digest	Digest from SHA-256 or HMAC/SHA-256 will be returned here (32 bytes). (Expects bytearray)

### Returns:

Status code

### 20.2.2.93 atcab\_sha\_hmac()

```
def cryptoauthlib.atcab.atcab_sha_hmac (  
    data,  
    data_size,  
    key_slot,  
    digest,  
    target )
```



Use the SHA command to compute an HMAC/SHA-256 operation.

Args:

<code>data</code>	Message data to be hashed. (bytearray or bytes)
<code>data_size</code>	Size of data in bytes. (int)
<code>key_slot</code>	Slot key id to use for the HMAC calculation (int)
<code>target</code>	Where to save the digest internal to the device. For ATECC608, can be <code>SHA_MODE_TARGET_TEMPKEY</code> , <code>SHA_MODE_TARGET_MSGDIGBUF</code> , or <code>SHA_MODE_TARGET_OUT_ONLY</code> . For all other devices, <code>SHA_MODE_TARGET_TEMPKEY</code> is the only option. (int)
<code>digest</code>	Digest is returned here (32 bytes). (Expects bytearray)

Return:

<code>Status code</code>
--------------------------

#### 20.2.2.94 `atcab_sha_hmac_finish()`

```
def cryptoauthlib.atcab.atcab_sha_hmac_finish (
    ctx,
    digest,
    target )
```

Executes SHA command to complete a HMAC/SHA-256 operation.

Args:

<code>ctx</code>	HMAC/SHA-256 context ( <code>atca_hmac_sha256_ctx_t</code> )
<code>target</code>	Where to save the digest internal to the device. For ATECC608, can be <code>SHA_MODE_TARGET_TEMPKEY</code> , <code>SHA_MODE_TARGET_MSGDIGBUF</code> , or <code>SHA_MODE_TARGET_OUT_ONLY</code> . For all other devices, <code>SHA_MODE_TARGET_TEMPKEY</code> is the only option. (int)
<code>digest</code>	HMAC/SHA-256 result is returned here (32 bytes). (Expects bytearray)

Returns:

<code>Status code</code>
--------------------------

#### 20.2.2.95 `atcab_sha_hmac_init()`

```
def cryptoauthlib.atcab.atcab_sha_hmac_init (
    ctx,
    key_slot )
```

Executes SHA command to start an HMAC/SHA-256 operation

Args:

<code>ctx</code>	HMAC/SHA-256 context ( <code>atca_hmac_sha256_ctx_t</code> )
<code>key_slot</code>	Slot key id to use for the HMAC calculation (int)

Returns:

<code>Status code</code>
--------------------------

### 20.2.2.96 atcab\_sha\_hmac\_update()

```
def cryptoauthlib.atcab.atcab_sha_hmac_update (
    ctx,
    data,
    data_size )
```

Executes SHA command to add an arbitrary amount of message data to a HMAC/SHA-256 operation.

Args:

ctx	HMAC/SHA-256 context (atca_hmac_sha256_ctx_t)
data	Message data to add (bytearray or bytes)
data_size	Size of message data in bytes (int)

Returns:

Status code
-------------

### 20.2.2.97 atcab\_sha\_read\_context()

```
def cryptoauthlib.atcab.atcab_sha_read_context (
    context,
    context_size )
```

Executes SHA command to read the SHA-256 context back. Only for ATECC608 with SHA-256 contexts. HMAC not supported.

Args:

context	Context data is returned here. (Expects bytearray)
context_size	As input, the size of the context buffer in bytes. As output, the size of the returned context data. (Expects AtcaReference)

Returns:

Status code
-------------

### 20.2.2.98 atcab\_sha\_start()

```
def cryptoauthlib.atcab.atcab_sha_start (
    void )
```

Executes SHA command to initialize SHA-256 calculation engine

Args:

None
------

Returns;

Status code
-------------

**20.2.2.99 atcab\_sha\_update()**

```
def cryptoauthlib.atcab.atcab_sha_update (
    message )
```

Executes SHA command to add 64 bytes of message data to the current context.

Args:

message	64 bytes of message data to add to add to operation. (Expects bytearray)
---------	---

Returns:

Status code
-------------

**20.2.2.100 atcab\_sha\_write\_context()**

```
def cryptoauthlib.atcab.atcab_sha_write_context (
    context,
    context_size )
```

Executes SHA command to write (restore) a SHA-256 context into the the device. Only supported for ATECC608 with SHA-256 contexts.

Args:

context	Context data to be restored. (bytearray or bytes)
context_size	Size of the context data in bytes. (int)

Returns:

Status code
-------------

**20.2.2.101 atcab\_sign()**

```
def cryptoauthlib.atcab.atcab_sign (
    key_id,
    msg,
    signature )
```

Executes Sign command, to sign a 32-byte external message using the private key in the specified slot. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.

Args:

key_id	Slot of the private key to be used to sign the message (int)
msg	32-byte message to be signed. Typically the SHA256 hash of the full message. (bytearray or bytes)
signature	Signature will be returned here. Format is R and S integers in big-endian format. 64 bytes for P256 curve. (Expects bytearray)

Returns:

Status code
-------------

### 20.2.2.102 atcab\_sign\_base()

```
def cryptoauthlib.atcab.atcab_sign_base (
    mode,
    key_id,
    signature )
```

Executes the Sign command, which generates a signature using the ECDSA algorithm.

Args:

mode	Mode determines what the source of the message to be signed (int)
key_id	Private key slot used to sign the message. (int)
signature	Signature is returned here. Format is R and S integers in big-endian format. 64 bytes for P256 curve (Expects bytearray)

Returns:

Stauts code

### 20.2.2.103 atcab\_sign\_internal()

```
def cryptoauthlib.atcab.atcab_sign_internal (
    key_id,
    is_invalidate,
    is_full_sn,
    signature )
```

Executes Sign command to sign an internally generated message.

Args:

key_id	Slot of the private key to be used to sign the message (int)
is_invalidate	Set to true if the signature will be used with the Verify(Invalidate) command. false for all other cases.
is_full_sn	Set to true if the message should incorporate the device's full serial number.
signature	Signature is returned here. Format is R and S integers in big-endian format. 64 bytes for P256 curve (Expects bytearray)

Returns:

Status code

### 20.2.2.104 atcab\_updateextra()

```
def cryptoauthlib.atcab.atcab_updateextra (
    mode,
    new_value )
```

Executes UpdateExtra command to update the values of the two extra bytes within the Configuration zone (bytes 84 and 85). an also be used to decrement the limited use counter associated with the key in slot NewValue.

Args:

mode	Mode determines what operations the UpdateExtra command performs. (int)
new_value	Value to be written. (int)

Returns:

Status code

**20.2.2.105 atcab\_verify()**

```
def cryptoauthlib.atcab.atcab_verify (
    mode,
    key_id,
    signature,
    public_key,
    other_data,
    mac )
```

Executes the Verify command, which takes an ECDSA [R,S] signature and verifies that it is correctly generated from a given message and public key. In all cases, the signature is an input to the command. For the Stored, External, and ValidateExternal Modes, the contents of TempKey (or Message Digest Buffer in some cases for the ATECC608) should contain the 32 byte message.

**Args:**

mode	Verify command mode and options (int)
key_id	Stored mode, the slot containing the public key to be used for the verification. ValidateExternal mode, the slot containing the public key to be validated. External mode, KeyID contains the curve type to be used to Verify the signature. Validate or Invalidate mode, the slot containing the public key to be (in)validated. (int)
signature	Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve. (bytearray or bytes)
public_key	If mode is External, the public key to be used for verification. X and Y integers in big-endian format. 64 bytes for P256 curve. NULL for all other modes. (bytearray or bytes)
other_data	If mode is Validate, the bytes used to generate the message for the validation (19 bytes). NULL for all other modes. (bytearray or bytes)
mac	If mode indicates a validating MAC, then the MAC will be returned here. Can be NULL otherwise. (Expects bytearray)

**Returns:**

Status code

**20.2.2.106 atcab\_verify\_extern()**

```
def cryptoauthlib.atcab.atcab_verify_extern (
    message,
    signature,
    public_key,
    is_verified )
```

Executes the Verify command, which verifies a signature (ECDSA verify operation) with all components (message, signature, and public key) supplied. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.

**Args:**

message	32 byte message to be verified. Typically the SHA256 hash of the full message. (Expects bytes)
signature	Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve. (Expects bytes)
public_key	The public key to be used for verification. X and Y integers in big-endian format. 64 bytes for P256 curve. (Expects bytes)

## 20.2 cryptoauthlib.atcab Namespace Reference

---

`is_verified` Boolean whether or not the message, signature, public key verified.  
(Expects AtcaReference)

Returns:  
Status code

### 20.2.2.107 atcab\_verify\_extern\_mac()

```
def cryptoauthlib.atcab.atcab_verify_extern_mac (
    message,
    signature,
    public_key,
    num_in,
    io_key,
    is_verified )
```

Executes the Verify command with verification MAC, which verifies a signature (ECDSA verify operation) with all components (message, signature, and public key) supplied. This function is only available on the ATECC608.

Args:

<code>message</code>	32 byte message to be verified. Typically the SHA256 hash of the full message. (bytearray or bytes)
<code>signature</code>	Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve. (bytearray or bytes)
<code>public_key</code>	The public key to be used for verification. X and Y integers in big-endian format. 64 bytes for P256 curve. (bytearray or bytes)
<code>num_in</code>	System nonce (32 byte) used for the verification MAC. (bytearray or bytes)
<code>io_key</code>	IO protection key for verifying the validation MAC. (bytearray or bytes)
<code>is_verified</code>	Boolean whether or not the message, signature, public key verified. (Expects AtcaReference)

Returns:  
Stats code

### 20.2.2.108 atcab\_verify\_extern\_stored\_mac()

```
def cryptoauthlib.atcab.atcab_verify_extern_stored_mac (
    mode,
    key_id,
    message,
    signature,
    public_key,
    num_in,
    io_key,
    is_verified )
```

Executes the Verify command with verification MAC for the External or Stored Verify modes..

Args:

<code>mode</code>	Verify command mode. Can be VERIFY_MODE_EXTERNAL or VERIFY_MODE_STORED. (int)
<code>key_id</code>	For VERIFY_MODE_STORED mode, the slot containing the public key

	to be used for the verification. For VERIFY_MODE_EXTERNAL mode, KeyID contains the curve type to be used to Verify the signature. Only VERIFY_KEY_P256 supported. (int)
message	32 byte message to be verified. Typically the SHA256 hash of the full message. (bytearray or bytes)
signature	Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve. (bytearray or bytes)
public_key	For VERIFY_MODE_EXTERNAL mode, the public key to be used for verification. X and Y integers in big-endian format. 64 bytes for P256 curve. Null for VERIFY_MODE_STORED mode. (bytearray or bytes)
num_in	System nonce (32 byte) used for the verification MAC. (bytearray or bytes)
io_key	IO protection key for verifying the validation MAC. (bytearray or bytes)
is_verified	Boolean whether or not the message, signature, public key verified. (Expects AtcaReference)

Returns:

Status code

### 20.2.2.109 atcab\_verify\_invalidate()

```
def cryptoauthlib.atcab.atcab_verify_invalidate (
    key_id,
    signature,
    other_data,
    is_verified )
```

Executes the Verify command in Invalidate mode which invalidates a previously validated public key stored in a slot. This command can only be run after GenKey has been used to create a PubKey digest of the public key to be invalidated in TempKey (mode=0x10).

Args:

key_id	Slot containing the public key to be invalidated. (int)
signature	Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve. (bytearray or bytes)
other_data	19 bytes of data used to build the verification message (bytearray or bytes)
is_verified	Boolean whether or not the message, signature, public key verified. (Expects AtcaReference)

Returns:

Status code

### 20.2.2.110 atcab\_verify\_stored()

```
def cryptoauthlib.atcab.atcab_verify_stored (
    message,
    signature,
    key_id,
    is_verified )
```

Executes the Verify command, which verifies a signature (ECDSA verify operation) with a public key stored in the device. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.

Args:

message	32 byte message to be verified. Typically the SHA256 hash of
---------	--

## 20.2 cryptoauthlib.atcab Namespace Reference

---

signature	the full message. (bytearray or bytes) Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve. (bytearray or bytes)
key_id	Slot containing the public key to be used in the verification.(int)
is_verified	Boolean whether or not the message, signature, public key verified. (Expects AtcaReference)

Returns:  
Status code

### 20.2.2.111 atcab\_verify\_stored\_mac()

```
def cryptoauthlib.atcab.atcab_verify_stored_mac (  
    message,  
    signature,  
    key_id,  
    num_in,  
    io_key,  
    is_verified )
```

Executes the Verify command with verification MAC, which verifies a signature (ECDSA verify operation) with a public key stored in the device. This function is only available on the ATECC608.

Args:

message	32 byte message to be verified. Typically the SHA256 hash of the full message. (bytearray or bytes)
signature	Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve. (bytearray or bytes)
key_id	Slot containing the public key to be used in the verification. (int)
num_in	System nonce (32 byte) used for the verification MAC. (bytearray or bytes)
io_key	IO protection key for verifying the validation MAC. (bytearray or bytes)
is_verified	Boolean whether or not the message, signature, public key verified. (Expects AtcaReference)

Returns:  
Status code

### 20.2.2.112 atcab\_verify\_validate()

```
def cryptoauthlib.atcab.atcab_verify_validate (  
    key_id,  
    signature,  
    other_data,  
    is_verified )
```

Executes the Verify command in Validate mode to validate a public key stored in a slot. This command can only be run after GenKey has been used to create a PubKey digest of the public key to be validated in TempKey (mode=0x10).

Args:

key_id	Slot containing the public key to be validated.(int)
--------	--



<code>signature</code>	Signature to be verified. R and S integers in big-endian format. 64 bytes for P256 curve. (bytearray or bytes)
<code>other_data</code>	19 bytes of data used to build the verification message (bytearray or bytes)
<code>is_verified</code>	Boolean whether or not the message, signature, public key verified. (Expects AtcaReference)

Returns:  
    Status code

### 20.2.2.113 atcab\_write()

```
def cryptoauthlib.atcab.atcab_write (
    zone,
    address,
    value,
    mac )
```

Executes the Write command, which writes either one four byte word or a 32-byte block to one of the EEPROM zones on the device. Depending upon the value of the WriteConfig byte for this slot, the data may be required to be encrypted by the system prior to being sent to the device. This command cannot be used to write slots configured as ECC private keys.

Args:

<code>zone</code>	Zone/Param1 for the write command. (int)
<code>address</code>	Address/Param2 for the write command. (int)
<code>value</code>	Plain-text data to be written or cipher-text for encrypted writes. 32 or 4 bytes depending on bit 7 in the zone. (bytearray or bytes)
<code>data</code>	Data to be written. (bytearray or bytes)
<code>mac</code>	MAC required for encrypted writes (32 bytes). (bytearray or bytes)

Returns:  
    Status code

### 20.2.2.114 atcab\_write\_bytes\_zone()

```
def cryptoauthlib.atcab.atcab_write_bytes_zone (
    zone,
    slot,
    offset_bytes,
    data,
    length )
```

Executes the Write command, which writes data into config, otp, or data zone with a given byte offset and length. Offset and length must be multiples of a word (4 bytes).

Config zone must be unlocked for writes to that zone. If data zone is unlocked, only 32-byte writes are allowed to slots and OTP and the offset and length must be multiples of 32 or the write will fail.

Args:

<code>zone</code>	Zone to write data to: Zones.ATCA_ZONE_CONFIG, Zones.ATCA_ZONE_OTP, or Zones.ATCA_ZONE_DATA. (int)
<code>slot</code>	If zone is Zones.ATCA_ZONE_DATA, the slot number to write to.

	Ignored for all other zones. (int)
<code>offset_bytes</code>	Byte offset within the zone to write to. Must be a multiple of a word (4 bytes). (int)
<code>data</code>	bytearray containing Data to be written. (bytearray or bytes)
<code>length</code>	Number of bytes to be written. Must be a multiple of a word (4 bytes). (int)

Returns:  
None

### 20.2.2.115 `atcab_write_config_counter()`

```
def cryptoauthlib.atcab.atcab_write_config_counter (
    counter_id,
    counter_value )
```

Initialize one of the monotonic counters in device with a specific value. The monotonic counters are stored in the configuration zone using a special format. This encodes a binary count value into the 8 byte encoded value required. This can only be set while the configuration zone is unlocked.

Args:

<code>counter_id</code>	Counter to be written (int)
<code>counter_value</code>	Counter value to set (int)

### 20.2.2.116 `atcab_write_config_zone()`

```
def cryptoauthlib.atcab.atcab_write_config_zone (
    conf )
```

Executes the Write command, which writes the configuration zone. First 16 bytes are skipped as they are not writable. LockValue and LockConfig are also skipped and can only be changed via the Lock command.

This command may fail if UserExtra and/or Selector bytes have already been set to non-zero values.

Args:

<code>conf</code>	Data to the config zone data. This should be a 88 byte bytearray for SHA devices and 128 byte bytearray for ECC devices. (bytearray or bytes)
-------------------	---

Returns:  
Status code

**20.2.2.117 atcab\_write\_enc()**

```
def cryptoauthlib.atcab.atcab_write_enc (
    key_id,
    block,
    data,
    enc_key,
    enc_key_id,
    num_in = None )
```

Executes the Write command, which performs an encrypted write of a 32 byte block into given slot. The function takes clear text bytes and encrypts them for writing over the wire. Data zone must be locked and the slot configuration must be set to encrypted write for the block to be successfully written.

**Args:**

key_id	Slot ID to write to. (int)
block	Index of the 32 byte block to write in the slot. (int)
data	32 bytes of clear text data to be written to the slot. (bytearray or bytes)
enc_key	WriteKey to encrypt with for writing (bytearray or bytes)
enc_key_id	The KeyID of the WriteKey (int)
num_in	Bytearray - Host nonce used to calculate nonce (20 bytes)

**Returns:**

Status code

**20.2.2.118 atcab\_write\_pubkey()**

```
def cryptoauthlib.atcab.atcab_write_pubkey (
    slot,
    public_key )
```

Executes the Write command, which writes a public key to a data slot in the device format.

**Args:**

slot	Slot number to write. Only slots 8 to 15 are large enough to store a public key. (int)
public_key	Public key to write into the slot specified. X and Y integers in big-endian format. 64 bytes for P256 curve. (bytearray or bytes)

**Returns:**

Status code

**20.2.2.119 atcab\_write\_zone()**

```
def cryptoauthlib.atcab.atcab_write_zone (
    zone,
    slot,
    block,
    offset,
    data,
    length )
```

## 20.3 cryptauthlib.atcacert Namespace Reference

---

Executes the Write command, which writes either 4 or 32 bytes of data into a device zone.

Args:

zone	Device zone to write to (0=config, 1=OTP, 2=data). (int)
slot	If writing to the data zone, it is the slot to write to, otherwise it should be 0. (int)
block	32-byte block to write to. (int)
offset	4-byte word within the specified block to write to. If performing a 32-byte write, this should be 0. (int)
data	Data to be written. (bytearray or bytes)
len	Number of bytes to be written. Must be either 4 or 32. (int)

Returns:

Status code

## 20.3 cryptauthlib.atcacert Namespace Reference

### Data Structures

- class [atcacert\\_cert\\_element\\_t](#)
- class [atcacert\\_cert\\_loc\\_t](#)
- class [atcacert\\_cert\\_sn\\_src\\_t](#)
- class [atcacert\\_cert\\_type\\_t](#)
- class [atcacert\\_comp\\_data\\_t](#)
- class [atcacert\\_date\\_format\\_t](#)
- class [atcacert\\_def\\_t](#)
- class [atcacert\\_device\\_loc\\_t](#)
- class [atcacert\\_device\\_zone\\_t](#)
- class [atcacert\\_std\\_cert\\_element\\_t](#)
- class [atcacert\\_tm\\_utc\\_t](#)
- class [atcacert\\_transform\\_t](#)
- class [CertStatus](#)

### Functions

- def [\\_atcacert\\_convert\\_bytes](#) (kwargs, name, pointer)
- def [\\_atcacert\\_convert\\_enum](#) (kwargs, name, enum)
- def [atcacert\\_max\\_cert\\_size](#) (cert\_def, max\_cert\_size)
- def [atcacert\\_get\\_response](#) (device\_private\_key\_slot, challenge, response)
- def [atcacert\\_read\\_cert](#) (cert\_def, ca\_public\_key, cert, cert\_size)
- def [atcacert\\_write\\_cert](#) (cert\_def, cert, cert\_size)
- def [atcacert\\_create\\_csr](#) (csr\_def, csr, csr\_size)
- def [atcacert\\_create\\_csr\\_pem](#) (csr\_def, csr, csr\_size)
- def [atcacert\\_date\\_enc](#) (date\_format, timestamp, formatted\_date, formatted\_date\_size)
- def [atcacert\\_date\\_dec](#) (date\_format, formatted\_date, formatted\_date\_size, timestamp)
- def [atcacert\\_date\\_enc\\_compcert](#) (issue\_date, expire\_years, enc\_dates)
- def [atcacert\\_date\\_dec\\_compcert](#) (enc\_dates, expire\_date\_format, issue\_date, expire\_date)
- def [atcacert\\_date\\_get\\_max\\_date](#) (date\_format, timestamp)

### 20.3.1 Detailed Description

ATCACERT: classes and functions for interacting with compressed certificates

## 20.3.2 Function Documentation

### 20.3.2.1 `_atcacert_convert_bytes()`

```
def cryptoauthlib.atcacert._atcacert_convert_bytes (
    kwargs,
    name,
    pointer ) [protected]
```

Internal Helper Function: Convert python 'bytes' into memory pointer for ctypes structure  
:param kwargs: kwargs dictionary  
:param name: `_field_` name that will be converted  
:param pointer: Conversion Class (resulting type - pointer of type x)  
:return:

### 20.3.2.2 `_atcacert_convert_enum()`

```
def cryptoauthlib.atcacert._atcacert_convert_enum (
    kwargs,
    name,
    enum ) [protected]
```

Internal Helper Function: Convert python enum into ctypes integer  
:param kwargs: kwargs dictionary  
:param name: `_field_` name that will be converted  
:param enum: Conversion Class (resulting type)  
:return:

### 20.3.2.3 `atcacert_create_csr()`

```
def cryptoauthlib.atcacert.atcacert_create_csr (
    csr_def,
    csr,
    csr_size )
```

Creates a CSR specified by the CSR definition from the ATECC508A device.  
This process involves reading the dynamic CSR data from the device and combining it  
with the template found in the CSR definition, then signing it. Return the CSR int der format

Args:

<code>csr_def</code>	CSR definition describing where to find the dynamic CSR information on the device and how to incorporate it into the template. Expects <code>atcacert_def_t</code> .
<code>csr</code>	Buffer to receive the CSR. Expects bytearray.
<code>csr_size</code>	As input, the size of the CSR buffer in bytes. As output, the size of the CSR as PEM returned in cert in bytes. Expects <code>AtcaReference</code> .

Returns:

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 20.3.2.4 atcacert\_create\_csr\_pem()

```
def cryptoauthlib.atcacert.atcacert_create_csr_pem (
    csr_def,
    csr,
    csr_size )
```

Creates a CSR specified by the CSR definition from the ATECC508A device. This process involves reading the dynamic CSR data from the device and combining it with the template found in the CSR definition, then signing it. Return the CSR in der format

Args:

csr_def	CSR definition describing where to find the dynamic CSR information on the device and how to incorporate it into the template. Expects atcacert_def_t.
csr	Buffer to receive the CSR. Expects bytearray.
csr_size	As input, the size of the CSR buffer in bytes. As output, the size of the CSR as PEM returned in cert in bytes. Expects AtcaReference.

Returns:

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 20.3.2.5 atcacert\_date\_dec()

```
def cryptoauthlib.atcacert.atcacert_date_dec (
    date_format,
    formatted_date,
    formatted_date_size,
    timestamp )
```

Parse a formatted timestamp according to the specified format.

Args:

date_format	Format to parse the formatted date as.
formatted_date	Formatted date to be parsed.
formatted_date_size	Size of the formatted date in bytes.
timestamp	Parsed timestamp is returned here. Expects atcacert_tm_utc_t.

Returns:

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 20.3.2.6 atcacert\_date\_dec\_compcert()

```
def cryptoauthlib.atcacert.atcacert_date_dec_compcert (
    enc_dates,
    expire_date_format,
    issue_date,
    expire_date )
```

Decode the issue and expire dates from the format used by the compressed certificate.

Args:

<code>enc_dates</code>	Encoded date from the compressed certificate. 3 bytes.
<code>expire_date_format</code>	Expire date format. Only used to determine max date when no expiration date is specified by the encoded date.
<code>issue_date</code>	Decoded issue date is returned here. Expects <code>atcacert_tm_utc_t</code> .
<code>expire_date</code>	Decoded expire date is returned here. If there is no expiration date, the expire date will be set to a maximum value for the given <code>expire_date_format</code> . Expects <code>atcacert_tm_utc_t</code> .

Returns:

`ATCACERT_E_SUCCESS` on success

### 20.3.2.7 `atcacert_date_enc()`

```
def cryptoauthlib.atcacert.atcacert_date_enc (
    date_format,
    timestamp,
    formatted_date,
    formatted_date_size )
```

Format a timestamp according to the format type.

Args:

<code>date_format</code>	Format to use.
<code>timestamp</code>	Timestamp to format. Expects <code>atcacert_tm_utc_t</code> .
<code>formatted_date</code>	Formatted date will be returned in this buffer. Expects bytearray.
<code>formatted_date_size</code>	As input, the size of the <code>formatted_date</code> buffer. As output, the size of the returned <code>formatted_date</code> . Expects <code>AtcaReference</code> .

Returns:

`ATCACERT_E_SUCCESS` on success, otherwise an error code.

### 20.3.2.8 `atcacert_date_enc_compcert()`

```
def cryptoauthlib.atcacert.atcacert_date_enc_compcert (
    issue_date,
    expire_years,
    enc_dates )
```

Encode the issue and expire dates in the format used by the compressed certificate.

Args:

<code>issue_date</code>	Issue date to encode. Note that minutes and seconds will be ignored. Expects <code>atcacert_tm_utc_t</code> .
<code>expire_years</code>	Expire date is expressed as a number of years past the issue date. 0 should be used if there is no expire date.
<code>enc_dates</code>	Encoded dates for use in the compressed certificate is returned here. 3 bytes. Expects bytearray.

Returns:

`ATCACERT_E_SUCCESS` on success

### 20.3.2.9 atcacert\_date\_get\_max\_date()

```
def cryptoauthlib.atcacert.atcacert_date_get_max_date (
    date_format,
    timestamp )
```

Return the maximum date available for the given format.

Args:

format	Format to get the max date for.
timestamp	Max date is returned here. Expects atcacert_tm_utc_t.

Returns:

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 20.3.2.10 atcacert\_get\_response()

```
def cryptoauthlib.atcacert.atcacert_get_response (
    device_private_key_slot,
    challenge,
    response )
```

Calculates the response to a challenge sent from the host.

The challenge-response protocol is an ECDSA Sign and Verify. This performs the ECDSA Sign on the challenge and returns the signature as the response.

Args:

device_private_key_slot	Slot number for the device's private key. This must be the same slot used to generate the public key included in the device's certificate.
challenge	Challenge to generate the response for. Must be 32 bytes.
response	Response will be returned in this buffer. 64 bytes.

Returns:

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 20.3.2.11 atcacert\_max\_cert\_size()

```
def cryptoauthlib.atcacert.atcacert_max_cert_size (
    cert_def,
    max_cert_size )
```

Return the maximum possible certificate size in bytes for a given cert def. Certificate can be variable size, so this gives an appropriate buffer size when reading the certificates.

Args:

cert_def	Certificate definition to find a max size for. Expects atcacert_def_t.
max_cert_size	Maximum certificate size will be returned here in bytes. Expects AtcaReference.

Returns:

ATCACERT\_E\_SUCCESS on success, otherwise an error code.



### 20.3.2.12 atcacert\_read\_cert()

```
def cryptoauthlib.atcacert.atcacert_read_cert (
    cert_def,
    ca_public_key,
    cert,
    cert_size )
```

Reads the certificate specified by the certificate definition from the ATECC508A device.

This process involves reading the dynamic cert data from the device and combining it with the template found in the certificate definition.

**Args:**

cert_def	Certificate definition describing where to find the dynamic certificate information on the device and how to incorporate it into the template. Expects atcacert_def_t.
ca_public_key	The ECC P256 public key of the certificate authority that signed this certificate. Formatted as the 32 byte X and Y integers concatenated together (64 bytes total). Set to NULL if the authority key id is not needed, set properly in the cert_def template, or stored on the device as specified in the cert_def cert_elements.
cert	Buffer to received the certificate. Expects bytearray.
cert_size	As input, the size of the cert buffer in bytes. As output, the size of the certificate returned in cert in bytes. Expects AtcaReference.

**Returns:**

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 20.3.2.13 atcacert\_write\_cert()

```
def cryptoauthlib.atcacert.atcacert_write_cert (
    cert_def,
    cert,
    cert_size )
```

Take a full certificate and write it to the ATECC508A device according to the certificate definition.

**Args:**

cert_def	Certificate definition describing where the dynamic certificate information is and how to store it on the device. Expects atcacert_def_t.
cert	Full certificate to be stored.
cert_size	Size of the full certificate in bytes.

**Returns:**

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

## 20.4 cryptoauthlib.atcaenum Namespace Reference

### Data Structures

- class [AtcaEnum](#)

### 20.4.1 Detailed Description

Enum Extension for improved comparisons

## 20.5 cryptauthlib.atjwt Namespace Reference

### Data Structures

- class [HwEcAlgorithm](#)
- class [HwHmacAlgorithm](#)
- class [PyJWT](#)

### Variables

- `try` :

### 20.5.1 Detailed Description

JWT: Extension to the `jwt` module with hardware based security

## 20.6 cryptauthlib.device Namespace Reference

### Data Structures

- class [AesEnable](#)
- class [Atecc508aConfig](#)
- class [Atecc608Config](#)
- class [Atsha204aConfig](#)
- class [ChipMode508](#)
- class [ChipMode608](#)
- class [ChipOptions](#)
- class [Counter204](#)
- class [CountMatch](#)
- class [I2cEnable](#)
- class [KeyConfig](#)
- class [SecureBoot](#)
- class [SlotConfig](#)
- class [UseLock](#)
- class [VolatileKeyPermission](#)
- class [X509Format](#)

### 20.6.1 Detailed Description

Cryptauthlib Device Configuration

## 20.7 cryptoauthlib.exceptions Namespace Reference

### Data Structures

- class [AssertionFailure](#)
- class [BadArgumentError](#)
- class [BadCrcError](#)
- class [BadOpcodeError](#)
- class [CheckmacVerifyFailedError](#)
- class [CommunicationError](#)
- class [ConfigZoneLockedError](#)
- class [CrcError](#)
- class [CryptoError](#)
- class [DataZoneLockedError](#)
- class [EccFaultError](#)
- class [ExecutionError](#)
- class [FunctionError](#)
- class [GenericError](#)
- class [HealthTestError](#)
- class [InvalidIdentifierError](#)
- class [InvalidSizeError](#)
- class [LibraryLoadError](#)
- class [LibraryMemoryError](#)
- class [LibraryNotInitialized](#)
- class [NoDevicesFoundError](#)
- class [NoResponseError](#)
- class [NoUseFlagError](#)
- class [ParityError](#)
- class [ParseError](#)
- class [ReceiveError](#)
- class [ReceiveTimeoutError](#)
- class [ResyncWithWakeupError](#)
- class [StatusUnknownError](#)
- class [TimeOutError](#)
- class [TransmissionError](#)
- class [TransmissionTimeoutError](#)
- class [UnimplementedError](#)
- class [UnsupportedInterface](#)
- class [WakeFailedError](#)
- class [ZoneNotLockedError](#)

### 20.7.1 Detailed Description

Cryptoauthlib Exceptions

## 20.8 cryptauthlib.iface Namespace Reference

### Data Structures

- class [\\_ATCACUSTOM](#)
- class [\\_ATCAHID](#)
- class [\\_ATCAI2C](#)
- class [\\_ATCAIfaceParams](#)
- class [\\_ATCAKIT](#)
- class [\\_ATCASPI](#)
- class [\\_ATCASWI](#)
- class [\\_ATCAUART](#)
- class [\\_U\\_Address](#)
- class [ATCADeviceType](#)
- class [ATCAIfaceCfg](#)
- class [ATCAIfaceType](#)
- class [ATCAKitType](#)

### Functions

- def [\\_iface\\_load\\_default\\_config](#) (name)
- def [cfg\\_ateccx08a\\_i2c\\_default](#) ()
- def [cfg\\_ateccx08a\\_swi\\_default](#) ()
- def [cfg\\_ateccx08a\\_kithid\\_default](#) ()
- def [cfg\\_atsha20xa\\_i2c\\_default](#) ()
- def [cfg\\_atsha20xa\\_swi\\_default](#) ()
- def [cfg\\_atsha20xa\\_kithid\\_default](#) ()

#### 20.8.1 Detailed Description

Interface Configuration

#### 20.8.2 Function Documentation

##### 20.8.2.1 [\\_iface\\_load\\_default\\_config\(\)](#)

```
def cryptauthlib.iface._iface_load_default_config (  
    name ) [protected]
```

"Attempt to load the default configuration structure from the library by name

### 20.8.2.2 `cfg_ateccx08a_i2c_default()`

```
def cryptoauthlib.iface.cfg_ateccx08a_i2c_default ( )
```

Default configuration for an ECCx08A device on the first logical I2C bus

### 20.8.2.3 `cfg_ateccx08a_kithid_default()`

```
def cryptoauthlib.iface.cfg_ateccx08a_kithid_default ( )
```

Default configuration for Kit protocol over a HID interface

### 20.8.2.4 `cfg_ateccx08a_swi_default()`

```
def cryptoauthlib.iface.cfg_ateccx08a_swi_default ( )
```

Default configuration for an ECCx08A device on the logical SWI bus over UART

### 20.8.2.5 `cfg_atsha20xa_i2c_default()`

```
def cryptoauthlib.iface.cfg_atsha20xa_i2c_default ( )
```

Default configuration for a SHA204A device on the first logical I2C bus

### 20.8.2.6 `cfg_atsha20xa_kithid_default()`

```
def cryptoauthlib.iface.cfg_atsha20xa_kithid_default ( )
```

Default configuration for Kit protocol over a HID interface for SHA204

### 20.8.2.7 `cfg_atsha20xa_swi_default()`

```
def cryptoauthlib.iface.cfg_atsha20xa_swi_default ( )
```

Default configuration for an SHA204A device on the logical SWI bus over UART

## 20.9 cryptoauthlib.library Namespace Reference

### Data Structures

- class [\\_CtypeIterator](#)
- class [AtcaReference](#)
- class [AtcaStructure](#)
- class [AtcaUnion](#)

### Functions

- def **indent** (lines, insert)
- def [\\_force\\_local\\_library](#) ()
- def [load\\_cryptoauthlib](#) (lib=None)
- def [get\\_cryptoauthlib](#) ()
- def [get\\_device\\_name](#) (revision)
- def [get\\_device\\_name\\_with\\_device\\_id](#) (revision)
- def [get\\_device\\_type\\_id](#) (name)
- def [get\\_size\\_by\\_name](#) (name)
- def [get\\_ctype\\_by\\_name](#) (name)
- def [get\\_ctype\\_structure\\_instance](#) (structure, value)
- def [get\\_ctype\\_array\\_instance](#) (array, value)
- def [\\_get\\_field\\_definition](#) (obj, name)
- def [\\_def\\_to\\_field](#) (f\_type, f\_size=None)
- def [\\_convert\\_pointer\\_to\\_list](#) (p, length)
- def [\\_get\\_attribute\\_from\\_ctypes](#) (obj, obj\_type, length=None, \*args)
- def [\\_check\\_type\\_rationality](#) (cls)
- def [\\_array\\_to\\_code](#) (obj, name=None, parent=None, \*\*kwargs)
- def [\\_object\\_definition\\_code](#) (obj, name=None, parent=None, parent\_name=None, anon=None, type↵ info=None, check\_names={}, \*\*kwargs)
- def [\\_union\\_to\\_code](#) (obj, name=None, parent=None, anon=None, entry=None, parent\_name=None, type↵ \_info=None, \*\*kwargs)
- def [\\_structure\\_to\\_code](#) (obj, name=None, parent=None, type\_info=None, parent\_name=None, \*\*kwargs)
- def [\\_obj\\_to\\_code](#) (obj, name, parent=None, anon=None, parent\_name=None, \*\*kwargs)
- def [\\_pointer\\_to\\_code](#) (obj, name=None, parent=None, parent\_name=None, check\_names={}, skip↵ references=[], \*\*kwargs)
- def [\\_is\\_pointer](#) (obj, type\_info=None, \*\*kwargs)
- def [\\_to\\_code](#) (obj, name=None, \*\*kwargs)
- def [\\_structure\\_to\\_string](#) (item, int level=0)
- def [\\_ctype\\_from\\_definition](#) (cls)
- def [ctypes\\_to\\_bytes](#) (obj)
- def [create\\_byte\\_buffer](#) (init\_or\_size)

## Variables

- **try :**
- dict **ATCA\_NAMES** = {'i2c': 'i2c', 'hid': 'kithid', 'sha': 'sha204', 'ecc': 'eccx08'}
- None **\_CRYPTO\_LIB** = None
- dict **\_CTYPES\_BY\_SIZE** = {1: c\_uint8, 2: c\_uint16, 4:c\_uint32}
- **\_fields\_**

### 20.9.1 Detailed Description

Cryptoauthlib Library Management

### 20.9.2 Function Documentation

#### 20.9.2.1 `_array_to_code()`

```
def cryptoauthlib.library._array_to_code (
    obj,
    name = None,
    parent = None,
    ** kwargs ) [protected]
```

Convert an array like item from a ctypes structure into a C language formatted string

#### 20.9.2.2 `_check_type_rationality()`

```
def cryptoauthlib.library._check_type_rationality (
    cls ) [protected]
```

This checks the structure or union size against the constants that are stored in the library during compilation. This is not an absolute guarentee that alignment is completely correct but it will catch most cases of incompatibility between the compiled library that is installed and the python module

#### 20.9.2.3 `_convert_pointer_to_list()`

```
def cryptoauthlib.library._convert_pointer_to_list (
    p,
    length ) [protected]
```

Pointer types can be frustrating to interact with generally when processing data in python so this converts them into types that are iterable and bounded

### 20.9.2.4 `_ctype_from_definition()`

```
def cryptoauthlib.library._ctype_from_definition (
    cls ) [protected]
```

Extends the ctypes structure and union types to add a new attribute `_def_` which is a dictionary of field attributes. This extends functionality by quite a bit by supporting additional types and field linkages

### 20.9.2.5 `_def_to_field()`

```
def cryptoauthlib.library._def_to_field (
    f_type,
    f_size = None ) [protected]
```

Helper function to convert an entry in the `_def_` dictionary to the tuple required for a `_field_` entry

### 20.9.2.6 `_force_local_library()`

```
def cryptoauthlib.library._force_local_library ( ) [protected]
```

In some environments loading seems to fail under all circumstances unless brute forcing it.

### 20.9.2.7 `_get_attribute_from_ctypes()`

```
def cryptoauthlib.library._get_attribute_from_ctypes (
    obj,
    obj_type,
    length = None,
    * args ) [protected]
```

Helper function that is used by `AtcaStructure` and `AtcaUnion` to intercept attribute access to those objects and convert the resulting values into easier to use python objects based on the configuration of the structure/union



### 20.9.2.8 `_get_field_definition()`

```
def cryptoauthlib.library._get_field_definition (
    obj,
    name ) [protected]
```

Get meta information about the ctypes structure/union by accessing the field description attributes of the class that were provided as part of the ctypes structure/union definition

### 20.9.2.9 `_is_pointer()`

```
def cryptoauthlib.library._is_pointer (
    obj,
    type_info = None,
    ** kwargs ) [protected]
```

Checks to see if object looks like a pointer

### 20.9.2.10 `_obj_to_code()`

```
def cryptoauthlib.library._obj_to_code (
    obj,
    name,
    parent = None,
    anon = None,
    parent_name = None,
    ** kwargs ) [protected]
```

Convert python/ctypes object into a C language representation

### 20.9.2.11 `_object_definition_code()`

```
def cryptoauthlib.library._object_definition_code (
    obj,
    name = None,
    parent = None,
    parent_name = None,
    anon = None,
    type_info = None,
    check_names = {},
    ** kwargs ) [protected]
```

Emits the first half of the assignment of this object

### 20.9.2.12 `_pointer_to_code()`

```
def cryptoauthlib.library._pointer_to_code (
    obj,
    name = None,
    parent = None,
    parent_name = None,
    check_names = {},
    skip_references = [],
    ** kwargs ) [protected]
```

Convert the pointer into a representative object by creating a definition in the prepend area

### 20.9.2.13 `_structure_to_code()`

```
def cryptoauthlib.library._structure_to_code (
    obj,
    name = None,
    parent = None,
    type_info = None,
    parent_name = None,
    ** kwargs ) [protected]
```

Emits a string with a C language representation of the structure(s) following pointers the best that is can

### 20.9.2.14 `_structure_to_string()`

```
def cryptoauthlib.library._structure_to_string (
    item,
    int level = 0 ) [protected]
```

Emits a readable string of the structure elements coverting types and following pointers and arrays the best that is can

### 20.9.2.15 `_to_code()`

```
def cryptoauthlib.library._to_code (
    obj,
    name = None,
    ** kwargs ) [protected]
```

Map object types to the proper renderer function by catching pointer like objects first

Returns: (append, prepend)

#### 20.9.2.16 ctypes\_to\_bytes()

```
def cryptoauthlib.library.ctypes_to_bytes (
    obj )
```

Convert a ctypes structure/array into bytes. This is for python2 compatibility

#### 20.9.2.17 get\_cryptoauthlib()

```
def cryptoauthlib.library.get_cryptoauthlib ( )
```

This is a helper function for the other python files in this module to use the loaded library

#### 20.9.2.18 get\_ctype\_array\_instance()

```
def cryptoauthlib.library.get_ctype_array_instance (
    array,
    value )
```

Internal Helper Function: Convert python list into ctype array  
:param value: Value to convert  
:param array: Conversion Class (resulting type)  
:return:

#### 20.9.2.19 get\_ctype\_by\_name()

```
def cryptoauthlib.library.get_ctype_by_name (
    name )
```

For known (atca\_utils\_sizes.c) types that are custom to the library retrieve the size

#### 20.9.2.20 get\_ctype\_structure\_instance()

```
def cryptoauthlib.library.get_ctype_structure_instance (
    structure,
    value )
```

Internal Helper Function: Convert a value into the correct ctypes structure for a given field  
:param value: Value to convert  
:param structure: Conversion Class (resulting type)  
:return:

### 20.9.2.21 `get_device_name()`

```
def cryptoauthlib.library.get_device_name (
    revision )
```

Returns the device name based on the info byte array values returned by `atcab_info`

### 20.9.2.22 `get_device_name_with_device_id()`

```
def cryptoauthlib.library.get_device_name_with_device_id (
    revision )
```

Returns the device name based on the info byte array values returned by `atcab_info` for ECC204 family

### 20.9.2.23 `get_device_type_id()`

```
def cryptoauthlib.library.get_device_type_id (
    name )
```

Returns the `ATCADeviceType` value based on the device name

### 20.9.2.24 `get_size_by_name()`

```
def cryptoauthlib.library.get_size_by_name (
    name )
```

Get the size of an object in the library using the `name_size` api from `atca_utils_sizes.c`

### 20.9.2.25 `load_cryptoauthlib()`

```
def cryptoauthlib.library.load_cryptoauthlib (
    lib = None )
```

Load `CryptoAuthLib` into Python environment  
raise `LibraryLoadError` if `cryptoauthlib` library can't be loaded

## 20.10 cryptoauthlib.sha206\_api Namespace Reference

### Functions

- def [sha206a\\_generate\\_derive\\_key](#) (parent\_key, derived\_key, param1, param2)
- def [sha206a\\_generate\\_challenge\\_response\\_pair](#) (key, challenge, response)
- def [sha206a\\_authenticate](#) (challenge, expected\_response, is\_verified)
- def [sha206a\\_write\\_data\\_store](#) (slot, data, block, offset, length, lock\_after\_write)
- def [sha206a\\_read\\_data\\_store](#) (slot, data, offset, length)
- def [sha206a\\_get\\_data\\_store\\_lock\\_status](#) (slot, is\_locked)
- def [sha206a\\_get\\_dk\\_update\\_count](#) (dk\_update\_count)
- def [sha206a\\_get\\_pk\\_useflag\\_count](#) (pk\_avail\_count)
- def [sha206a\\_get\\_dk\\_useflag\\_count](#) (dk\_avail\_count)
- def [sha206a\\_check\\_pk\\_useflag\\_validity](#) (is\_consumed)
- def [sha206a\\_check\\_dk\\_useflag\\_validity](#) (is\_consumed)
- def [sha206a\\_verify\\_device\\_consumption](#) (is\_consumed)
- def [sha206a\\_diversify\\_parent\\_key](#) (parent\_key, diversified\_key)

### 20.10.1 Detailed Description

SHA206 API: classes and functions for interacting with SHA206A device

### 20.10.2 Function Documentation

#### 20.10.2.1 sha206a\_authenticate()

```
def cryptoauthlib.sha206_api.sha206a_authenticate (
    challenge,
    expected_response,
    is_verified )
```

verifies the challenge and provided response using key in device

Args:

challenge	Challenge to be used in the response calculations (Expects bytearray of size 32)
expected_response	Expected response from the device (Expects bytearray of size 32)
is_authenticated	result of expected of response and calcualted response (AtcaReference expected)

Returns:

Status Code

### 20.10.2.2 sha206a\_check\_dk\_useflag\_validity()

```
def cryptoauthlib.sha206_api.sha206a_check_dk_useflag_validity (
    is_consumed )
```

verifies Derived Key use flags for consumption

Args:

is_consumed	indicates if derived key is available for consumption (Expected AtcaReference)
-------------	---

Returns:

Status Code
-------------

### 20.10.2.3 sha206a\_check\_pk\_useflag\_validity()

```
def cryptoauthlib.sha206_api.sha206a_check_pk_useflag_validity (
    is_consumed )
```

verifies Parent Key use flags for consumption

Args:

is_consumed	indicates if parent key is available for consumption (Expected AtcaReference)
-------------	--

Returns:

Status Code
-------------

### 20.10.2.4 sha206a\_diversify\_parent\_key()

```
def cryptoauthlib.sha206_api.sha206a_diversify_parent_key (
    parent_key,
    diversified_key )
```

Computes the diversified key based on the parent key provided and device serial number

Args:

parent_key	parent key to be diversified (Expected bytearray of size 32)
diversified_key	output diversified key is returned here (Expected bytearray of size 32)

Returns:

Status Code
-------------

### 20.10.2.5 sha206a\_generate\_challenge\_response\_pair()

```
def cryptoauthlib.sha206_api.sha206a_generate_challenge_response_pair (
    key,
    challenge,
    response )
```

Generates the response based on Key and Challenge provided

Args:

key	input data contains device's key (Expects bytearray of size 32)
challenge	input data to be used in challenge response calculation (Expects bytearray of size 32)
response	output response is returned here (Expects bytearray of size 32)

Returns:

Status Code
-------------

### 20.10.2.6 sha206a\_generate\_derive\_key()

```
def cryptoauthlib.sha206_api.sha206a_generate_derive_key (
    parent_key,
    derived_key,
    param1,
    param2 )
```

Generates the derived key based on the parent key and other parameters provided

Args:

parent_key	input data contains device's parent key (Expects bytearray of size 32)
derived key	output derived key is returned here (Expects bytearray of size 32)
param1	input data to be used in derive key calculation (int)
param2	input data to be used in derive key calculation (int)

Returns:

Status Code
-------------

### 20.10.2.7 sha206a\_get\_data\_store\_lock\_status()

```
def cryptoauthlib.sha206_api.sha206a_get_data_store_lock_status (
    slot,
    is_locked )
```

## 20.10 cryptoauthlib.sha206\_api Namespace Reference

---

Returns the lock status of the given data store

Args:

slot	Slot number of the data store (int)
is_locked	lock status of the data store slot (Expected AtcaReference)

Returns:

Status Code
-------------

### 20.10.2.8 sha206a\_get\_dk\_update\_count()

```
def cryptoauthlib.sha206_api.sha206a_get_dk_update_count (
    dk_update_count )
```

Read Derived Key slot update count. It will be wraps around 256

Args:

dk_update_count	returns number of times the slot has been updated with derived key (Expected AtcaReference)
-----------------	--

Returns:

Status Code
-------------

### 20.10.2.9 sha206a\_get\_dk\_useflag\_count()

```
def cryptoauthlib.sha206_api.sha206a_get_dk_useflag_count (
    dk_avail_count )
```

calculates available Derived Key use counts

Args:

dk_avail_count	counts available bit's as 1 (int)
----------------	-----------------------------------

Returns:

Status Code
-------------

### 20.10.2.10 sha206a\_get\_pk\_useflag\_count()

```
def cryptoauthlib.sha206_api.sha206a_get_pk_useflag_count (
    pk_avail_count )
```

calculates available Parent Key use counts

Args:

pk_avail_count	counts available bit's as 1 (int)
----------------	-----------------------------------

Returns:

Status Code
-------------



**20.10.2.11 sha206a\_read\_data\_store()**

```
def cryptoauthlib.sha206_api.sha206a_read_data_store (
    slot,
    data,
    offset,
    length )
```

Read the data stored in Data store

**Args:**

slot	Slot number to read from (int)
data	Pointer that holds the data (Expected bytearray of size 32)
offset	Byte offset within the zone to read from. (int)
length	data length (int)

**Returns:**

Status Code

**20.10.2.12 sha206a\_verify\_device\_consumption()**

```
def cryptoauthlib.sha206_api.sha206a_verify_device_consumption (
    is_consumed )
```

verifies the device is fully consumed or not based on Parent and Derived Key use flags.

**Args:**

is_consumed	result of device consumption is returned here (Expected AtcaReference)
-------------	---

**Returns:**

Status Code

**20.10.2.13 sha206a\_write\_data\_store()**

```
def cryptoauthlib.sha206_api.sha206a_write_data_store (
    slot,
    data,
    block,
    offset,
    length,
    lock_after_write )
```

## 20.11 cryptoauthlib.status Namespace Reference

---

Update the data store slot with user data and lock it if necessary

Args:

slot	Slot number to be written with data (int)
data	Pointer that holds the data (Expected bytearray of size 32)
block	32-byte block to write (int)
offset	4-byte word within the specified block to write to. If performing a 32-byte write, this should be 0. (int)
length	data length (int)
lock_after_write	set 1 to lock slot after write, otherwise 0 (Expected bool/int)

Returns:

Status Code

## 20.11 cryptoauthlib.status Namespace Reference

### Data Structures

- class [Status](#)

### Functions

- def [check\\_status](#) (status, \*args, \*\*kwargs)

### Variables

- dict **STATUS\_EXCEPTION\_MAP**

### 20.11.1 Detailed Description

Status codes and status to exception conversions.

### 20.11.2 Function Documentation

#### 20.11.2.1 check\_status()

```
def cryptoauthlib.status.check_status (
    status,
    * args,
    ** kwargs )
```

Look up the status return code from an API call and raise the exception that matches

## 20.12 cryptoauthlib.tng Namespace Reference

### Functions

- def [tng\\_get\\_device\\_pubkey](#) (public\_key)
- def [tng\\_atcacert\\_max\\_device\\_cert\\_size](#) (max\_cert\_size)
- def [tng\\_atcacert\\_read\\_device\\_cert](#) (cert, cert\_size, signer\_cert=None)
- def [tng\\_atcacert\\_device\\_public\\_key](#) (public\_key, cert=None)
- def [tng\\_atcacert\\_max\\_signer\\_cert\\_size](#) (max\_cert\_size)
- def [tng\\_atcacert\\_read\\_signer\\_cert](#) (cert, cert\_size)
- def [tng\\_atcacert\\_signer\\_public\\_key](#) (public\_key, cert=None)
- def [tng\\_atcacert\\_root\\_cert\\_size](#) (cert\_size)
- def [tng\\_atcacert\\_root\\_cert](#) (cert, cert\_size)
- def [tng\\_atcacert\\_root\\_public\\_key](#) (public\_key)

### 20.12.1 Detailed Description

TNG: classes and functions for interacting with TNG devices

### 20.12.2 Function Documentation

#### 20.12.2.1 tng\_atcacert\_device\_public\_key()

```
def cryptoauthlib.tng.tng_atcacert_device_public_key (
    public_key,
    cert = None )
```

Reads the device public key.

Args:

public_key	Public key will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve. Expects bytearray.
cert	If supplied, the device public key is used from this certificate. If set to None, the device public key is read from the device. Expects bytes or None.

Returns:

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 20.12.2.2 tng\_atcacert\_max\_device\_cert\_size()

```
def cryptoauthlib.tng.tng_atcacert_max_device_cert_size (
    max_cert_size )
```

Return the maximum possible certificate size in bytes for a TNG device certificate. Certificate can be variable size, so this gives an appropriate buffer size when reading the certificate.

Args:

max\_cert\_size Maximum certificate size will be returned here in bytes. Expects AtcaReference.

Returns:

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 20.12.2.3 tng\_atcacert\_max\_signer\_cert\_size()

```
def cryptoauthlib.tng.tng_atcacert_max_signer_cert_size (
    max_cert_size )
```

Return the maximum possible certificate size in bytes for a TNG signer certificate. Certificate can be variable size, so this gives an appropriate buffer size when reading the certificate.

Args:

max\_cert\_size Maximum certificate size will be returned here in bytes. Expects AtcaReference.

Returns:

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 20.12.2.4 tng\_atcacert\_read\_device\_cert()

```
def cryptoauthlib.tng.tng_atcacert_read_device_cert (
    cert,
    cert_size,
    signer_cert = None )
```

Reads the device certificate for a TNG device.

Args:

cert Buffer to received the certificate (DER format). Expects bytearray.  
cert\_size As input, the size of the cert buffer in bytes. As output, the size of the certificate returned in cert in bytes. Expects AtcaReference.  
signer\_cert If supplied, the signer public key is used from this certificate. If set to None, the signer public key is read from the device. Expects bytes or None.

Returns:

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 20.12.2.5 tng\_atcacert\_read\_signer\_cert()

```
def cryptoauthlib.tng.tng_atcacert_read_signer_cert (
    cert,
    cert_size )
```

Reads the signer certificate for a TNG device.

Args:

cert	Buffer to received the certificate (DER format). Expects bytearray.
cert_size	As input, the size of the cert buffer in bytes. As output, the size of the certificate returned in cert in bytes. Expects AtcaReference.

Returns:

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 20.12.2.6 tng\_atcacert\_root\_cert()

```
def cryptoauthlib.tng.tng_atcacert_root_cert (
    cert,
    cert_size )
```

Get the TNG root cert.

Args:

cert	Buffer to received the certificate (DER format). Expects bytearray.
cert_size	As input, the size of the cert buffer in bytes. As output, the size of the certificate returned in cert in bytes. Expects AtcaReference.

Returns:

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 20.12.2.7 tng\_atcacert\_root\_cert\_size()

```
def cryptoauthlib.tng.tng_atcacert_root_cert_size (
    cert_size )
```

Get the size of the TNG root cert.

Args:

cert_size	Certificate size will be returned here in bytes. Expects AtcaReference.
-----------	--

Returns:

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 20.12.2.8 tng\_atcacert\_root\_public\_key()

```
def cryptoauthlib.tng.tng_atcacert_root_public_key (
    public_key )
```

Gets the root public key.

Args:

public\_key Public key will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve. Expects bytearray.

Returns:

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 20.12.2.9 tng\_atcacert\_signer\_public\_key()

```
def cryptoauthlib.tng.tng_atcacert_signer_public_key (
    public_key,
    cert = None )
```

Reads the signer public key.

Args:

public\_key Public key will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve. Expects bytearray.  
cert If supplied, the signer public key is used from this certificate. If set to None, the signer public key is read from the device. Expects bytes or None.

Returns:

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 20.12.2.10 tng\_get\_device\_pubkey()

```
def cryptoauthlib.tng.tng_get_device_pubkey (
    public_key )
```

Uses GenKey command to calculate the public key from the primary device public key.

Args:

public\_key Public key will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve. Expects bytearray.

Returns:

ATCA\_SUCCESS on success, otherwise an error code.

## 20.13 test\_device Namespace Reference

### Functions

- def **test\_device\_config\_size** (config, size)
- def **test\_device\_config\_from\_def** (config, definition, vector)
- def **test\_device\_config\_from\_vector** (config, vector)
- def **test\_device\_serial\_number\_from\_def** (config, definition, vector)

### Variables

- bytearray **ATSHA204A\_SER\_NUM\_VECTOR** = bytearray.fromhex('01 23 6E AA CE FE 0B 8D EE')
- bytearray **ATSHA204A\_DEVICE\_CONFIG\_VECTOR**
- dict **ATSHA204A\_DEVICE\_CONFIG**
- bytearray **ATECC508A\_SER\_NUM\_VECTOR** = bytearray.fromhex('01 23 72 E8 B9 63 B2 D3 EE')
- bytearray **ATECC508A\_DEVICE\_CONFIG\_VECTOR**
- dict **ATECC508A\_DEVICE\_CONFIG**
- bytearray **ATECC608\_SER\_NUM\_VECTOR** = bytearray.fromhex('01 23 72 E8 B9 63 B2 D3 EE')
- bytearray **ATECC608\_DEVICE\_CONFIG\_VECTOR**
- dict **ATECC608\_DEVICE\_CONFIG**
- **id**

### 20.13.1 Detailed Description

Device.py tests. Covers the configuration structures

### 20.13.2 Variable Documentation

#### 20.13.2.1 ATECC508A\_DEVICE\_CONFIG

dict test\_device.ATECC508A\_DEVICE\_CONFIG

##### Initial value:

```
00001 = {
00002     'SN03': [0x01, 0x23, 0x72, 0xE8],
00003     'RevNum': [0x00, 0x00, 0x60, 0x02],
00004     'SN48': [0xB9, 0x63, 0xB2, 0xD3, 0xEE],
00005     'I2C_Enable': 0x2D,
00006     'I2C_Address': 0xB0,
00007     'OTPmode': 0x55,
00008     'SlotConfig': [0x208F, 0x44C4, 0x2087, 0x2087,
00009                   0x0F8F, 0x36C4, 0x0F9F, 0x2082,
00010                   0x0F0F, 0x44C4, 0x0F0F, 0x0F0F,
00011                   0x0F0F, 0x0F0F, 0x0F0F, 0x0F0F],
00012     'Counter0': [0xFF, 0xFF, 0xFF, 0xFF, 0x00, 0x00, 0x00, 0x00],
00013     'Counter1': [0xFF, 0xFF, 0xFF, 0xFF, 0x00, 0x00, 0x00, 0x00],
00014     'LastKeyUse': [0xFF, 0xFF, 0xFF, 0xFF,
00015                  0xFF, 0xFF, 0xFF, 0xFF,
00016                  0xFF, 0xFF, 0xFF, 0xFF,
00017                  0xFF, 0xFF, 0xFF, 0xFF],
00018     'LockValue': 0x55,
00019     'LockConfig': 0x55,
00020     'SlotLocked': 0xFFFF,
00021     'KeyConfig': [0x0033, 0x001C, 0x0013, 0x0013,
00022                  0x007C, 0x001C, 0x003C, 0x0033,
00023                  0x003C, 0x003C, 0x003C, 0x0030,
00024                  0x003C, 0x003C, 0x003C, 0x0030]
00025 }
```

### 20.13.2.2 ATECC508A\_DEVICE\_CONFIG\_VECTOR

```
bytearray test_device.ATECC508A_DEVICE_CONFIG_VECTOR
```

**Initial value:**

```
00001 = bytearray.fromhex(
00002     '01 23 72 E8 00 00 60 02 B9 63 B2 D3 EE 00 2D 00'
00003     'B0 00 55 00 8F 20 C4 44 87 20 87 20 8F 0F C4 36'
00004     '9F 0F 82 20 0F 0F C4 44 0F 0F 0F 0F 0F 0F 0F 0F'
00005     '0F 0F 0F 0F FF FF FF FF 00 00 00 00 FF FF FF FF'
00006     '00 00 00 00 FF FF FF FF FF FF FF FF FF FF FF FF'
00007     'FF FF FF FF 00 00 55 55 FF FF 00 00 00 00 00 00'
00008     '33 00 1C 00 13 00 13 00 7C 00 1C 00 3C 00 33 00'
00009     '3C 00 3C 00 3C 00 30 00 3C 00 3C 00 3C 00 30 00')
```

### 20.13.2.3 ATECC608\_DEVICE\_CONFIG

```
dict test_device.ATECC608_DEVICE_CONFIG
```

**Initial value:**

```
00001 = {
00002     'SN03': [0x01, 0x23, 0x72, 0xE8],
00003     'RevNum': [0x00, 0x00, 0x60, 0x02],
00004     'SN48': [0xB9, 0x63, 0xB2, 0xD3, 0xEE],
00005     'AES_Enable': {'Enable': 1},
00006     'I2C_Enable': 0x2D,
00007     'I2C_Address': 0xB0,
00008     'ChipMode': 1,
00009     'CountMatch': 0x55,
00010     'SlotConfig': [0x208F, 0x44C4, 0x2087, 0x2087,
00011                    0x0F8F, 0x36C4, 0x0F9F, 0x2082,
00012                    0x0F0F, 0x44C4, 0x0F0F, 0x0F0F,
00013                    0x0F0F, 0x0F0F, 0x0F0F, 0x0F0F],
00014     'Counter0': [0xFF, 0xFF, 0xFF, 0xFF, 0x00, 0x00, 0x00, 0x00],
00015     'Counter1': [0xFF, 0xFF, 0xFF, 0xFF, 0x00, 0x00, 0x00, 0x00],
00016     'SlotLocked': 0xFFFF,
00017     'ChipOptions': {
00018         'IoProtectionKeyEnable': 1,
00019         'KdfAesEnable': 1,
00020         'IoProtectionKey': 4
00021     },
00022     'KeyConfig': [0x0033, 0x001C, 0x0013, 0x0013,
00023                  0x007C, 0x001C, 0x003C, 0x0033,
00024                  0x003C, 0x003C, 0x003C, 0x0030,
00025                  0x003C, 0x003C, 0x003C, 0x0030]
00026 }
```

### 20.13.2.4 ATECC608\_DEVICE\_CONFIG\_VECTOR

```
bytearray test_device.ATECC608_DEVICE_CONFIG_VECTOR
```

**Initial value:**

```
00001 = bytearray.fromhex(
00002     '01 23 72 E8 00 00 60 02 B9 63 B2 D3 EE 01 2D 00'
00003     'B0 00 55 01 8F 20 C4 44 87 20 87 20 8F 0F C4 36'
00004     '9F 0F 82 20 0F 0F C4 44 0F 0F 0F 0F 0F 0F 0F 0F'
00005     '0F 0F 0F 0F FF FF FF FF 00 00 00 00 FF FF FF FF'
00006     '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00'
00007     '00 00 00 00 00 00 00 00 FF FF 06 40 00 00 00 00'
00008     '33 00 1C 00 13 00 13 00 7C 00 1C 00 3C 00 33 00'
00009     '3C 00 3C 00 3C 00 30 00 3C 00 3C 00 3C 00 30 00')
```



### 20.13.2.5 ATSHA204A\_DEVICE\_CONFIG

```
dict test_device.ATSHA204A_DEVICE_CONFIG
```

#### Initial value:

```
00001 = {
00002     'SN03': [0x01, 0x23, 0x6E, 0xAA],
00003     'RevNum': [0x00, 0x09, 0x04, 0x00],
00004     'SN48': [0xCE, 0xFE, 0x0B, 0x8D, 0xEE],
00005     'I2C_Enable': 0x01,
00006     'I2C_Address': 0xC8,
00007     'OTPmode': 0x55,
00008     'SlotConfig': [0x808F, 0xA180, 0xE082, 0xF4C4,
00009                     0x0084, 0x85A0, 0x4086, 0x0787,
00010                     0x000F, 0x64C4, 0x7A8A, 0x8B0B,
00011                     0x4C0C, 0x4DDD, 0x42C2, 0x8FAF],
00012     'Counter': [0xFF, 0xFF, 0xFF, 0xFF,
00013                 0xFF, 0xFF, 0xFF, 0xFF],
00014     'LastKeyUse': [0xFF, 0xFF, 0xFF, 0xFF,
00015                    0xFF, 0xFF, 0xFF, 0xFF,
00016                    0xFF, 0xFF, 0xFF, 0xFF,
00017                    0xFF, 0xFF, 0xFF, 0xFF],
00018     'LockValue': 0x55,
00019     'LockConfig': 0x55
00020 }
```

### 20.13.2.6 ATSHA204A\_DEVICE\_CONFIG\_VECTOR

```
bytearray test_device.ATSHA204A_DEVICE_CONFIG_VECTOR
```

#### Initial value:

```
00001 = bytearray.fromhex(
00002     '01 23 6E AA 00 09 04 00 CE FE 0B 8D EE 00 01 00'
00003     'C8 00 55 00 8F 80 80 A1 82 E0 C4 F4 84 00 A0 85'
00004     '86 40 87 07 0F 00 C4 64 8A 7A 0B 8B 0C 4C DD 4D'
00005     'C2 42 AF 8F FF 00 FF 00 FF 00 FF 00 FF 00 FF 00'
00006     'FF 00 FF 00 FF FF FF FF FF FF FF FF FF FF FF'
00007     'FF FF FF FF 00 00 55 55')
```

## 20.14 test\_iface Namespace Reference

### Functions

- def **test\_iface\_init** (test\_init\_with\_lib)
- def **test\_iface\_cfg\_size** (test\_iface\_init)
- def **test\_iface\_cfg\_ateccx08a\_i2c** (test\_iface\_init)
- def **test\_iface\_cfg\_ateccx08a\_swi** (test\_iface\_init)
- def **test\_iface\_cfg\_ateccx08a\_kithid** (test\_iface\_init)
- def **test\_iface\_cfg\_atsha20xa\_i2c** (test\_iface\_init)
- def **test\_iface\_cfg\_atsha20xa\_swi** (test\_iface\_init)
- def **test\_iface\_cfg\_atsha20xa\_kithid** (test\_iface\_init)

### 20.14.1 Detailed Description

These tests verify the structures match the expectation from what is in atca\_cfs.c. If that file has been modified then the tests will fail. If the file has not been modified then we can reasonably expect that there is a problem with the ctypes definition or assumptions of the platform build and memory alignment is wrong.

## Chapter 21

# Data Structure Documentation

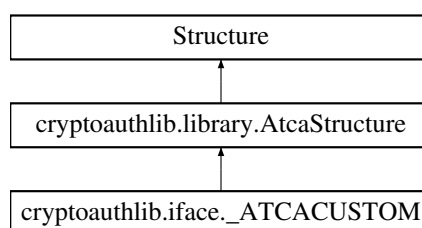
### 21.1 `_ascii_kit_host_context` Struct Reference

#### Data Fields

- const [atca\\_hal\\_kit\\_phy\\_t](#) \* **phy**
- `uint8_t` **buffer** [(2500)]
- [ATCADevice](#) **device**
- [ATCAIfaceCfg](#) \*\* **iface**
- `size_t` **iface\_count**
- `uint32_t` **flags**

### 21.2 `cryptoauthlib.iface._ATCACUSTOM` Class Reference

Inheritance diagram for `cryptoauthlib.iface._ATCACUSTOM`:



#### Static Protected Attributes

- list [\\_fields\\_](#)

## Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.library.AtcaStructure](#)

- None **\_\_init\_\_** (self, \*args, \*\*kwargs)
- def **from\_definition** (cls)
- def **check\_rationality** (cls)
- def **get\_field\_definition** (cls, str name)
- Any **\_\_getattr\_\_** (self, str name)
- def **\_\_iter\_\_** (self)
- def **\_\_str\_\_** (self)
- def **to\_c\_code** (self, name=None, \*\*kwargs)
- def **update\_from\_buffer** (self, buffer)

### 21.2.1 Detailed Description

Custom HAL configuration

### 21.2.2 Field Documentation

#### 21.2.2.1 `_fields_`

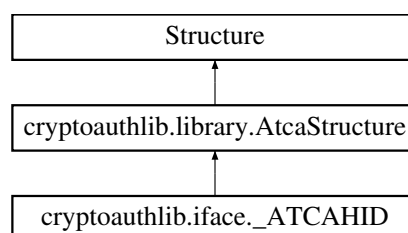
```
list cryptoauthlib.iface._ATCACUSTOM._fields_ [static], [protected]
```

Initial value:

```
= [('halinit', c_void_p),
    ('halpostinit', c_void_p),
    ('halsend', c_void_p),
    ('halreceive', c_void_p),
    ('halwake', c_void_p),
    ('halidle', c_void_p),
    ('halsleep', c_void_p),
    ('halrelease', c_void_p)]
```

## 21.3 `cryptoauthlib.iface._ATCAHID` Class Reference

Inheritance diagram for `cryptoauthlib.iface._ATCAHID`:



### Static Protected Attributes

- dict `_def_`

### Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.library.AtcaStructure](#)

- None `__init__` (self, \*args, \*\*kwargs)
- def `from_definition` (cls)
- def `check_rationality` (cls)
- def `get_field_definition` (cls, str name)
- Any `__getattr__` (self, str name)
- def `__iter__` (self)
- def `__str__` (self)
- def `to_c_code` (self, name=None, \*\*kwargs)
- def `update_from_buffer` (self, buffer)

### 21.3.1 Detailed Description

USB (HID) HAL configuration

### 21.3.2 Field Documentation

#### 21.3.2.1 `_def_`

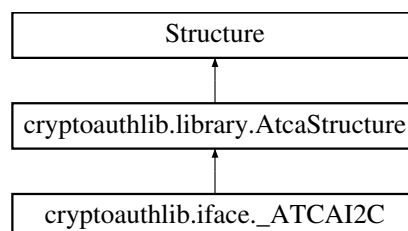
dict `cryptoauthlib.iface._ATCAHID._def_` [static], [protected]

Initial value:

```
= {
    'idx': (c_int,),
    'dev_interface': (ATCAKitType,),
    'dev_identity': (c_uint8,),
    'vid': (c_uint32,),
    'pid': (c_uint32,),
    'packet_size': (c_uint32,)
}
```

## 21.4 cryptoauthlib.iface.\_ATCAI2C Class Reference

Inheritance diagram for `cryptoauthlib.iface._ATCAI2C`:



## Static Protected Attributes

- tuple `_anonymous_` = ('u',)
- dict `_map_`
- list `_fields_`

## Additional Inherited Members

### Public Member Functions inherited from `cryptoauthlib.library.AtcaStructure`

- None `__init__` (self, \*args, \*\*kwargs)
- def `from_definition` (cls)
- def `check_rationality` (cls)
- def `get_field_definition` (cls, str name)
- Any `__getattr__` (self, str name)
- def `__iter__` (self)
- def `__str__` (self)
- def `to_c_code` (self, name=None, \*\*kwargs)
- def `update_from_buffer` (self, buffer)

## 21.4.1 Detailed Description

I2C/TWI HAL configuration

## 21.4.2 Field Documentation

### 21.4.2.1 `_fields_`

```
list cryptoauthlib.iface._ATCAI2C._fields_ [static], [protected]
```

#### Initial value:

```
= [ ('u', _U_Address),
    ('bus', c_uint8),
    ('baud', c_uint32)]
```

### 21.4.2.2 `_map_`

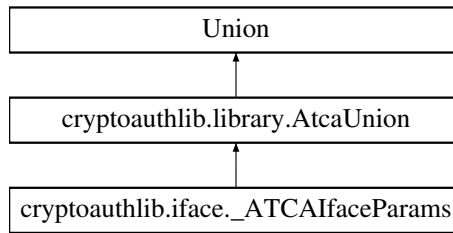
```
dict cryptoauthlib.iface._ATCAI2C._map_ [static], [protected]
```

#### Initial value:

```
= {
    'u': (1,)
}
```

## 21.5 cryptoauthlib.iface.\_ATCAIfaceParams Class Reference

Inheritance diagram for cryptoauthlib.iface.\_ATCAIfaceParams:



### Static Protected Attributes

- list [\\_fields\\_](#)

### Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.library.AtcaUnion](#)

- def `__init__` (self, \*args, \*\*kwargs)
- def [from\\_definition](#) (cls)
- def [check\\_rationality](#) (cls)
- def [get\\_field\\_definition](#) (cls, str name)
- Any `__getattr__` (self, str name)
- def `__iter__` (self)
- def `__str__` (self)
- def [to\\_c\\_code](#) (self, name=None, \*\*kwargs)
- def [update\\_from\\_buffer](#) (self, buffer)

Protected Attributes inherited from [cryptoauthlib.library.AtcaUnion](#)

- `_selected`

### 21.5.1 Detailed Description

HAL Configurations supported by the library (this is a union)

### 21.5.2 Field Documentation

### 21.5.2.1 `_fields_`

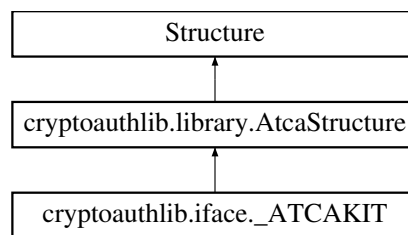
```
list cryptoauthlib.iface._ATCAIfaceParams._fields_ [static], [protected]
```

#### Initial value:

```
= [ ('atcai2c', _ATCAI2C),
    ('atcaswi', _ATCASWI),
    ('atcaspi', _ATCASPI),
    ('atcauart', _ATCAUART),
    ('atcahid', _ATCAHID),
    ('atcakit', _ATCAKIT),
    ('atcacustom', _ATCACUSTOM) ]
```

## 21.6 cryptoauthlib.iface.\_ATCAKIT Class Reference

Inheritance diagram for `cryptoauthlib.iface._ATCAKIT`:



### Static Protected Attributes

- dict `_def_`

### Additional Inherited Members

Public Member Functions inherited from `cryptoauthlib.library.AtcaStructure`

- None `__init__` (self, \*args, \*\*kwargs)
- def `from_definition` (cls)
- def `check_rationality` (cls)
- def `get_field_definition` (cls, str name)
- Any `__getattr__` (self, str name)
- def `__iter__` (self)
- def `__str__` (self)
- def `to_c_code` (self, name=None, \*\*kwargs)
- def `update_from_buffer` (self, buffer)

### 21.6.1 Detailed Description

Kit (Bridge) HAL Configuration

### 21.6.2 Field Documentation

### 21.6.2.1 `_def_`

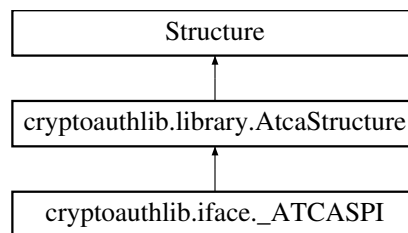
```
dict cryptoauthlib.iface._ATCAKIT._def_ [static], [protected]
```

#### Initial value:

```
= {  
    'dev_interface': (ATCAKitType,),  
    'dev_identity': (c_uint8,),  
    'flags': (c_uint32,)  
}
```

## 21.7 cryptoauthlib.iface.\_ATCASPI Class Reference

Inheritance diagram for `cryptoauthlib.iface._ATCASPI`:



### Static Protected Attributes

- list [\\_fields\\_](#)

### Additional Inherited Members

#### Public Member Functions inherited from [cryptoauthlib.library.AtcaStructure](#)

- None `__init__` (self, \*args, \*\*kwargs)
- def [from\\_definition](#) (cls)
- def [check\\_rationality](#) (cls)
- def [get\\_field\\_definition](#) (cls, str name)
- Any `__getattr__` (self, str name)
- def `__iter__` (self)
- def `__str__` (self)
- def [to\\_c\\_code](#) (self, name=None, \*\*kwargs)
- def [update\\_from\\_buffer](#) (self, buffer)

### 21.7.1 Detailed Description

SPI HAL configuration

### 21.7.2 Field Documentation



### 21.7.2.1 `_fields_`

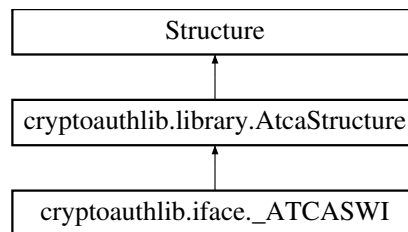
```
list cryptoauthlib.iface._ATCASPI._fields_ [static], [protected]
```

#### Initial value:

```
= [('bus', c_uint8),
    ('select_pin', c_uint8),
    ('baud', c_uint32)]
```

## 21.8 `cryptoauthlib.iface._ATCASWI` Class Reference

Inheritance diagram for `cryptoauthlib.iface._ATCASWI`:



### Static Protected Attributes

- list [\\_fields\\_](#)

### Additional Inherited Members

#### Public Member Functions inherited from [cryptoauthlib.library.AtcaStructure](#)

- None `__init__` (self, \*args, \*\*kwargs)
- def [from\\_definition](#) (cls)
- def [check\\_rationality](#) (cls)
- def [get\\_field\\_definition](#) (cls, str name)
- Any `__getattr__` (self, str name)
- def `__iter__` (self)
- def `__str__` (self)
- def [to\\_c\\_code](#) (self, name=None, \*\*kwargs)
- def [update\\_from\\_buffer](#) (self, buffer)

### 21.8.1 Detailed Description

SWI (Atmel Single Wire Interface) HAL configuration

### 21.8.2 Field Documentation

### 21.8.2.1 `_fields_`

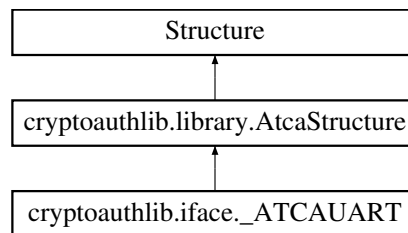
```
list cryptoauthlib.iface._ATCASWI._fields_ [static], [protected]
```

#### Initial value:

```
= [('address', c_uint8),  
    ('bus', c_uint8)]
```

## 21.9 cryptoauthlib.iface.\_ATCAUART Class Reference

Inheritance diagram for cryptoauthlib.iface.\_ATCAUART:



### Static Protected Attributes

- dict `_def_`

### Additional Inherited Members

#### Public Member Functions inherited from [cryptoauthlib.library.AtcaStructure](#)

- None `__init__` (self, \*args, \*\*kwargs)
- def [from\\_definition](#) (cls)
- def [check\\_rationality](#) (cls)
- def [get\\_field\\_definition](#) (cls, str name)
- Any `__getattr__` (self, str name)
- def `__iter__` (self)
- def `__str__` (self)
- def [to\\_c\\_code](#) (self, name=None, \*\*kwargs)
- def [update\\_from\\_buffer](#) (self, buffer)

### 21.9.1 Detailed Description

Generic UART HAL configuration

### 21.9.2 Field Documentation

### 21.9.2.1 `_def_`

```
dict cryptoauthlib.iface._ATCAUART._def_ [static], [protected]
```

#### Initial value:

```
= {
    'dev_interface': (ATCAKitType,),
    'dev_identity': (c_uint8,),
    'port': (c_uint8,),
    'baud': (c_uint32,),
    'wordsize': (c_uint8,),
    'parity': (c_uint8,),
    'stopbits': (c_uint8,)
}
```

## 21.10 `cryptoauthlib.library._CtpeIterator` Class Reference

### Public Member Functions

- None `__init__` (self, obj)
- `def __iter__` (self)
- `def __next__` (self)

### Protected Attributes

- `_obj`
- `_index`
- `_end`

### 21.10.1 Detailed Description

Used to iterate through a ctypes structure or union. This iterator returns a tuple of three elements:

```
<field_name>, <field_contents>, <field_info>
```

Of course `field_info` is a tuple of varying size depending on how the field was defined (arrays, bitfields, etc)

## 21.11 `_kit_host_map_entry` Struct Reference

```
#include <app/kit_host/ascii_kit_host.h>
```

### Data Fields

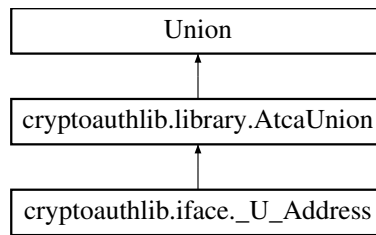
- `const char * id`
- `ATCA_STATUS(* fp_command)(ascii\_kit\_host\_context\_t *ctx, int argc, char *argv[], uint8\_t *response, size\_t *rlen)`

### 21.11.1 Detailed Description

Used to create command tables for the kit host parser

## 21.12 cryptoauthlib.iface.\_U\_Address Class Reference

Inheritance diagram for cryptoauthlib.iface.\_U\_Address:



### Static Protected Attributes

- list [\\_fields\\_](#)

### Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.library.AtcaUnion](#)

- def [\\_\\_init\\_\\_](#) (self, \*args, \*\*kwargs)
- def [from\\_definition](#) (cls)
- def [check\\_rationality](#) (cls)
- def [get\\_field\\_definition](#) (cls, str name)
- Any [\\_\\_getattr\\_\\_](#) (self, str name)
- def [\\_\\_iter\\_\\_](#) (self)
- def [\\_\\_str\\_\\_](#) (self)
- def [to\\_c\\_code](#) (self, name=None, \*\*kwargs)
- def [update\\_from\\_buffer](#) (self, buffer)

Protected Attributes inherited from [cryptoauthlib.library.AtcaUnion](#)

- [\\_selected](#)

### 21.12.1 Detailed Description

Hidden union to provide backward compatibility with the api change

### 21.12.2 Field Documentation

#### 21.12.2.1 [\\_fields\\_](#)

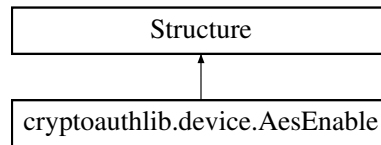
```
list cryptoauthlib.iface._U_Address._fields_ [static], [protected]
```

Initial value:

```
= [ ('slave_address', c_uint8),
    ('address', c_uint8)]
```

## 21.13 cryptauthlib.device.AesEnable Class Reference

Inheritance diagram for cryptauthlib.device.AesEnable:



### Static Protected Attributes

- list [\\_fields\\_](#)
- int [\\_pack\\_](#) = 1

#### 21.13.1 Detailed Description

AES Enable (608) Field Definition

#### 21.13.2 Field Documentation

##### 21.13.2.1 [\\_fields\\_](#)

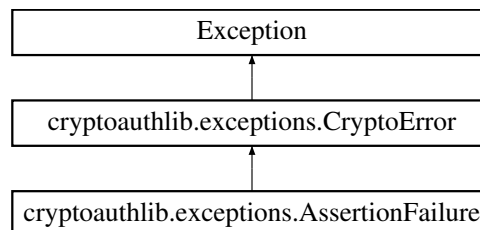
```
list cryptauthlib.device.AesEnable._fields_ [static], [protected]
```

**Initial value:**

```
= [('Enable', c_uint8, 1),
    ('Reserved', c_uint8, 6)]
```

## 21.14 cryptauthlib.exceptions.AssertionFailure Class Reference

Inheritance diagram for cryptauthlib.exceptions.AssertionFailure:

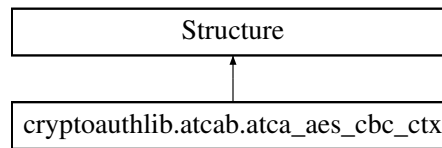


#### 21.14.1 Detailed Description

Code failed run-time consistency check

## 21.15 cryptauthlib.atcab.atca\_aes\_cbc\_ctx Class Reference

Inheritance diagram for cryptauthlib.atcab.atca\_aes\_cbc\_ctx:



### Static Protected Attributes

- list [\\_fields\\_](#)

#### 21.15.1 Detailed Description

AES CBC Context

#### 21.15.2 Field Documentation

##### 21.15.2.1 [\\_fields\\_](#)

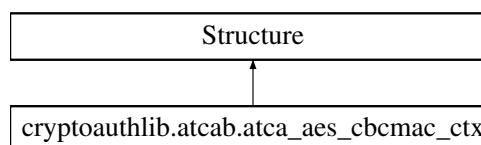
```
list cryptauthlib.atcab.atca_aes_cbc_ctx._fields_ [static], [protected]
```

##### Initial value:

```
= [{"device", c_void_p),
    ("key_id", c_uint16),
    ("key_block", c_uint8),
    ("ciphertext", c_char*16)]
```

## 21.16 cryptauthlib.atcab.atca\_aes\_cbcmac\_ctx Class Reference

Inheritance diagram for cryptauthlib.atcab.atca\_aes\_cbcmac\_ctx:



### Static Protected Attributes

- list [\\_fields\\_](#)

21.16.1 Detailed Description

AES CBCMAC Context

21.16.2 Field Documentation

21.16.2.1 `_fields_`

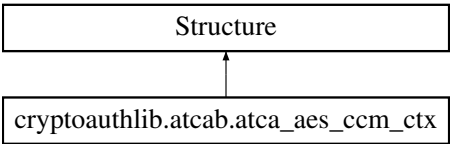
```
list cryptoauthlib.atcab.atca_aes_cbcmac_ctx._fields_ [static], [protected]
```

**Initial value:**

```
= [{"cbc_ctx", atca_aes_cbc_ctx},  
   {"block_size", c_uint8},  
   {"block", c_char*16}]
```

21.17 cryptoauthlib.atcab.atca\_aes\_ccm\_ctx Class Reference

Inheritance diagram for cryptoauthlib.atcab.atca\_aes\_ccm\_ctx:



Static Protected Attributes

- [list `\_fields\_`](#)

21.17.1 Detailed Description

AES CCM Context

21.17.2 Field Documentation

### 21.17.2.1 `_fields_`

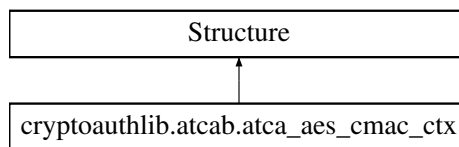
```
list cryptoauthlib.atcab.atca_aes_ccm_ctx._fields_ [static], [protected]
```

#### Initial value:

```
= [{"cbc_mac_ctx", atca_aes_cbc_ctx),  
    ("ctr_ctx", atca_aes_ctr_ctx),  
    ("iv_size", c_uint8),  
    ("M", c_uint8),  
    ("counter", c_char*16),  
    ("partial_aad", c_char*16),  
    ("partial_aad_size", c_uint32),  
    ("text_size", c_uint32),  
    ("enc_cb", c_char*16),  
    ("data_size", c_uint32),  
    ("ciphertext_block", c_char*16)]
```

## 21.18 cryptoauthlib.atcab.atca\_aes\_cmac\_ctx Class Reference

Inheritance diagram for cryptoauthlib.atcab.atca\_aes\_cmac\_ctx:



### Static Protected Attributes

- list [\\_fields\\_](#)

### 21.18.1 Detailed Description

AES CMAC Context

### 21.18.2 Field Documentation

#### 21.18.2.1 `_fields_`

```
list cryptoauthlib.atcab.atca_aes_cmac_ctx._fields_ [static], [protected]
```

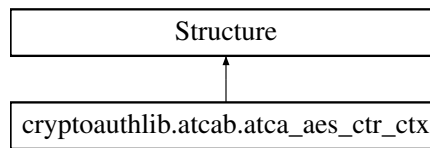
#### Initial value:

```
= [{"cbc_ctx", atca_aes_cbc_ctx),  
    ("block_size", c_uint32),  
    ("block", c_char*16)]
```



## 21.19 cryptauthlib.atcab.atca\_aes\_ctr\_ctx Class Reference

Inheritance diagram for cryptauthlib.atcab.atca\_aes\_ctr\_ctx:



### Static Protected Attributes

- list [\\_fields\\_](#)

### 21.19.1 Detailed Description

AES CTR Context

### 21.19.2 Field Documentation

#### 21.19.2.1 [\\_fields\\_](#)

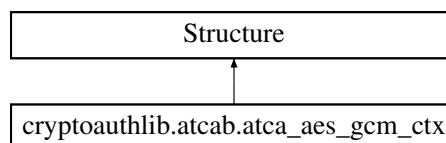
```
list cryptauthlib.atcab.atca_aes_ctr_ctx._fields_ [static], [protected]
```

#### Initial value:

```
= [{"key_id", c_uint16},  
    ("key_block", c_uint8),  
    ("iv", c_char*16),  
    ("counter_size", c_uint8)]
```

## 21.20 cryptauthlib.atcab.atca\_aes\_gcm\_ctx Class Reference

Inheritance diagram for cryptauthlib.atcab.atca\_aes\_gcm\_ctx:



### Static Protected Attributes

- list [\\_fields\\_](#)

### 21.20.1 Detailed Description

Context structure for AES GCM operations

### 21.20.2 Field Documentation

#### 21.20.2.1 \_fields\_

```
list cryptoauthlib.atcab.atca_aes_gcm_ctx._fields_ [static], [protected]
```

**Initial value:**

```
= [{"key_id", c_uint16},
    ("key_block", c_uint8),
    ("cb", c_char*16),
    ("data_size", c_uint32),
    ("aad_size", c_uint32),
    ("h", c_char*16),
    ("j0", c_char*16),
    ("y", c_char*16),
    ("partial_aad", c_char*16),
    ("partial_aad_size", c_uint32),
    ("enc_cb", c_char*16),
    ("ciphertext_block", c_char*16)]
```

## 21.21 atca\_check\_mac\_in\_out Struct Reference

Input/output parameters for function atcah\_check\_mac().

```
#include <lib/host/atca_host.h>
```

### Data Fields

- **uint8\_t mode**  
*[in] CheckMac command Mode*
- **uint16\_t key\_id**  
*[in] CheckMac command KeyID*
- **const uint8\_t \* sn**  
*[in] Device serial number SN[0:8]. Only SN[0:1] and SN[8] are required though.*
- **const uint8\_t \* client\_chal**  
*[in] ClientChal data, 32 bytes. Can be NULL if mode[0] is 1.*
- **uint8\_t \* client\_resp**  
*[out] Calculated ClientResp will be returned here.*
- **const uint8\_t \* other\_data**  
*[in] OtherData, 13 bytes*
- **const uint8\_t \* otp**  
*[in] First 8 bytes of the OTP zone data. Can be NULL is mode[5] is 0.*
- **const uint8\_t \* slot\_key**
- **const uint8\_t \* target\_key**
- **struct atca\_temp\_key \* temp\_key**  
*[in,out] Current state of TempKey. Required if mode[0] or mode[1] are 1.*

### 21.21.1 Detailed Description

Input/output parameters for function `atcah_check_mac()`.

### 21.21.2 Field Documentation

#### 21.21.2.1 `slot_key`

```
const uint8_t* atca_check_mac_in_out::slot_key
```

[in] 32 byte key value in the slot specified by `slot_id`. Can be NULL if `mode[1]` is 1.

#### 21.21.2.2 `target_key`

```
const uint8_t* atca_check_mac_in_out::target_key
```

[in] If this is not NULL, it assumes CheckMac copy is enabled for the specified `key_id` (`ReadKey=0`). If `key_id` is even, this should be the 32-byte key value for the slot `key_id+1`, otherwise this should be set to `slot_key`.

## 21.22 `atca_decrypt_in_out` Struct Reference

Input/output parameters for function `atca_decrypt()`.

```
#include <lib/host/atca_host.h>
```

### Data Fields

- `uint8_t * crypto_data`  
[in,out] Pointer to 32-byte data. Input encrypted data from Read command (Contents field), output decrypted.
- struct `atca_temp_key * temp_key`  
[in,out] Pointer to TempKey structure.

### 21.22.1 Detailed Description

Input/output parameters for function `atca_decrypt()`.

## 21.23 `atca_delete_in_out` Struct Reference

Input/Output paramters for calculating the mac.Used with Delete command.

```
#include <lib/host/atca_host.h>
```

### Data Fields

- uint16\_t **key\_id**
- const uint8\_t \* **sn**
- uint8\_t \* **nonce**
- const uint8\_t \* **key**
- uint8\_t \* **mac**

### 21.23.1 Detailed Description

Input/Output paramters for calculating the mac.Used with Delete command.

## 21.24 atca\_derive\_key\_in\_out Struct Reference

Input/output parameters for function atcah\_derive\_key().

```
#include <lib/host/atca_host.h>
```

### Data Fields

- uint8\_t **mode**  
*Mode (param 1) of the derive key command.*
- uint16\_t **target\_key\_id**  
*Key ID (param 2) of the target slot to run the command on.*
- const uint8\_t \* **sn**  
*Device serial number SN[0:8]. Only SN[0:1] and SN[8] are required though.*
- const uint8\_t \* **parent\_key**  
*Parent key to be used in the derive key calculation (32 bytes).*
- uint8\_t \* **target\_key**  
*Derived key will be returned here (32 bytes).*
- struct [atca\\_temp\\_key](#) \* **temp\_key**  
*Current state of TempKey.*

### 21.24.1 Detailed Description

Input/output parameters for function atcah\_derive\_key().

## 21.25 atca\_derive\_key\_mac\_in\_out Struct Reference

Input/output parameters for function atcah\_derive\_key\_mac().

```
#include <lib/host/atca_host.h>
```

## Data Fields

- `uint8_t mode`  
*Mode (param 1) of the derive key command.*
- `uint16_t target_key_id`  
*Key ID (param 2) of the target slot to run the command on.*
- `const uint8_t * sn`  
*Device serial number SN[0:8]. Only SN[0:1] and SN[8] are required though.*
- `const uint8_t * parent_key`  
*Parent key to be used in the derive key calculation (32 bytes).*
- `uint8_t * mac`  
*DeriveKey MAC will be returned here.*

### 21.25.1 Detailed Description

Input/output parameters for function `atcah_derive_key_mac()`.

## 21.26 atca\_device Struct Reference

[atca\\_device](#) is the C object backing ATCADevice. See the [atca\\_device.h](#) file for details on the ATCADevice methods

```
#include <lib/atca_device.h>
```

## Data Fields

- [atca\\_iface\\_t](#) `mlface`
- `uint8_t` [device\\_state](#)
- `uint8_t` `clock_divider`
- `uint16_t` `execution_time_msec`
- `void *` `session_ctx`
- [ctx\\_cb](#) `session_cb`

### 21.26.1 Detailed Description

[atca\\_device](#) is the C object backing ATCADevice. See the [atca\\_device.h](#) file for details on the ATCADevice methods

### 21.26.2 Field Documentation

#### 21.26.2.1 device\_state

```
uint8_t atca_device::device_state
```

Device Power State

### 21.26.2.2 miface

`atca_iface_t` `atca_device::mIface`

Physical interface

## 21.27 atca\_diversified\_key\_in\_out Struct Reference

Input/output parameters for function `atcah_gendivkey()`.

```
#include <lib/host/atca_host.h>
```

### Data Fields

- `const uint8_t * parent_key`
- `const uint8_t * other_data`
- `const uint8_t * sn`  
*[in] Device serial number SN[0:8]. Only SN[0:1] and SN[8] are required though.*
- `const uint8_t * input_data`
- `struct atca_temp_key * temp_key`  
*[inout] Current state of TempKey*

### 21.27.1 Detailed Description

Input/output parameters for function `atcah_gendivkey()`.

## 21.28 atca\_evp\_ctx Struct Reference

### Data Fields

- `void * ptr`

## 21.29 atca\_gen\_dig\_in\_out Struct Reference

Input/output parameters for function `atcah_gen_dig()`.

```
#include <lib/host/atca_host.h>
```

## Data Fields

- `uint8_t zone`  
*[in] Zone/Param1 for the GenDig command*
- `uint16_t key_id`  
*[in] KeyId/Param2 for the GenDig command*
- `uint16_t slot_conf`  
*[in] Slot config for the GenDig command*
- `uint16_t key_conf`  
*[in] Key config for the GenDig command*
- `uint8_t slot_locked`  
*[in] slot locked for the GenDig command*
- `uint32_t counter`  
*[in] counter for the GenDig command*
- `bool is_key_nomac`  
*[in] Set to true if the slot pointed to be key\_id has the SotConfig.NoMac bit set*
- `const uint8_t * sn`  
*[in] Device serial number SN[0:8]. Only SN[0:1] and SN[8] are required though.*
- `const uint8_t * stored_value`  
*[in] 32-byte slot value, config block, OTP block as specified by the Zone/KeyId parameters*
- `const uint8_t * other_data`  
*[in] 32-byte value for shared nonce zone, 4-byte value if is\_key\_nomac is true, ignored and/or NULL otherwise*
- `struct atca_temp_key * temp_key`  
*[inout] Current state of TempKey*

### 21.29.1 Detailed Description

Input/output parameters for function `atcah_gen_dig()`.

## 21.30 atca\_gen\_key\_in\_out Struct Reference

Input/output parameters for calculating the PubKey digest put into TempKey by the GenKey command with the `atcah_gen_key_msg()` function.

```
#include <lib/host/atca_host.h>
```

## Data Fields

- `uint8_t mode`  
*[in] GenKey Mode*
- `uint16_t key_id`  
*[in] GenKey KeyID*
- `const uint8_t * public_key`  
*[in] Public key to be used in the PubKey digest. X and Y integers in big-endian format. 64 bytes for P256 curve.*
- `size_t public_key_size`  
*[in] Total number of bytes in the public key. 64 bytes for P256 curve.*
- `const uint8_t * other_data`  
*[in] 3 bytes required when bit 4 of the mode is set. Can be NULL otherwise.*
- `const uint8_t * sn`  
*[in] Device serial number SN[0:8] (9 bytes). Only SN[0:1] and SN[8] are required though.*
- `struct atca_temp_key * temp_key`  
*[in,out] As input the current state of TempKey. As output, the resulting PubKey digest.*

### 21.30.1 Detailed Description

Input/output parameters for calculating the PubKey digest put into TempKey by the GenKey command with the atcah\_gen\_key\_msg() function.

## 21.31 atca\_hal\_kit\_phy\_t Struct Reference

### Data Fields

- ATCA\_STATUS(\* [send](#))(void \*ctx, uint8\_t \*txdata, uint16\_t txlen)
- ATCA\_STATUS(\* [recv](#))(void \*ctx, uint8\_t \*rxdata, uint16\_t \*rxlen)
- void (\* [packet\\_alloc](#))(size\_t bytes)
- void(\* [packet\\_free](#))(void \*packet)
- void \* [hal\\_data](#)

### 21.31.1 Field Documentation

#### 21.31.1.1 hal\_data

```
void* atca_hal_kit_phy_t::hal_data
```

Physical layer context

#### 21.31.1.2 packet\_alloc

```
void (* atca_hal_kit_phy_t::packet_alloc) (size_t bytes)
```

Allocate a phy packet

#### 21.31.1.3 packet\_free

```
void(* atca_hal_kit_phy_t::packet_free) (void *packet)
```

Free a phy packet

#### 21.31.1.4 recv

```
ATCA_STATUS(* atca_hal_kit_phy_t::recv) (void *ctx, uint8_t *rxdata, uint16_t *rxlen)
```

Must be a blocking receive



### 21.31.1.5 send

```
ATCA_STATUS(* atca_hal_kit_phy_t::send) (void *ctx, uint8_t *txdata, uint16_t txlen)
```

Must be a blocking send

## 21.32 atca\_hal\_list\_entry\_t Struct Reference

Structure that holds the hal/phy mapping for different interface types.

### Data Fields

- `uint8_t iface_type`
- `ATCAHAL_t * hal`
- `ATCAHAL_t * phy`

### 21.32.1 Detailed Description

Structure that holds the hal/phy mapping for different interface types.

### 21.32.2 Field Documentation

#### 21.32.2.1 phy

```
ATCAHAL_t* atca_hal_list_entry_t::phy
```

Physical interface for the specific HAL

## 21.33 atca\_hal\_shm\_t Struct Reference

### Data Fields

- `int recordedPID`
- `uint8_t sessionID`
- `uint8_t index`

## 21.34 atca\_hmac\_in\_out Struct Reference

Input/output parameters for function `atca_hmac()`.

```
#include <lib/host/atca_host.h>
```

## Data Fields

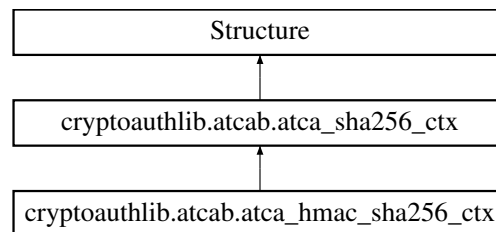
- `uint8_t mode`  
*[in] Mode parameter used in HMAC command (Param1).*
- `uint16_t key_id`  
*[in] KeyID parameter used in HMAC command (Param2).*
- `const uint8_t * key`  
*[in] Pointer to 32-byte key used to generate HMAC digest.*
- `const uint8_t * otp`  
*[in] Pointer to 11-byte OTP, optionally included in HMAC digest, depending on mode.*
- `const uint8_t * sn`  
*[in] Pointer to 9-byte SN, optionally included in HMAC digest, depending on mode.*
- `uint8_t * response`  
*[out] Pointer to 32-byte SHA-256 HMAC digest.*
- `struct atca\_temp\_key * temp_key`  
*[in,out] Pointer to TempKey structure.*

### 21.34.1 Detailed Description

Input/output parameters for function `atca_hmac()`.

## 21.35 cryptoauthlib.atcab.atca\_hmac\_sha256\_ctx Class Reference

Inheritance diagram for `cryptoauthlib.atcab.atca_hmac_sha256_ctx`:



## Additional Inherited Members

Static Protected Attributes inherited from `cryptoauthlib.atcab.atca\_sha256\_ctx`

- `list \_fields\_`

### 21.35.1 Detailed Description

HMAC-SHA256 context

## 21.36 atca\_i2c\_host\_s Struct Reference

### Data Fields

- char **i2c\_file** [16]
- int **ref\_ct**

## 21.37 atca\_iface Struct Reference

[atca\\_iface](#) is the context structure for a configured interface

```
#include <lib/atca_iface.h>
```

### Data Fields

- [ATCAIfaceCfg](#) \* **mIfaceCFG**
- [ATCAHAL\\_t](#) \* **hal**
- [ATCAHAL\\_t](#) \* **phy**
- void \* **hal\_data**

### 21.37.1 Detailed Description

[atca\\_iface](#) is the context structure for a configured interface

### 21.37.2 Field Documentation

#### 21.37.2.1 hal

```
ATCAHAL\_t* atca_iface::hal
```

The configured HAL for the interface

#### 21.37.2.2 hal\_data

```
void* atca_iface::hal_data
```

Pointer to HAL specific context/data

#### 21.37.2.3 mIfaceCFG

```
ATCAIfaceCfg* atca_iface::mIfaceCFG
```

Points to previous defined/given Cfg object, the caller manages this

### 21.37.2.4 phy

`ATCAHAL_t* atca_iface::phy`

When a HAL is not a "native" hal it needs a physical layer to be associated with it

## 21.38 atca\_include\_data\_in\_out Struct Reference

Input / output parameters for function `atca_include_data()`.

```
#include <lib/host/atca_host.h>
```

### Data Fields

- `uint8_t * p_temp`  
*[out] pointer to output buffer*
- `const uint8_t * otp`  
*[in] pointer to one-time-programming data*
- `const uint8_t * sn`  
*[in] pointer to serial number data*
- `uint8_t mode`

### 21.38.1 Detailed Description

Input / output parameters for function `atca_include_data()`.

## 21.39 atca\_io\_decrypt\_in\_out Struct Reference

### Data Fields

- `const uint8_t * io_key`  
*IO protection key (32 bytes).*
- `const uint8_t * out_nonce`  
*OutNonce returned from command (32 bytes).*
- `uint8_t * data`  
*As input, encrypted data. As output, decrypted data.*
- `size_t data_size`  
*Size of data in bytes (32 or 64).*

## 21.40 atca\_mac\_in\_out Struct Reference

Input/output parameters for function `atca_mac()`.

```
#include <lib/host/atca_host.h>
```

## Data Fields

- `uint8_t mode`  
*[in] Mode parameter used in MAC command (Param1).*
- `uint16_t key_id`  
*[in] KeyID parameter used in MAC command (Param2).*
- `const uint8_t * challenge`  
*[in] Pointer to 32-byte Challenge data used in MAC command, depending on mode.*
- `const uint8_t * key`  
*[in] Pointer to 32-byte key used to generate MAC digest.*
- `const uint8_t * otp`  
*[in] Pointer to 11-byte OTP, optionally included in MAC digest, depending on mode.*
- `const uint8_t * sn`  
*[in] Pointer to 9-byte SN, optionally included in MAC digest, depending on mode.*
- `uint8_t * response`  
*[out] Pointer to 32-byte SHA-256 digest (MAC).*
- `struct atca\_temp\_key * temp_key`  
*[in,out] Pointer to TempKey structure.*

### 21.40.1 Detailed Description

Input/output parameters for function `atca_mac()`.

## 21.41 `atca_mbedtls_eckey_s` Struct Reference

```
#include <lib/mbedtls/atca_mbedtls_wrap.h>
```

## Data Fields

- `ATCADevice device`
- `uint16_t handle`

### 21.41.1 Detailed Description

Structure to hold metadata - is written into the mbedtls pk structure as the private key bignum value 'd' which otherwise would be unused. Bignums can be any arbitrary length of bytes

## 21.42 `atca_nonce_in_out` Struct Reference

Input/output parameters for function `atca_nonce()`.

```
#include <lib/host/atca_host.h>
```

### Data Fields

- `uint8_t mode`  
*[in] Mode parameter used in Nonce command (Param1).*
- `uint16_t zero`  
*[in] Zero parameter used in Nonce command (Param2).*
- `const uint8_t * num_in`  
*[in] Pointer to 20-byte NumIn data used in Nonce command.*
- `const uint8_t * rand_out`  
*[in] Pointer to 32-byte RandOut data from Nonce command.*
- `struct atca_temp_key * temp_key`  
*[in,out] Pointer to TempKey structure.*

### 21.42.1 Detailed Description

Input/output parameters for function `atca_nonce()`.

## 21.43 atca\_plib\_i2c\_api Struct Reference

### Data Fields

- `atca_i2c_plib_read read`
- `atca_i2c_plib_write write`
- `atca_i2c_plib_is_busy is_busy`
- `atca_i2c_error_get error_get`
- `atca_i2c_plib_transfer_setup transfer_setup`

## 21.44 atca\_resp\_mac\_in\_out Struct Reference

Input/Output parameters for calculating the output response mac in SHA105 device. Used with the `atcah_gen_↔ output_resp_mac()` function.

```
#include <lib/host/atca_host.h>
```

### Data Fields

- `const uint8_t * slot_key`
- `uint8_t mode`
- `uint16_t key_id`
- `const uint8_t * sn`
- `uint8_t * client_resp`
- `uint8_t checkmac_result`
- `uint8_t * mac_output`

### 21.44.1 Detailed Description

Input/Output parameters for calculating the output response mac in SHA105 device. Used with the `atcah_gen_output_resp_mac()` function.

## 21.45 atca\_secureboot\_enc\_in\_out Struct Reference

### Data Fields

- `const uint8_t * io_key`  
*IO protection key value (32 bytes)*
- `const struct atca_temp_key * temp_key`  
*Current value of TempKey.*
- `const uint8_t * digest`  
*Plaintext digest as input.*
- `uint8_t * hashed_key`  
*Calculated key is returned here (32 bytes)*
- `uint8_t * digest_enc`  
*Encrypted (ciphertext) digest is return here (32 bytes)*

## 21.46 atca\_secureboot\_mac\_in\_out Struct Reference

### Data Fields

- `uint8_t mode`  
*SecureBoot mode (param1)*
- `uint16_t param2`  
*SecureBoot param2.*
- `uint16_t secure_boot_config`  
*SecureBootConfig value from configuration zone.*
- `const uint8_t * hashed_key`  
*Hashed key. SHA256(IO Protection Key | TempKey)*
- `const uint8_t * digest`  
*Digest (unencrypted)*
- `const uint8_t * signature`  
*Signature (can be NULL if not required)*
- `uint8_t * mac`  
*MAC is returned here.*

## 21.47 atca\_session\_key\_in\_out Struct Reference

Input/Output paramters for calculating the session key by the nonce command. Used with the `atcah_gen_session_key()` function.

```
#include <lib/host/atca_host.h>
```

## Data Fields

- `uint8_t * transport_key`
- `uint16_t transport_key_id`
- `const uint8_t * sn`
- `uint8_t * nonce`
- `uint8_t * session_key`

### 21.47.1 Detailed Description

Input/Output paramters for calculating the session key by the nonce command. Used with the `atcah_gen_session_key()` function.

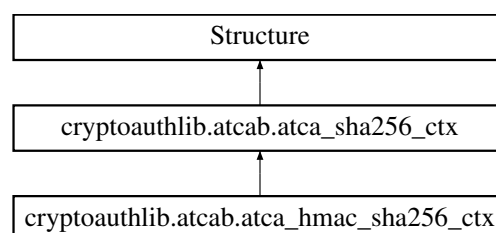
## 21.48 atca\_sha256\_ctx Struct Reference

## Data Fields

- `uint32_t total_msg_size`  
*Total number of message bytes processed.*
- `uint32_t block_size`  
*Number of bytes in current block.*
- `uint8_t block [ATCA_SHA256_BLOCK_SIZE * 2]`  
*Unprocessed message storage.*

## 21.49 cryptoauthlib.atcab.atca\_sha256\_ctx Class Reference

Inheritance diagram for `cryptoauthlib.atcab.atca_sha256_ctx`:



## Static Protected Attributes

- `list_fields_`

### 21.49.1 Detailed Description

SHA256 context



## 21.49.2 Field Documentation

### 21.49.2.1 `_fields_`

```
list cryptoauthlib.atcab.atca_sha256_ctx._fields_ [static], [protected]
```

#### Initial value:

```
= [{"total_msg_size", c_uint32},
    {"block_size", c_uint32},
    {"block", c_char*64*2}]
```

## 21.50 `atca_sign_internal_in_out` Struct Reference

Input/output parameters for calculating the message and digest used by the `Sign(internal)` command. Used with the `atcah_sign_internal_msg()` function.

```
#include <lib/host/atca_host.h>
```

### Data Fields

- `uint8_t mode`  
*[in] Sign Mode*
- `uint16_t key_id`  
*[in] Sign KeyID*
- `uint16_t slot_config`  
*[in] SlotConfig[TempKeyFlags.keyId]*
- `uint16_t key_config`  
*[in] KeyConfig[TempKeyFlags.keyId]*
- `uint8_t use_flag`  
*[in] UseFlag[TempKeyFlags.keyId], 0x00 for slots 8 and above and for ATECC508A*
- `uint8_t update_count`  
*[in] UpdateCount[TempKeyFlags.keyId], 0x00 for slots 8 and above and for ATECC508A*
- `bool is_slot_locked`  
*[in] Is TempKeyFlags.keyId slot locked.*
- `bool for_invalidate`  
*[in] Set to true if this will be used for the Verify(Invalidate) command.*
- `const uint8_t * sn`  
*[in] Device serial number SN[0:8] (9 bytes)*
- `const struct atca_temp_key * temp_key`  
*[in] The current state of TempKey.*
- `uint8_t * message`  
*[out] Full 55 byte message the Sign(internal) command will build. Can be NULL if not required.*
- `uint8_t * verify_other_data`  
*[out] The 19 byte OtherData bytes to be used with the Verify(In/Validate) command. Can be NULL if not required.*
- `uint8_t * digest`  
*[out] SHA256 digest of the full 55 byte message. Can be NULL if not required.*

### 21.50.1 Detailed Description

Input/output parameters for calculating the message and digest used by the Sign(internal) command. Used with the atcah\_sign\_internal\_msg() function.

## 21.51 atca\_spi\_host\_s Struct Reference

### Data Fields

- char **spi\_file** [20]
- int **f\_spi**

## 21.52 atca\_temp\_key Struct Reference

Structure to hold TempKey fields.

```
#include <lib/host/atca_host.h>
```

### Data Fields

- uint8\_t **value** [ATCA\_KEY\_SIZE \*2]  
*Value of TempKey (64 bytes for ATECC608 only)*
- unsigned **key\_id**: 4  
*If TempKey was derived from a slot or transport key (GenDig or GenKey), that key ID is saved here.*
- unsigned **source\_flag**: 1  
*Indicates id TempKey started from a random nonce (0) or not (1).*
- unsigned **gen\_dig\_data**: 1  
*TempKey was derived from the GenDig command.*
- unsigned **gen\_key\_data**: 1  
*TempKey was derived from the GenKey command (ATECC devices only).*
- unsigned **no\_mac\_flag**: 1  
*TempKey was derived from a key that has the NoMac bit set preventing the use of the MAC command. Known as CheckFlag in ATSHA devices).*
- unsigned **valid**: 1  
*TempKey is valid.*
- uint8\_t **is\_64**  
*TempKey has 64 bytes of valid data.*

### 21.52.1 Detailed Description

Structure to hold TempKey fields.

## 21.53 atca\_uart\_host\_s Struct Reference

### Data Fields

- char **uart\_file** [20]
- int **fd\_uart**
- int **ref\_ct**
- HANDLE **hSerial**

## 21.54 atca\_verify\_in\_out Struct Reference

Input/output parameters for function atcah\_verify().

```
#include <lib/host/atca_host.h>
```

### Data Fields

- uint16\_t **curve\_type**  
*[in] Curve type used in Verify command (Param2).*
- const uint8\_t \* **signature**  
*[in] Pointer to ECDSA signature to be verified*
- const uint8\_t \* **public\_key**  
*[in] Pointer to the public key to be used for verification*
- struct [atca\\_temp\\_key](#) \* **temp\_key**  
*[in,out] Pointer to TempKey structure.*

### 21.54.1 Detailed Description

Input/output parameters for function atcah\_verify().

## 21.55 atca\_verify\_mac Struct Reference

### Data Fields

- uint8\_t **mode**  
*Mode (Param1) parameter used in Verify command.*
- uint16\_t **key\_id**  
*KeyID (Param2) used in Verify command.*
- const uint8\_t \* **signature**  
*Signature used in Verify command (64 bytes).*
- const uint8\_t \* **other\_data**  
*OtherData used in Verify command (19 bytes).*
- const uint8\_t \* **msg\_dig\_buf**  
*Message digest buffer (64 bytes).*
- const uint8\_t \* **io\_key**  
*IO protection key value (32 bytes).*
- const uint8\_t \* **sn**  
*Serial number (9 bytes).*
- const [atca\\_temp\\_key\\_t](#) \* **temp\_key**  
*TempKey.*
- uint8\_t \* **mac**  
*Calculated verification MAC is returned here (32 bytes).*

## 21.56 atca\_write\_mac\_in\_out Struct Reference

Input/output parameters for function atcah\_write\_auth\_mac() and atcah\_privwrite\_auth\_mac().

```
#include <lib/host/atca_host.h>
```

### Data Fields

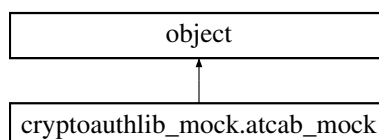
- `uint8_t zone`  
*Zone/Param1 for the Write or PrivWrite command.*
- `uint16_t key_id`  
*KeyID/Param2 for the Write or PrivWrite command.*
- `const uint8_t * sn`  
*Device serial number SN[0:8]. Only SN[0:1] and SN[8] are required though.*
- `const uint8_t * input_data`  
*Data to be encrypted. 32 bytes for Write command, 36 bytes for PrivWrite command.*
- `uint8_t * encrypted_data`  
*Encrypted version of input\_data will be returned here. 32 bytes for Write command, 36 bytes for PrivWrite command.*
- `uint8_t * auth_mac`  
*Write MAC will be returned here. 32 bytes.*
- `struct atca_temp_key * temp_key`  
*Current state of TempKey.*

### 21.56.1 Detailed Description

Input/output parameters for function atcah\_write\_auth\_mac() and atcah\_privwrite\_auth\_mac().

## 21.57 cryptoauthlib\_mock.atcab\_mock Class Reference

Inheritance diagram for cryptoauthlib\_mock.atcab\_mock:



## Public Member Functions

- def **atcab\_init** (self)
- def **atcab\_release** (self)
- def **atcab\_get\_device\_type** (self)
- def **atcab\_aes** (self, mode, key\_id, aes\_in, aes\_out)
- def **atcab\_aes\_encrypt** (self, key\_id, key\_block, plaintext, ciphertext)
- def **atcab\_aes\_decrypt** (self, key\_id, key\_block, ciphertext, plaintext)
- def **atcab\_aes\_gfm** (self, hash\_key, inp, output)
- def **atcab\_aes\_cbc\_init** (self, ctx, key\_id, key\_block, iv)
- def **atcab\_aes\_cbc\_encrypt\_block** (self, ctx, plaintext, ciphertext)
- def **atcab\_aes\_cbc\_decrypt\_block** (self, ctx, ciphertext, plaintext)
- def **atcab\_aes\_cmac\_init** (self, ctx, key\_id, key\_block)
- def **atcab\_aes\_cmac\_update** (self, ctx, data, data\_size)
- def **atcab\_aes\_cmac\_finish** (self, ctx, cmac, size)
- def **atcab\_aes\_ctr\_init** (self, ctx, key\_id, key\_block, counter\_size, iv)
- def **atcab\_aes\_ctr\_init\_rand** (self, ctx, key\_id, key\_block, counter\_size, iv)
- def **atcab\_aes\_ctr\_encrypt\_block** (self, ctx, plaintext, ciphertext)
- def **atcab\_aes\_ctr\_decrypt\_block** (self, ctx, ciphertext, plaintext)
- def **atcab\_aes\_gcm\_init** (self, ctx, key\_id, key\_block, iv, iv\_size)
- def **atcab\_aes\_gcm\_init\_rand** (self, ctx, key\_id, key\_block, rand\_size, free\_field, free\_field\_size, iv)
- def **atcab\_aes\_gcm\_aad\_update** (self, ctx, aad, aad\_size)
- def **atcab\_aes\_gcm\_encrypt\_update** (self, ctx, plaintext, plaintext\_size, ciphertext)
- def **atcab\_aes\_gcm\_encrypt\_finish** (self, ctx, tag, tag\_size)
- def **atcab\_aes\_gcm\_decrypt\_update** (self, ctx, ciphertext, ciphertext\_size, plaintext)
- def **atcab\_aes\_gcm\_decrypt\_finish** (self, ctx, tag, tag\_size, is\_verified)
- def **atcab\_aes\_cbcmac\_init** (self, ctx, key\_id, key\_block)
- def **atcab\_aes\_cbcmac\_update** (self, ctx, data, data\_size)
- def **atcab\_aes\_cbcmac\_finish** (self, ctx, mac, mac\_size)
- def **atcab\_aes\_ccm\_init** (self, ctx, key\_id, key\_block, iv, iv\_size, aad\_size, text\_size, tag\_size)
- def **atcab\_aes\_ccm\_init\_rand** (self, ctx, key\_id, key\_block, iv, iv\_size, aad\_size, text\_size, tag\_size)
- def **atcab\_aes\_ccm\_aad\_update** (self, ctx, aad, aad\_size)
- def **atcab\_aes\_ccm\_aad\_finish** (self, ctx)
- def **atcab\_aes\_ccm\_encrypt\_update** (self, ctx, plaintext, plaintext\_size, ciphertext)
- def **atcab\_aes\_ccm\_decrypt\_update** (self, ctx, ciphertext, ciphertext\_size, plaintext)
- def **atcab\_aes\_ccm\_encrypt\_finish** (self, ctx, tag, tag\_size)
- def **atcab\_aes\_ccm\_decrypt\_finish** (self, ctx, tag, is\_verified)
- def **atcab\_checkmac** (self, mode, key\_id, challenge, response, other\_data)
- def **atcab\_counter** (self, mode, counter\_id, counter\_value)
- def **atcab\_counter\_increment** (self, counter\_id, counter\_value)
- def **atcab\_counter\_read** (self, counter\_id, counter\_value)
- def **atcab\_derivekey** (self, mode, target\_key, mac)
- def **atcab\_ecdh\_base** (self, mode, key\_id, public\_key, pms, out\_nonce)
- def **atcab\_ecdh** (self, key\_id, public\_key, pms)
- def **atcab\_ecdh\_enc** (self, key\_id, public\_key, pms, read\_key, read\_key\_id, num\_in)
- def **atcab\_ecdh\_ioenc** (self, key\_id, public\_key, pms, io\_key)
- def **atcab\_ecdh\_tempkey** (self, public\_key, pms)
- def **atcab\_ecdh\_tempkey\_ioenc** (self, public\_key, pms, io\_key)
- def **atcab\_gendig** (self, zone, key\_id, other\_data, other\_data\_size)
- def **atcab\_genkey\_base** (self, mode, key\_id, other\_data, public\_key)
- def **atcab\_genkey** (self, key\_id, public\_key)
- def **atcab\_get\_pubkey** (self, key\_id, public\_key)
- def **atcab\_hmac** (self, mode, key\_id, digest)
- def **atcab\_info\_base** (self, mode, param2, out\_data)
- def **atcab\_info** (self, revision)

- def **atcab\_info\_get\_latch** (self, state)
- def **atcab\_info\_set\_latch** (self, state)
- def **atcab\_kdf** (self, mode, key\_id, details, message, out\_data, out\_nonce)
- def **atcab\_lock** (self, mode, summary\_crc)
- def **atcab\_lock\_config\_zone** (self)
- def **atcab\_lock\_config\_zone\_crc** (self, summary\_crc)
- def **atcab\_lock\_data\_zone** (self)
- def **atcab\_lock\_data\_zone\_crc** (self, summary\_crc)
- def **atcab\_lock\_data\_slot** (self, slot)
- def **atcab\_mac** (self, mode, key\_id, challenge, digest)
- def **atcab\_nonce\_base** (self, mode, zero, num\_in, rand\_out)
- def **atcab\_nonce** (self, num\_in)
- def **atcab\_nonce\_load** (self, target, num\_in, num\_in\_size)
- def **atcab\_nonce\_rand** (self, num\_in, rand\_out)
- def **atcab\_challenge** (self, num\_in)
- def **atcab\_challenge\_seed\_update** (self, num\_in, rand\_out)
- def **atcab\_priv\_write** (self, key\_id, priv\_key, write\_key\_id, write\_key, num\_in)
- def **atcab\_random** (self, random\_number)
- def **atcab\_read\_zone** (self, zone, slot, block, offset, data, length)
- def **atcab\_read\_serial\_number** (self, serial\_number)
- def **atcab\_is\_slot\_locked** (self, slot, is\_locked)
- def **atcab\_is\_locked** (self, zone, is\_locked)
- def **atcab\_read\_enc** (self, key\_id, block, data, enc\_key, enc\_key\_id, num\_in)
- def **atcab\_read\_config\_zone** (self, config\_data)
- def **atcab\_cmp\_config\_zone** (self, config\_data, same\_config)
- def **atcab\_read\_sig** (self, slot, sig)
- def **atcab\_read\_pubkey** (self, slot, public\_key)
- def **atcab\_read\_bytes\_zone** (self, zone, slot, offset, data, length)
- def **atcab\_secureboot** (self, mode, param2, digest, signature, mac)
- def **atcab\_secureboot\_mac** (self, mode, digest, signature, num\_in, io\_keys, is\_verified)
- def **atcab\_selftest** (self, mode, param2, result)
- def **atcab\_sha\_base** (self, mode, length, message, data\_out, data\_out\_size)
- def **atcab\_sha\_start** (self)
- def **atcab\_sha\_update** (self, message)
- def **atcab\_sha\_end** (self, digest, length, message)
- def **atcab\_sha\_read\_context** (self, context, context\_size)
- def **atcab\_sha\_write\_context** (self, context, context\_size)
- def **atcab\_sha** (self, length, message, digest)
- def **atcab\_hw\_sha2\_256\_init** (self, ctx)
- def **atcab\_hw\_sha2\_256\_update** (self, ctx, data, data\_size)
- def **atcab\_hw\_sha2\_256\_finish** (self, ctx, digest)
- def **atcab\_hw\_sha2\_256** (self, data, data\_size, digest)
- def **atcab\_sha\_hmac\_init** (self, ctx, key\_slot)
- def **atcab\_sha\_hmac\_update** (self, ctx, data, data\_size)
- def **atcab\_sha\_hmac\_finish** (self, ctx, digest, target)
- def **atcab\_sha\_hmac** (self, data, data\_size, key\_slot, digest, target)
- def **atcab\_sign\_base** (self, mode, key\_id, signature)
- def **atcab\_sign** (self, key\_id, msg, signature)
- def **atcab\_sign\_internal** (self, key\_id, is\_invalidate, is\_full\_sn, signature)
- def **atcab\_updateextra** (self, mode, new\_value)
- def **atcab\_verify** (self, mode, key\_id, signature, public\_key, other\_data, mac)
- def **atcab\_verify\_extern\_stored\_mac** (self, mode, key\_id, message, signature, public\_key, num\_in, io\_key, is\_verified)
- def **atcab\_verify\_extern** (self, message, signature, public\_key, is\_verified)
- def **atcab\_verify\_extern\_mac** (self, message, signature, public\_key, num\_in, io\_key, is\_verified)

- def **atcab\_verify\_stored** (self, message, signature, key\_id, is\_verified)
- def **atcab\_verify\_stored\_mac** (self, message, signature, key\_id, num\_in, io\_key, is\_verified)
- def **atcab\_verify\_validate** (self, key\_id, signature, other\_data, is\_verified)
- def **atcab\_verify\_invalidate** (self, key\_id, signature, other\_data, is\_verified)
- def **atcab\_write** (self, zone, [address](#), value, mac)
- def **atcab\_write\_zone** (self, zone, slot, block, offset, data, length)
- def **atcab\_write\_enc** (self, key\_id, block, data, enc\_key, enc\_key\_id, num\_in)
- def **atcab\_write\_config\_zone** (self, conf)
- def **atcab\_write\_pubkey** (self, slot, public\_key)
- def **atcab\_write\_bytes\_zone** (self, zone, slot, offset\_bytes, data, length)
- def **atcab\_write\_config\_counter** (self, counter\_id, counter\_value)
- def **atcacert\_get\_response** (self, device\_private\_key\_slot, challenge, response)
- def **atcacert\_read\_cert** (self, cert\_def, ca\_public\_key, cert, cert\_size)
- def **atcacert\_write\_cert** (self, cert\_def, cert, cert\_size)
- def **atcacert\_create\_csr** (self, csr\_def, csr, csr\_size)
- def **atcacert\_create\_csr\_pem** (self, csr\_def, csr, csr\_size)
- def **atcacert\_date\_enc** (self, format, timestamp, formatted\_date, formatted\_date\_size)
- def **atcacert\_date\_dec** (self, format, formatted\_date, formatted\_date\_size, timestamp)
- def **atcacert\_date\_enc\_compcert** (self, issue\_date, expire\_years, enc\_dates)
- def **atcacert\_date\_dec\_compcert** (self, enc\_dates, expire\_date\_format, issue\_date, expire\_date)
- def **atcacert\_date\_get\_max\_date** (self, date\_format, timestamp)
- def **atcacert\_max\_cert\_size** (self, cert\_def, max\_cert\_size)
- def **tng\_get\_device\_pubkey** (self, public\_key)
- def **tng\_atcacert\_max\_device\_cert\_size** (self, max\_cert\_size)
- def **tng\_atcacert\_read\_device\_cert** (self, cert, cert\_size, signer\_cert)
- def **tng\_atcacert\_device\_public\_key** (self, public\_key, cert)
- def **tng\_atcacert\_max\_signer\_cert\_size** (self, max\_cert\_size)
- def **tng\_atcacert\_read\_signer\_cert** (self, cert, cert\_size)
- def **tng\_atcacert\_signer\_public\_key** (self, public\_key, cert)
- def **tng\_atcacert\_root\_cert\_size** (self, cert\_size)
- def **tng\_atcacert\_root\_cert** (self, cert, cert\_size)
- def **tng\_atcacert\_root\_public\_key** (self, public\_key)
- def **sha206a\_generate\_derive\_key** (self, parent\_key, derived\_key, param1, param2)
- def **sha206a\_diversify\_parent\_key** (self, parent\_key, diversified\_key)
- def **sha206a\_generate\_challenge\_response\_pair** (self, key, challenge, response)
- def **sha206a\_authenticate** (self, challenge, expected\_response, is\_verified)
- def **sha206a\_write\_data\_store** (self, slot, data, block, offset, length, lock\_after\_write)
- def **sha206a\_read\_data\_store** (self, slot, data, offset, length)
- def **sha206a\_get\_data\_store\_lock\_status** (self, slot, is\_locked)
- def **sha206a\_get\_dk\_update\_count** (self, dk\_update\_count)
- def **sha206a\_get\_pk\_useflag\_count** (self, pk\_avail\_count)
- def **sha206a\_get\_dk\_useflag\_count** (self, dk\_avail\_count)
- def **sha206a\_check\_pk\_useflag\_validity** (self, is\_consumed)
- def **sha206a\_check\_dk\_useflag\_validity** (self, is\_consumed)
- def **sha206a\_verify\_device\_consumption** (self, is\_consumed)

## Static Public Attributes

- int **r\_devtype** = 3
- create\_string\_buffer **r\_aes\_out** = create\_string\_buffer(16)
- **value**
- create\_string\_buffer **r\_ciphertext** = create\_string\_buffer(16)
- create\_string\_buffer **r\_plaintext** = create\_string\_buffer(16)
- create\_string\_buffer **r\_aes\_gfm\_output** = create\_string\_buffer(16)

- create\_string\_buffer **r\_aes\_cmac\_output** = create\_string\_buffer(16)
- create\_string\_buffer **r\_aes\_ctr\_output** = create\_string\_buffer(16)
- create\_string\_buffer **r\_iv** = create\_string\_buffer(16)
- create\_string\_buffer **r\_tag** = create\_string\_buffer(16)
- c\_uint8 **r\_is\_verified** = c\_uint8()
- create\_string\_buffer **r\_aes\_ccmac\_output** = create\_string\_buffer(16)
- c\_uint8 **r\_tag\_size** = c\_uint8()
- c\_uint32 **r\_counter\_value** = c\_uint32()
- create\_string\_buffer **r\_ecdh\_pms** = create\_string\_buffer(32)
- create\_string\_buffer **r\_ecdh\_out\_nonce** = create\_string\_buffer(32)
- create\_string\_buffer **r\_genkey\_pubkey** = create\_string\_buffer(64)
- create\_string\_buffer **r\_hmac\_digest** = create\_string\_buffer(32)
- create\_string\_buffer **r\_revision** = create\_string\_buffer(4)
- c\_uint8 **r\_latch\_state** = c\_uint8()
- create\_string\_buffer **r\_kdf\_out\_data** = create\_string\_buffer(64)
- create\_string\_buffer **r\_kdf\_out\_nonce** = create\_string\_buffer(32)
- create\_string\_buffer **r\_mac\_digest** = create\_string\_buffer(32)
- create\_string\_buffer **r\_nonce\_rand\_out** = create\_string\_buffer(32)
- create\_string\_buffer **r\_rand\_out** = create\_string\_buffer(32)
- create\_string\_buffer **r\_read\_zone\_data** = create\_string\_buffer(32)
- create\_string\_buffer **r\_ser\_num** = create\_string\_buffer(9)
- c\_uint8 **r\_is\_locked** = c\_uint8()
- create\_string\_buffer **r\_read\_enc\_data** = create\_string\_buffer(32)
- create\_string\_buffer **r\_read\_config\_data** = create\_string\_buffer(128)
- c\_uint8 **r\_same\_config** = c\_uint8()
- create\_string\_buffer **r\_read\_sig** = create\_string\_buffer(64)
- create\_string\_buffer **r\_read\_pubkey** = create\_string\_buffer(64)
- create\_string\_buffer **r\_read\_bytes\_zone\_data** = create\_string\_buffer(64)
- create\_string\_buffer **r\_sboot\_mac** = create\_string\_buffer(32)
- c\_uint8 **r\_sboot\_is\_verified** = c\_uint8()
- c\_uint8 **r\_stest\_res** = c\_uint8()
- create\_string\_buffer **r\_sha\_base\_data** = create\_string\_buffer(130)
- c\_uint8 **r\_sha\_base\_data\_size** = c\_uint8()
- create\_string\_buffer **r\_sha\_digest** = create\_string\_buffer(32)
- create\_string\_buffer **r\_sha\_context\_data** = create\_string\_buffer(130)
- c\_uint8 **r\_sha\_context\_size** = c\_uint8()
- create\_string\_buffer **r\_signature** = create\_string\_buffer(64)
- create\_string\_buffer **r\_mac** = create\_string\_buffer(64)
- c\_uint8 **r\_verify\_is\_verified** = c\_uint8()
- create\_string\_buffer **r\_response** = create\_string\_buffer(64)
- c\_size\_t **r\_cert\_size** = c\_size\_t(64)
- create\_string\_buffer **r\_cert** = create\_string\_buffer(r\_cert\_size.value)
- c\_uint8 **r\_csr\_size** = c\_uint8()
- create\_string\_buffer **r\_csr** = create\_string\_buffer(64)
- create\_string\_buffer **r\_formatted\_date** = create\_string\_buffer(3)
- c\_uint8 **r\_formatted\_date\_size** = c\_uint8()
- create\_string\_buffer **r\_enc\_dates** = create\_string\_buffer(3)
- c\_size\_t **r\_max\_cert\_size** = c\_size\_t(123)
- c\_int **r\_tng\_type** = c\_int(1)
- create\_string\_buffer **r\_derived\_key** = create\_string\_buffer(32)
- create\_string\_buffer **r\_diversified\_key** = create\_string\_buffer(32)
- create\_string\_buffer **r\_challenge\_response** = create\_string\_buffer(32)
- c\_uint8 **r\_verify\_is\_locked** = c\_uint8()
- c\_uint8 **r\_dk\_update\_count** = c\_uint8()
- c\_uint8 **r\_pk\_avail\_count** = c\_uint8()
- c\_uint8 **r\_dk\_avail\_count** = c\_uint8()
- c\_uint8 **r\_verify\_is\_consumed** = c\_uint8()



## 21.58 atcac\_aes\_cmac\_ctx Struct Reference

### Data Fields

- mbedtls\_cipher\_context\_t **mctx**
- void \* **ptr**

## 21.59 atcac\_aes\_gcm\_ctx Struct Reference

### Data Fields

- mbedtls\_cipher\_context\_t **mctx**

## 21.60 atcac\_hmac\_ctx Struct Reference

### Data Fields

- mbedtls\_md\_context\_t \* **mctx**
- void \* **ptr**

## 21.61 atcac\_pk\_ctx Struct Reference

### Data Fields

- mbedtls\_pk\_context **mctx**
- void \* **ptr**

## 21.62 atcac\_sha1\_ctx Struct Reference

### Data Fields

- mbedtls\_md\_context\_t **mctx**
- void \* **ptr**

## 21.63 atcac\_sha2\_256\_ctx Struct Reference

### Data Fields

- mbedtls\_md\_context\_t **mctx**
- void \* **ptr**

## 21.64 atcac\_x509\_ctx Struct Reference

### Data Fields

- void \* **ptr**

## 21.65 atcacert\_build\_state\_s Struct Reference

```
#include <lib/atcacert/atcacert_def.h>
```

### Data Fields

- const [atcacert\\_def\\_t](#) \* **cert\_def**  
*Certificate definition for the certificate being rebuilt.*
- uint8\_t \* **cert**  
*Buffer to contain the rebuilt certificate.*
- size\_t \* **cert\_size**  
*Current size of the certificate in bytes.*
- size\_t **max\_cert\_size**  
*Max size of the cert buffer in bytes.*
- uint8\_t **is\_device\_sn**  
*Indicates the structure contains the device SN.*
- ATCADeviceType **devtype**  
*Device type info for the certificate being rebuilt.*
- uint8\_t **device\_sn** [9]  
*Storage for the device SN, when it's found.*
- uint8\_t **is\_comp\_cert**  
*Indicates the structure contains the compressed certificate.*
- uint8\_t **comp\_cert** [72]  
*Storage for the compressed certificate when it's found.*

### 21.65.1 Detailed Description

Tracks the state of a certificate as it's being rebuilt from device information.

## 21.66 atcacert\_cert\_element\_s Struct Reference

```
#include <lib/atcacert/atcacert_def.h>
```

## Data Fields

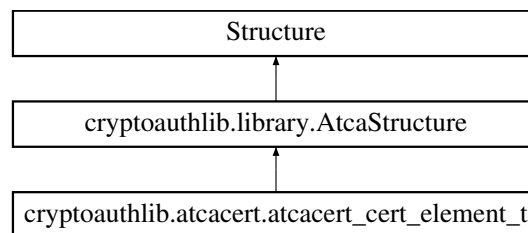
- char **id** [25]  
*ID identifying this element.*
- [atcacert\\_device\\_loc\\_t](#) **device\_loc**  
*Location in the device for the element.*
- [atcacert\\_cert\\_loc\\_t](#) **cert\_loc**  
*Location in the certificate template for the element.*
- [atcacert\\_transform\\_t](#) **transforms** [2]  
*List of transforms from device to cert for this element.*

### 21.66.1 Detailed Description

Defines a generic dynamic element for a certificate including the device and template locations.

## 21.67 cryptauthlib.atcacert.atcacert\_cert\_element\_t Class Reference

Inheritance diagram for cryptauthlib.atcacert.atcacert\_cert\_element\_t:



## Static Protected Attributes

- int **\_\_pack\_\_** = 1
- dict **\_\_def\_\_**

## Additional Inherited Members

Public Member Functions inherited from [cryptauthlib.library.AtcaStructure](#)

- None **\_\_init\_\_** (self, \*args, \*\*kwargs)
- def **from\_definition** (cls)
- def **check\_rationality** (cls)
- def **get\_field\_definition** (cls, str name)
- Any **\_\_getattr\_\_** (self, str name)
- def **\_\_iter\_\_** (self)
- def **\_\_str\_\_** (self)
- def **to\_c\_code** (self, name=None, \*\*kwargs)
- def **update\_from\_buffer** (self, buffer)

### 21.67.1 Detailed Description

CTypes mirror of atcacert\_cert\_element\_t from atcacert\_def.h

### 21.67.2 Field Documentation

#### 21.67.2.1 \_def\_

```
dict cryptoauthlib.atcacert.atcacert_cert_element_t._def_ [static], [protected]
```

**Initial value:**

```
= {
    'id': (c_char, 25), # ID identifying this element.
    'device_loc': (atcacert_device_loc_t,), # Location in the device for the element.
    'cert_loc': (atcacert_cert_loc_t,), # Location in the certificate template for the element.
    'transforms': (atcacert_transform_t, 2) # Transforms for converting the device data.
}
```

## 21.68 atcacert\_cert\_loc\_s Struct Reference

```
#include <lib/atcacert/atcacert_def.h>
```

### Data Fields

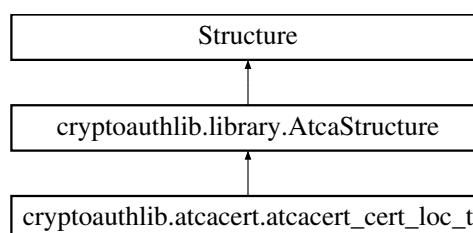
- **uint16\_t offset**  
*Byte offset in the certificate template.*
- **uint16\_t count**  
*Byte count. Set to 0 if it doesn't exist.*

### 21.68.1 Detailed Description

Defines a chunk of data in a certificate template.

## 21.69 cryptoauthlib.atcacert.atcacert\_cert\_loc\_t Class Reference

Inheritance diagram for cryptoauthlib.atcacert.atcacert\_cert\_loc\_t:



## Static Protected Attributes

- `int __pack__ = 1`
- `list __fields__ = [('offset', c_uint16), ('count', c_uint16)]`

## Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.library.AtcaStructure](#)

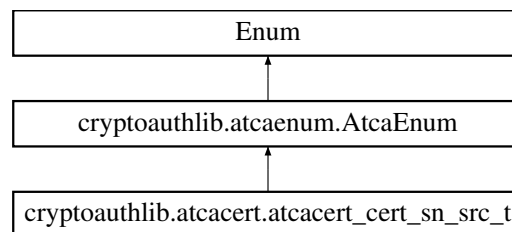
- `None __init__ (self, *args, **kwargs)`
- `def from_definition (cls)`
- `def check_rationality (cls)`
- `def get_field_definition (cls, str name)`
- `Any __getattr__ (self, str name)`
- `def __iter__ (self)`
- `def __str__ (self)`
- `def to_c_code (self, name=None, **kwargs)`
- `def update_from_buffer (self, buffer)`

### 21.69.1 Detailed Description

CTypes mirror of `atcacert_cert_loc_t` from `atcacert_def.h`

## 21.70 cryptoauthlib.atcacert.atcacert\_cert\_sn\_src\_t Class Reference

Inheritance diagram for `cryptoauthlib.atcacert.atcacert_cert_sn_src_t`:



## Static Public Attributes

- `int SNSRC_STORED = 0x0`
- `int SNSRC_STORED_DYNAMIC = 0x7`
- `int SNSRC_DEVICE_SN = 0x8`
- `int SNSRC_SIGNER_ID = 0x9`
- `int SNSRC_PUB_KEY_HASH = 0xA`
- `int SNSRC_DEVICE_SN_HASH = 0xB`
- `int SNSRC_PUB_KEY_HASH_POS = 0xC`
- `int SNSRC_DEVICE_SN_HASH_POS = 0xD`
- `int SNSRC_PUB_KEY_HASH_RAW = 0xE`
- `int SNSRC_DEVICE_SN_HASH_RAW = 0xF`

## Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

- `def __str__ (self)`
- `def __eq__ (self, other)`
- `def __ne__ (self, other)`
- `def __int__ (self)`
- `def __hash__ (self)`

Data Fields inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

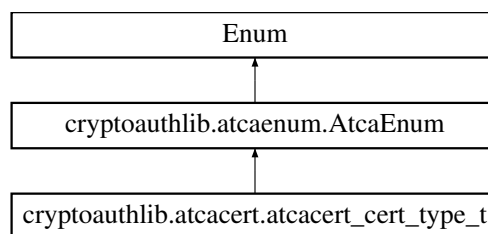
- `name`
- `value`

### 21.70.1 Detailed Description

Sources for the certificate serial number

## 21.71 cryptoauthlib.atcacert.atcacert\_cert\_type\_t Class Reference

Inheritance diagram for `cryptoauthlib.atcacert.atcacert_cert_type_t`:



## Static Public Attributes

- `int CERTTYPE_X509 = 0`
- `int CERTTYPE_CUSTOM = 1`

## Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

- `def __str__ (self)`
- `def __eq__ (self, other)`
- `def __ne__ (self, other)`
- `def __int__ (self)`
- `def __hash__ (self)`

### Data Fields inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

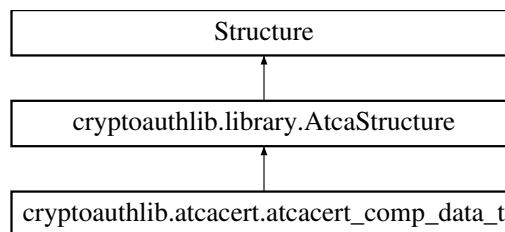
- **name**
- **value**

## 21.71.1 Detailed Description

Types of certificates

## 21.72 [cryptoauthlib.atcacert.atcacert\\_comp\\_data\\_t](#) Class Reference

Inheritance diagram for [cryptoauthlib.atcacert.atcacert\\_comp\\_data\\_t](#):



### Static Protected Attributes

- `int __pack_ = 1`
- `int __size_ = 72`
- `list \_fields\_`

### Additional Inherited Members

#### Public Member Functions inherited from [cryptoauthlib.library.AtcaStructure](#)

- `None __init__ (self, *args, **kwargs)`
- `def from\_definition (cls)`
- `def check\_rationality (cls)`
- `def get\_field\_definition (cls, str name)`
- `Any __getattr__ (self, str name)`
- `def __iter__ (self)`
- `def __str__ (self)`
- `def to\_c\_code (self, name=None, **kwargs)`
- `def update\_from\_buffer (self, buffer)`

## 21.72.1 Detailed Description

CTypes definition of certificate signature storage which includes other certificate metadata which is why it's often identified as "compresessed cert" for the slot in configurators

## 21.72.2 Field Documentation

### 21.72.2.1 \_fields\_

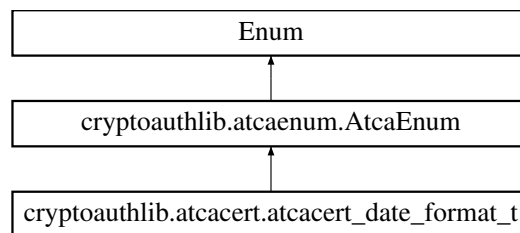
list cryptoauthlib.atcacert.atcacert\_comp\_data\_t.\_fields\_ [static], [protected]

Initial value:

```
= [
    ('r', c_uint8*32),          # P256 signature 'r' value - big endian
    ('s', c_uint8*32),          # P256 signature 's' value - big endian
    ('year', c_uint64, 5),      # Years after 2000
    ('month', c_uint64, 4),     # Month (0 - 11), see atcacert_tm_utc_t
    ('day', c_uint64, 5),       # Day (1 - 31), see atcacert_tm_utc_t
    ('hour', c_uint64, 5),      # Hour (0 - 23), see atcacert_tm_utc_t
    ('expire', c_uint64, 5),     # Expire years (<=31)
    ('signer_id', c_uint64, 16), # Value used in the signing cert subject name
    ('chain_id', c_uint64, 4),   # Revision identifier
    ('template_id', c_uint64, 4), # Location in a chain
    ('reserved_70_4', c_uint64, 4), # Reserved - lower four bits of byte 70
    ('sn_source', c_uint64, 4),  # Serial number format, see atcacert_cert_sn_src_t
    ('reserved_71_8', c_uint64, 8) # Reserved - byte 71
]
```

## 21.73 cryptoauthlib.atcacert.atcacert\_date\_format\_t Class Reference

Inheritance diagram for cryptoauthlib.atcacert.atcacert\_date\_format\_t:



### Static Public Attributes

- int `DATEFMT_ISO8601_SEP` = 0
- int `DATEFMT_RFC5280.UTC` = 1
- int `DATEFMT_POSIX_UINT32_BE` = 2
- int `DATEFMT_POSIX_UINT32_LE` = 3
- int `DATEFMT_RFC5280_GEN` = 4

### Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

- def `__str__` (self)
- def `__eq__` (self, other)
- def `__ne__` (self, other)
- def `__int__` (self)
- def `__hash__` (self)



Data Fields inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

- **name**
- **value**

### 21.73.1 Detailed Description

Support Date formats by the atcacert

## 21.74 atcacert\_def\_s Struct Reference

```
#include <lib/atcacert/atcacert_def.h>
```

### Data Fields

- [atcacert\\_cert\\_type\\_t](#) **type**  
*Certificate type.*
- [atcacert\\_device\\_loc\\_t](#) **comp\_cert\_dev\_loc**  
*Where on the device the compressed cert can be found.*
- const struct [atcacert\\_def\\_s](#) \* **ca\_cert\_def**  
*Certificate definition of the CA certificate.*

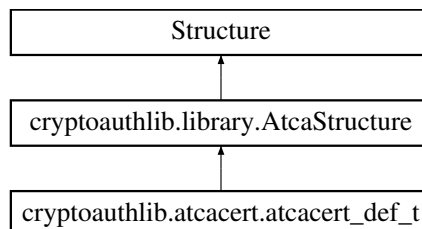
### 21.74.1 Detailed Description

Defines a certificate and all the pieces to work with it.

If any of the standard certificate elements (`std_cert_elements`) are not a part of the certificate definition, set their count to 0 to indicate their absence.

## 21.75 cryptoauthlib.atcacert.atcacert\_def\_t Class Reference

Inheritance diagram for `cryptoauthlib.atcacert.atcacert_def_t`:



### Static Protected Attributes

- **\_def\_**

## Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.library.AtcaStructure](#)

- None `__init__` (self, \*args, \*\*kwargs)
- def `from_definition` (cls)
- def `check_rationality` (cls)
- def `get_field_definition` (cls, str name)
- Any `__getattr__` (self, str name)
- def `__iter__` (self)
- def `__str__` (self)
- def `to_c_code` (self, name=None, \*\*kwargs)
- def `update_from_buffer` (self, buffer)

### 21.75.1 Detailed Description

CTypes mirror of `atcacert_def_t` from `atcacert_def.h`

## 21.76 atcacert\_device\_loc\_s Struct Reference

```
#include <lib/atcacert/atcacert_def.h>
```

### Data Fields

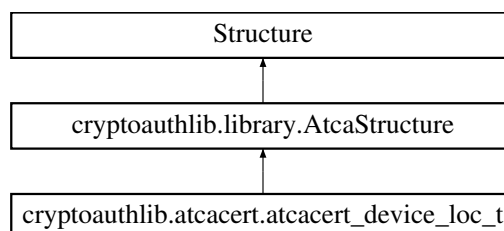
- [atcacert\\_device\\_zone\\_t zone](#)  
*Zone in the device.*
- `uint16_t slot`  
*Slot within the data zone. Only applies if zone is DEVZONE\_DATA.*
- `uint8_t is_genkey`  
*If true, use GenKey command to get the contents instead of Read.*
- `uint16_t offset`  
*Byte offset in the zone.*
- `uint16_t count`  
*Byte count.*

### 21.76.1 Detailed Description

Defines a chunk of data in an ATECC device.

## 21.77 cryptoauthlib.atcacert.atcacert\_device\_loc\_t Class Reference

Inheritance diagram for `cryptoauthlib.atcacert.atcacert_device_loc_t`:



Static Protected Attributes

- int `_pack_` = 1
- dict `_def_`

Additional Inherited Members

Public Member Functions inherited from `cryptoauthlib.library.AtcaStructure`

- None `__init__` (self, \*args, \*\*kwargs)
- def `from_definition` (cls)
- def `check_rationality` (cls)
- def `get_field_definition` (cls, str name)
- Any `__getattr__` (self, str name)
- def `__iter__` (self)
- def `__str__` (self)
- def `to_c_code` (self, name=None, \*\*kwargs)
- def `update_from_buffer` (self, buffer)

21.77.1 Detailed Description

CTypes mirror of `atcacert_device_loc_t` from `atcacert_def.h`

21.77.2 Field Documentation

21.77.2.1 `_def_`

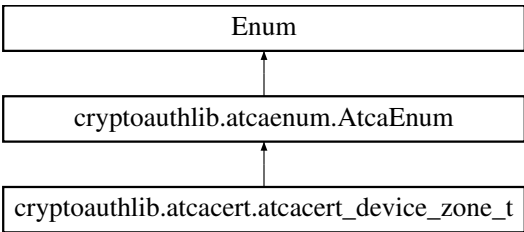
dict `cryptoauthlib.atcacert.atcacert_device_loc_t._def_` [static], [protected]

Initial value:

```
= {
    'zone': (atcacert_device_zone_t), # Zone in the device.
    'slot': (c_uint16,), # Slot within the data zone. Only applies if zone is DEVZONE_DATA.
    'is_genkey': (c_uint8,), # If true, use GenKey command to get the contents instead of Read.
    'offset': (c_uint16,), # Byte offset in the zone.
    'count': (c_uint16,) # Byte count.
}
```

21.78 `cryptoauthlib.atcacert.atcacert_device_zone_t` Class Reference

Inheritance diagram for `cryptoauthlib.atcacert.atcacert_device_zone_t`:



### Static Public Attributes

- int **DEVZONE\_CONFIG** = 0x00
- int **DEVZONE\_OTP** = 0x01
- int **DEVZONE\_DATA** = 0x02
- int **DEVZONE\_GENKEY** = 0x03,
- int **DEVZONE\_NONE** = 0x07

### Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

- def **\_\_str\_\_** (self)
- def **\_\_eq\_\_** (self, other)
- def **\_\_ne\_\_** (self, other)
- def **\_\_int\_\_** (self)
- def **\_\_hash\_\_** (self)

Data Fields inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

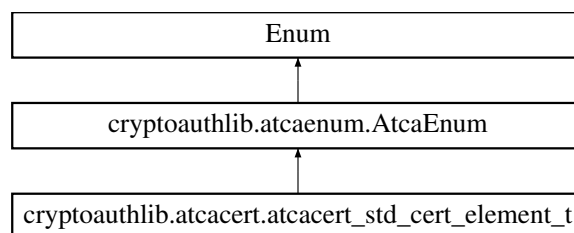
- **name**
- **value**

### 21.78.1 Detailed Description

ATECC device zones. The values match the Zone Encodings as specified in the datasheet

## 21.79 cryptoauthlib.atcacert.atcacert\_std\_cert\_element\_t Class Reference

Inheritance diagram for cryptoauthlib.atcacert.atcacert\_std\_cert\_element\_t:



### Static Public Attributes

- int **STDCERT\_PUBLIC\_KEY** = 0
- int **STDCERT\_SIGNATURE** = 1
- int **STDCERT\_ISSUE\_DATE** = 2
- int **STDCERT\_EXPIRE\_DATE** = 3
- int **STDCERT\_SIGNER\_ID** = 4
- int **STDCERT\_CERT\_SN** = 5
- int **STDCERT\_AUTH\_KEY\_ID** = 6
- int **STDCERT\_SUBJ\_KEY\_ID** = 7

Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

- def `__str__` (self)
- def `__eq__` (self, other)
- def `__ne__` (self, other)
- def `__int__` (self)
- def `__hash__` (self)

Data Fields inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

- `name`
- `value`

21.79.1 Detailed Description

Standard dynamic certificate elements

21.80 atcacert\_tm\_utc\_s Struct Reference

```
#include <lib/atcacert/atcacert_date.h>
```

Data Fields

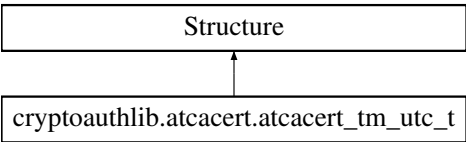
- int `tm_sec`
- int `tm_min`
- int `tm_hour`
- int `tm_mday`
- int `tm_mon`
- int `tm_year`

21.80.1 Detailed Description

Holds a broken-down date in UTC. Mimics `atcacert_tm_utc_t` from `time.h`.

21.81 cryptoauthlib.atcacert.atcacert\_tm\_utc\_t Class Reference

Inheritance diagram for `cryptoauthlib.atcacert.atcacert_tm_utc_t`:



## Public Member Functions

- `def __init__ (self, *args, **kwargs)`

## Static Protected Attributes

- `list \_fields\_`

### 21.81.1 Detailed Description

CTypes mirror of `atcacert_tm_utc_t` from `atcacert_date.h` which mimics the posix time structure

### 21.81.2 Field Documentation

#### 21.81.2.1 `_fields_`

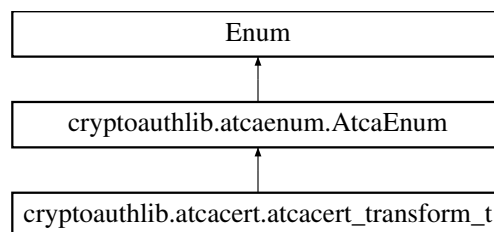
`list cryptoauthlib.atcacert.atcacert_tm_utc_t._fields_ [static], [protected]`

Initial value:

```
= [
    ('tm_sec', c_int),      # 0 to 59
    ('tm_min', c_int),      # 0 to 59
    ('tm_hour', c_int),     # 0 to 23
    ('tm_mday', c_int),     # 1 to 31
    ('tm_mon', c_int),      # 0 to 11
    ('tm_year', c_int),     # years since 1900
]
```

## 21.82 cryptoauthlib.atcacert.atcacert\_transform\_t Class Reference

Inheritance diagram for `cryptoauthlib.atcacert.atcacert_transform_t`:



## Static Public Attributes

- `int TF_NONE = 0x00`
- `int TF_REVERSE = 0x01`
- `int TF_BIN2HEX_UC = 0x02`
- `int TF_BIN2HEX_LC = 0x03`
- `int TF_HEX2BIN_UC = 0x04`
- `int TF_HEX2BIN_LC = 0x05`
- `int TF_BIN2HEX_SPACE_UC = 0x06`
- `int TF_BIN2HEX_SPACE_LC = 0x07`
- `int TF_HEX2BIN_SPACE_UC = 0x08`
- `int TF_HEX2BIN_SPACE_LC = 0x09`

## Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

- `def __str__(self)`
- `def __eq__(self, other)`
- `def __ne__(self, other)`
- `def __int__(self)`
- `def __hash__(self)`

Data Fields inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

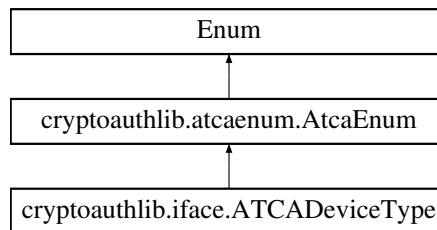
- `name`
- `value`

### 21.82.1 Detailed Description

Transforms for converting the device data.

## 21.83 cryptoauthlib.iface.ATCADeviceType Class Reference

Inheritance diagram for `cryptoauthlib.iface.ATCADeviceType`:



### Static Public Attributes

- `int ATSHA204A = 0`
- `int ATECC108A = 1`
- `int ATECC508A = 2`
- `int ATECC608A = 3`
- `int ATECC608B = 3`
- `int ATECC608 = 3`
- `int ATSHA206A = 4`
- `int TA100 = 0x10`
- `int TA101 = 0x11`
- `int ECC204 = 0x20`
- `int TA010 = 0x21`
- `int ECC206 = 0x22`
- `int RNG90 = 0x23`
- `int SHA104 = 0x24`
- `int SHA105 = 0x25`
- `int SHA106 = 0x26`
- `int ATCA_DEV_UNKNOWN = 0x7E`
- `int ATCA_DEV_INVALID = 0x7F`

## Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

- `def __str__ (self)`
- `def __eq__ (self, other)`
- `def __ne__ (self, other)`
- `def __int__ (self)`
- `def __hash__ (self)`

Data Fields inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

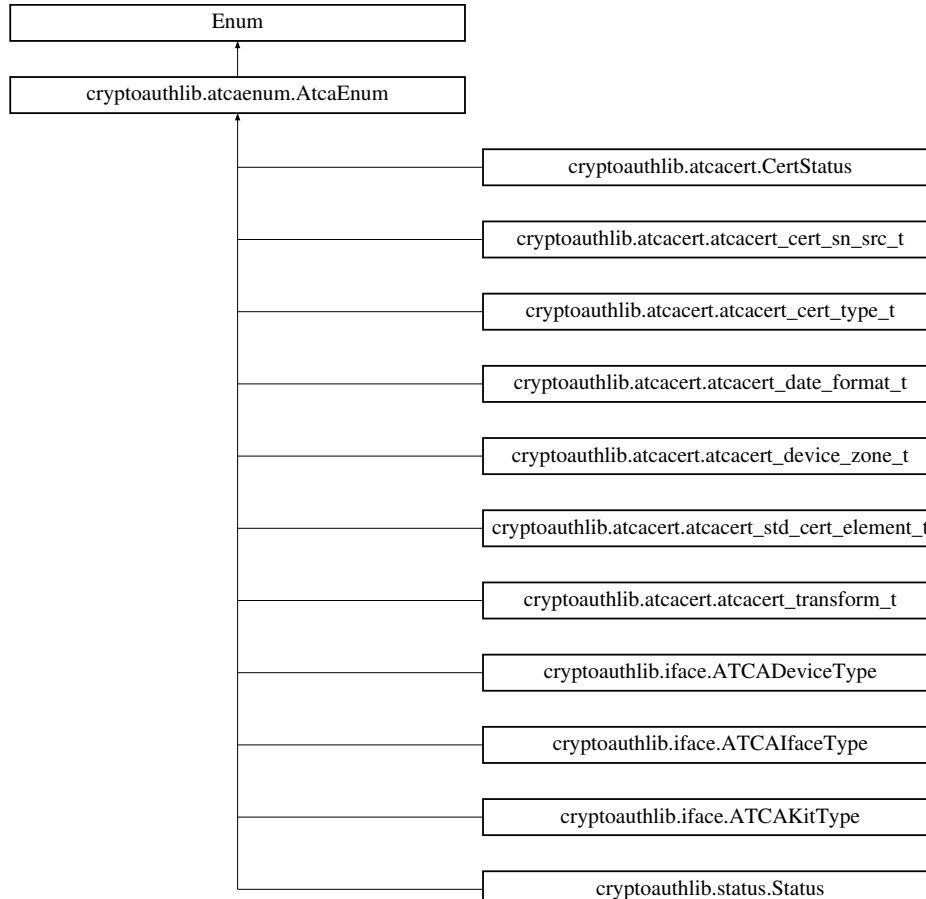
- `name`
- `value`

### 21.83.1 Detailed Description

Device Type Enumeration from `atca_devtypes.h`

## 21.84 cryptoauthlib.atcaenum.AtcaEnum Class Reference

Inheritance diagram for `cryptoauthlib.atcaenum.AtcaEnum`:





## Public Member Functions

- `def __str__(self)`
- `def __eq__(self, other)`
- `def __ne__(self, other)`
- `def __int__(self)`
- `def __hash__(self)`

## Data Fields

- `name`
- `value`

### 21.84.1 Detailed Description

Overload of standard python enum for some additional convenience features. Assumes closer alignment to C style where the value is always an integer

## 21.85 ATCAHAL\_t Struct Reference

HAL Driver Structure.

```
#include <lib/atca_iface.h>
```

## Data Fields

- `ATCA_STATUS(* halinit)(ATCAIface iface, ATCAIfaceCfg *cfg)`
- `ATCA_STATUS(* halpostinit)(ATCAIface iface)`
- `ATCA_STATUS(* halsend)(ATCAIface iface, uint8_t word_address, uint8_t *txdata, int txlength)`
- `ATCA_STATUS(* halreceive)(ATCAIface iface, uint8_t word_address, uint8_t *rxdata, uint16_t *rxlength)`
- `ATCA_STATUS(* halcontrol)(ATCAIface iface, uint8_t option, void *param, size_t paramlen)`
- `ATCA_STATUS(* halrelease)(void *hal_data)`

### 21.85.1 Detailed Description

HAL Driver Structure.

## 21.86 atcal2Cmaster Struct Reference

this is the hal\_data for ATCA HAL for ASF SERCOM

```
#include <lib/hal/hal_uc3_i2c_asf.h>
```

## Data Fields

- int **id**
- i2c\_config\_t **conf**
- int **ref\_ct**
- uint8\_t **twi\_id**
- avr32\_twi\_t \* **twi\_master\_instance**
- int **bus\_index**

### 21.86.1 Detailed Description

this is the hal\_data for ATCA HAL for ASF SERCOM

## 21.87 ATCAIfaceCfg Struct Reference

## Data Fields

- [ATCAIfaceType](#) **iface\_type**
- ATCADeviceType **devtype**
- 

```
union {
    struct {
        uint8_t address
        uint8_t bus
        uint32_t baud
    } atcai2c
    struct {
        uint8_t address
        uint8_t bus
    } atcaswi
    struct {
        uint8_t bus
        uint8_t select_pin
        uint32_t baud
    } atcaspi
    struct {
        ATCAKitType dev_interface
        uint8_t dev_identity
        uint8_t port
        uint32_t baud
        uint8_t wordsize
        uint8_t parity
        uint8_t stopbits
    } atcauart
    struct {
        int idx
        ATCAKitType dev_interface
        uint8_t dev_identity
        uint32_t vid
        uint32_t pid
        uint32_t packetsize
    } atcahid
    struct {
```

```
ATCAKitType dev_interface
uint8_t dev_identity
uint32_t flags
} atcakit
struct {
    ATCA_STATUS(* halinit )(void *hal, void *cfg)
    ATCA_STATUS(* halpostinit )(void *iface)
    ATCA_STATUS(* halsend )(void *iface, uint8_t
        word_address, uint8_t *txdata,
        int txlength)
    ATCA_STATUS(* halreceive )(void *iface, uint8_t
        word_address, uint8_t *rxdata,
        uint16_t *rxlength)
    ATCA_STATUS(* halwake )(void *iface)
    ATCA_STATUS(* halidle )(void *iface)
    ATCA_STATUS(* halsleep )(void *iface)
    ATCA_STATUS(* halrelease )(void *hal_data)
    } atcacustom
} cfg

• uint16_t wake_delay
• int rx_retries
• void * cfg_data
```

21.87.1 Field Documentation

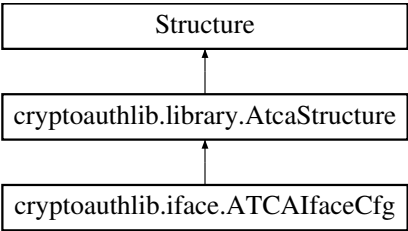
21.87.1.1 address

uint8\_t ATCAIfaceCfg::address

Device address - the upper 7 bits are the I2c address bits

21.88 cryptoauthlib.iface.ATCAIfaceCfg Class Reference

Inheritance diagram for cryptoauthlib.iface.ATCAIfaceCfg:



Static Protected Attributes

- tuple `_anonymous_` = ('cfg',)
- dict `_map_`
- dict `_def_`

## Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.library.AtcaStructure](#)

- None `__init__` (self, \*args, \*\*kwargs)
- def `from_definition` (cls)
- def `check_rationality` (cls)
- def `get_field_definition` (cls, str name)
- Any `__getattr__` (self, str name)
- def `__iter__` (self)
- def `__str__` (self)
- def `to_c_code` (self, name=None, \*\*kwargs)
- def `update_from_buffer` (self, buffer)

### 21.88.1 Detailed Description

Interface configuration structure used by `atcab_init()`

### 21.88.2 Field Documentation

#### 21.88.2.1 `_def_`

dict `cryptoauthlib.iface.ATCAIfaceCfg._def_` [static], [protected]

Initial value:

```
= {
    'iface_type': (ATCAIfaceType,),
    'devtype': (ATCADeviceType,),
    'cfg': (_ATCAIfaceParams,),
    'wake_delay': (c_uint16,),
    'rx_retries': (c_int,),
    'cfg_data': (c_void_p,)
}
```

#### 21.88.2.2 `_map_`

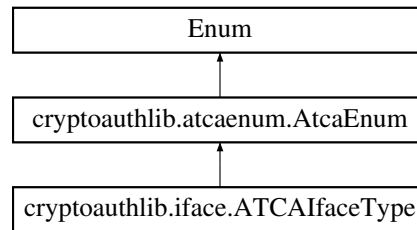
dict `cryptoauthlib.iface.ATCAIfaceCfg._map_` [static], [protected]

Initial value:

```
= {
    'cfg': ('iface_type', {
        ATCAIfaceType.ATCA_I2C_IFACE: 'atcai2c',
        ATCAIfaceType.ATCA_SWI_IFACE: 'atcaswi',
        ATCAIfaceType.ATCA_UART_IFACE: 'atcauart',
        ATCAIfaceType.ATCA_SPI_IFACE: 'atcaspi',
        ATCAIfaceType.ATCA_HID_IFACE: 'atcahid',
        ATCAIfaceType.ATCA_KIT_IFACE: 'atcakit',
        ATCAIfaceType.ATCA_CUSTOM_IFACE: 'atcacustom'
    })
}
```

## 21.89 cryptoauthlib.iface.ATCAIfaceType Class Reference

Inheritance diagram for cryptoauthlib.iface.ATCAIfaceType:



### Static Public Attributes

- int **ATCA\_I2C\_IFACE** = 0
- int **ATCA\_SWI\_IFACE** = 1
- int **ATCA\_UART\_IFACE** = 2
- int **ATCA\_SPI\_IFACE** = 3
- int **ATCA\_HID\_IFACE** = 4
- int **ATCA\_KIT\_IFACE** = 5
- int **ATCA\_CUSTOM\_IFACE** = 6
- int **ATCA\_I2C\_GPIO\_IFACE** = 7
- int **ATCA\_SWI\_GPIO\_IFACE** = 8
- int **ATCA\_SPI\_GPIO\_IFACE** = 9
- int **ATCA\_UNKNOWN\_IFACE** = 0xFE

### Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

- def **\_\_str\_\_** (self)
- def **\_\_eq\_\_** (self, other)
- def **\_\_ne\_\_** (self, other)
- def **\_\_int\_\_** (self)
- def **\_\_hash\_\_** (self)

Data Fields inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

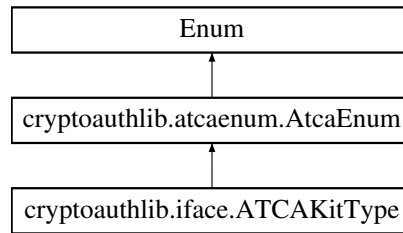
- **name**
- **value**

### 21.89.1 Detailed Description

Interface Type Enumerations from `atca_iface.h`

## 21.90 cryptoauthlib.iface.ATCAKitType Class Reference

Inheritance diagram for cryptoauthlib.iface.ATCAKitType:



### Static Public Attributes

- int **ATCA\_KIT\_AUTO\_IFACE** = 0
- int **ATCA\_KIT\_I2C\_IFACE** = 1
- int **ATCA\_KIT\_SWI\_IFACE** = 2
- int **ATCA\_KIT\_SPI\_IFACE** = 3
- int **ATCA\_KIT\_UNKNOWN\_IFACE** = 4

### Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

- def **\_\_str\_\_** (self)
- def **\_\_eq\_\_** (self, other)
- def **\_\_ne\_\_** (self, other)
- def **\_\_int\_\_** (self)
- def **\_\_hash\_\_** (self)

Data Fields inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

- **name**
- **value**

### 21.90.1 Detailed Description

Interface Type Enumerations for Kit devices

## 21.91 ATCAPacket Struct Reference

### Data Fields

- uint8\_t **reserved**
- uint8\_t **txsize**
- uint8\_t **opcode**
- uint8\_t **param1**
- uint16\_t **param2**
- uint8\_t **data** [((198u)) - 6]
- uint8\_t **execTime**

## 21.92 cryptoauthlib.library.AtcaReference Class Reference

### Public Member Functions

- def `__init__` (self, value)
- def `__eq__` (self, other)
- def `__ne__` (self, other)
- def `__lt__` (self, other)
- def `__le__` (self, other)
- def `__gt__` (self, other)
- def `__ge__` (self, other)
- def `__int__` (self)
- def `__str__` (self)

### Data Fields

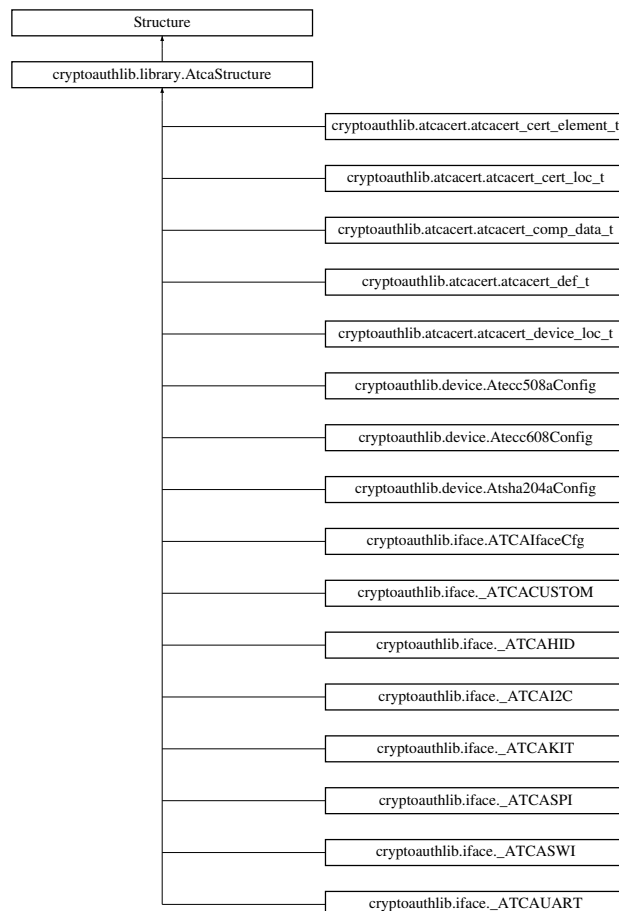
- value

### 21.92.1 Detailed Description

A simple wrapper to pass an immutable type to a function for return

## 21.93 cryptoauthlib.library.AtcaStructure Class Reference

Inheritance diagram for cryptoauthlib.library.AtcaStructure:



## Public Member Functions

- None `__init__` (self, \*args, \*\*kwargs)
- def `from_definition` (cls)
- def `check_rationality` (cls)
- def `get_field_definition` (cls, str name)
- Any `__getattr__` (self, str name)
- def `__iter__` (self)
- def `__str__` (self)
- def `to_c_code` (self, name=None, \*\*kwargs)
- def `update_from_buffer` (self, buffer)

### 21.93.1 Detailed Description

An extended ctypes structure to accept complex inputs

### 21.93.2 Member Function Documentation

#### 21.93.2.1 `check_rationality()`

```
def cryptoauthlib.library.AtcaStructure.check_rationality (
    cls )
```

Perform a rationality check on the structure definition against the expected definition by checking structure sizes between the compiled library and the python library

#### 21.93.2.2 `from_definition()`

```
def cryptoauthlib.library.AtcaStructure.from_definition (
    cls )
```

Trigger `_field_` creation from the values provided in `_def_` - must be run before the class is instantiated

## 21.94 atcaSWImaster Struct Reference

this is the `hal_data` for ATCA HAL for ASF SERCOM

```
#include <lib/hal/swi_uart_start.h>
```



## Data Fields

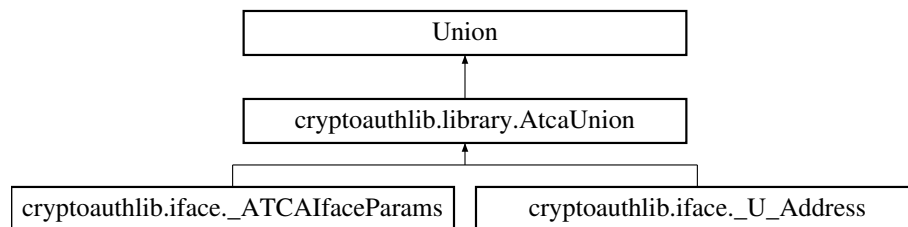
- struct usart\_module **usart\_instance**
- int **ref\_ct**
- int **bus\_index**
- struct usart\_sync\_descriptor **USART\_SWI**
- uint32\_t **sercom\_core\_freq**

### 21.94.1 Detailed Description

this is the hal\_data for ATCA HAL for ASF SERCOM

## 21.95 cryptoauthlib.library.AtcaUnion Class Reference

Inheritance diagram for cryptoauthlib.library.AtcaUnion:



## Public Member Functions

- def **\_\_init\_\_** (self, \*args, \*\*kwargs)
- def [from\\_definition](#) (cls)
- def [check\\_rationality](#) (cls)
- def **get\_field\_definition** (cls, str name)
- Any **\_\_getattr\_\_** (self, str name)
- def **\_\_iter\_\_** (self)
- def **\_\_str\_\_** (self)
- def **to\_c\_code** (self, name=None, \*\*kwargs)
- def **update\_from\_buffer** (self, buffer)

## Protected Attributes

- **\_selected**

### 21.95.1 Detailed Description

An extended ctypes structure to accept complex inputs

### 21.95.2 Member Function Documentation

### 21.95.2.1 check\_rationality()

```
def cryptoauthlib.library.AtcaUnion.check_rationality (
    cls )
```

Perform a rationality check on the structure definition against the expected definition by checking structure sizes between the compiled library and the python library

### 21.95.2.2 from\_definition()

```
def cryptoauthlib.library.AtcaUnion.from_definition (
    cls )
```

Trigger `_field_` creation from the values provided in `_def_` - must be run before the class is instantiated

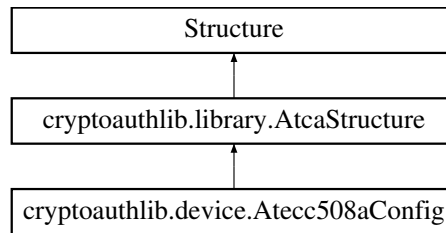
## 21.96 atecc508a\_config\_s Struct Reference

### Data Fields

- uint32\_t **SN03**
- uint32\_t **RevNum**
- uint32\_t **SN47**
- uint8\_t **SN8**
- uint8\_t **Reserved0**
- uint8\_t **I2C\_Enable**
- uint8\_t **Reserved1**
- uint8\_t **I2C\_Address**
- uint8\_t **Reserved2**
- uint8\_t **OTPmode**
- uint8\_t **ChipMode**
- uint16\_t **SlotConfig** [16]
- uint8\_t **Counter0** [8]
- uint8\_t **Counter1** [8]
- uint8\_t **LastKeyUse** [16]
- uint8\_t **UserExtra**
- uint8\_t **Selector**
- uint8\_t **LockValue**
- uint8\_t **LockConfig**
- uint16\_t **SlotLocked**
- uint16\_t **RFU**
- uint32\_t **X509format**
- uint16\_t **KeyConfig** [16]

## 21.97 cryptoauthlib.device.Atecc508aConfig Class Reference

Inheritance diagram for `cryptoauthlib.device.Atecc508aConfig`:



### Static Protected Attributes

- list `__fields__`
- int `__pack__` = 1

### Additional Inherited Members

Public Member Functions inherited from `cryptoauthlib.library.AtcaStructure`

- None `__init__` (self, \*args, \*\*kwargs)
- def `from_definition` (cls)
- def `check_rationality` (cls)
- def `get_field_definition` (cls, str name)
- Any `__getattr__` (self, str name)
- def `__iter__` (self)
- def `__str__` (self)
- def `to_c_code` (self, name=None, \*\*kwargs)
- def `update_from_buffer` (self, buffer)

### 21.97.1 Detailed Description

ATECC508A Config Zone Definition

### 21.97.2 Field Documentation

### 21.97.2.1 `_fields_`

```
list cryptoauthlib.device.Atecc508aConfig._fields_ [static], [protected]
```

#### Initial value:

```
= [ ('SN03', c_uint8*4),  
    ('RevNum', c_uint8*4),  
    ('SN48', c_uint8*5),  
    ('Reserved13', c_uint8),  
    ('I2C_Enable', I2cEnable),  
    ('Reserved15', c_uint8),  
    ('I2C_Address', c_uint8),  
    ('Reserved17', c_uint8),  
    ('OTPmode', c_uint8),  
    ('ChipMode', ChipMode508),  
    ('SlotConfig', SlotConfig*16),  
    ('Counter0', c_uint8*8),  
    ('Counter1', c_uint8*8),  
    ('LastKeyUse', c_uint8*16),  
    ('UserExtra', c_uint8),  
    ('Selector', c_uint8),  
    ('LockValue', c_uint8),  
    ('LockConfig', c_uint8),  
    ('SlotLocked', c_uint16),  
    ('RFU', c_uint16),  
    ('X509format', X509Format*4),  
    ('KeyConfig', KeyConfig*16)]
```

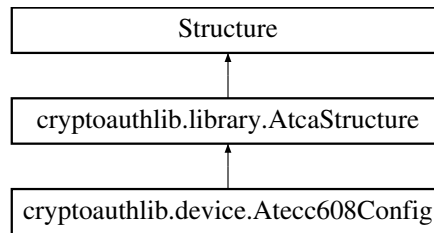
## 21.98 atecc608\_config\_s Struct Reference

### Data Fields

- `uint32_t` **SN03**
- `uint32_t` **RevNum**
- `uint32_t` **SN47**
- `uint8_t` **SN8**
- `uint8_t` **AES\_Enable**
- `uint8_t` **I2C\_Enable**
- `uint8_t` **Reserved1**
- `uint8_t` **I2C\_Address**
- `uint8_t` **Reserved2**
- `uint8_t` **CountMatch**
- `uint8_t` **ChipMode**
- `uint16_t` **SlotConfig** [16]
- `uint8_t` **Counter0** [8]
- `uint8_t` **Counter1** [8]
- `uint8_t` **UseLock**
- `uint8_t` **VolatileKeyPermission**
- `uint16_t` **SecureBoot**
- `uint8_t` **KdflvLoc**
- `uint16_t` **KdflvStr**
- `uint8_t` **Reserved3** [9]
- `uint8_t` **UserExtra**
- `uint8_t` **UserExtraAdd**
- `uint8_t` **LockValue**
- `uint8_t` **LockConfig**
- `uint16_t` **SlotLocked**
- `uint16_t` **ChipOptions**
- `uint32_t` **X509format**
- `uint16_t` **KeyConfig** [16]

## 21.99 cryptoauthlib.device.Atecc608Config Class Reference

Inheritance diagram for cryptoauthlib.device.Atecc608Config:



### Static Protected Attributes

- list [\\_fields\\_](#)
- int [\\_pack\\_](#) = 1

### Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.library.AtcaStructure](#)

- None [\\_\\_init\\_\\_](#) (self, \*args, \*\*kwargs)
- def [from\\_definition](#) (cls)
- def [check\\_rationality](#) (cls)
- def [get\\_field\\_definition](#) (cls, str name)
- Any [\\_\\_getattr\\_\\_](#) (self, str name)
- def [\\_\\_iter\\_\\_](#) (self)
- def [\\_\\_str\\_\\_](#) (self)
- def [to\\_c\\_code](#) (self, name=None, \*\*kwargs)
- def [update\\_from\\_buffer](#) (self, buffer)

### 21.99.1 Detailed Description

ATECC608 Config Zone Definition

### 21.99.2 Field Documentation

### 21.99.2.1 \_\_fields\_\_

```
list cryptoauthlib.device.Atecc608Config.__fields__ [static], [protected]
```

#### Initial value:

```
= [('SN03', c_uint8*4),
    ('RevNum', c_uint8*4),
    ('SN48', c_uint8*5),
    ('AES_Enable', AesEnable),
    ('I2C_Enable', I2cEnable),
    ('Reserved15', c_uint8),
    ('I2C_Address', c_uint8),
    ('Reserved17', c_uint8),
    ('CountMatch', CountMatch),
    ('ChipMode', ChipMode608),
    ('SlotConfig', SlotConfig*16),
    ('Counter0', c_uint8*8),
    ('Counter1', c_uint8*8),
    ('UseLock', UseLock),
    ('VolatileKeyPermission', VolatileKeyPermission),
    ('SecureBoot', SecureBoot),
    ('KdfIvLoc', c_uint8),
    ('KdfIvStr', c_uint8*2),
    ('Reserved68', c_uint8*9),
    ('UserExtra', c_uint8),
    ('UserExtraAdd', c_uint8),
    ('LockValue', c_uint8),
    ('LockConfig', c_uint8),
    ('SlotLocked', c_uint16),
    ('ChipOptions', ChipOptions),
    ('X509Format', X509Format*4),
    ('KeyConfig', KeyConfig*16)]
```

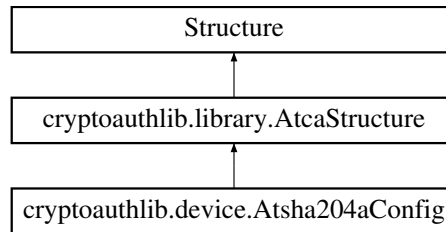
## 21.100 atsha204a\_config\_s Struct Reference

### Data Fields

- uint32\_t **SN03**
- uint32\_t **RevNum**
- uint32\_t **SN47**
- uint8\_t **SN8**
- uint8\_t **Reserved0**
- uint8\_t **I2C\_Enable**
- uint8\_t **Reserved1**
- uint8\_t **I2C\_Address**
- uint8\_t **Reserved2**
- uint8\_t **OTPmode**
- uint8\_t **ChipMode**
- uint16\_t **SlotConfig** [16]
- uint16\_t **Counter** [8]
- uint8\_t **LastKeyUse** [16]
- uint8\_t **UserExtra**
- uint8\_t **Selector**
- uint8\_t **LockValue**
- uint8\_t **LockConfig**

## 21.101 cryptauthlib.device.Atsha204aConfig Class Reference

Inheritance diagram for cryptauthlib.device.Atsha204aConfig:



### Static Protected Attributes

- list `_fields_`
- int `_pack_` = 1

### Additional Inherited Members

Public Member Functions inherited from [cryptauthlib.library.AtcaStructure](#)

- None `__init__` (self, \*args, \*\*kwargs)
- def `from_definition` (cls)
- def `check_rationality` (cls)
- def `get_field_definition` (cls, str name)
- Any `__getattr__` (self, str name)
- def `__iter__` (self)
- def `__str__` (self)
- def `to_c_code` (self, name=None, \*\*kwargs)
- def `update_from_buffer` (self, buffer)

### 21.101.1 Detailed Description

ATSHA204A Config Zone Definition

### 21.101.2 Field Documentation

#### 21.101.2.1 `_fields_`

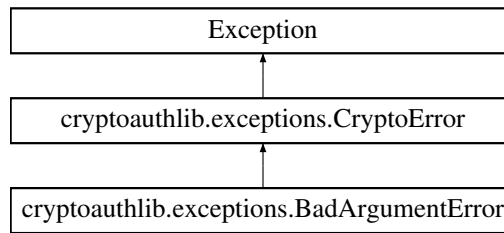
```
list cryptauthlib.device.Atsha204aConfig._fields_ [static], [protected]
```

**Initial value:**

```
= [ ('SN03', c_uint8*4),
    ('RevNum', c_uint8*4),
    ('SN48', c_uint8*5),
    ('Reserved13', c_uint8),
    ('I2C_Enable', I2cEnable),
    ('Reserved15', c_uint8),
    ('I2C_Address', c_uint8),
    ('CheckMacConfig', c_uint8),
    ('OTPMode', c_uint8),
    ('SelectorMode', c_uint8),
    ('SlotConfig', SlotConfig*16),
    ('Counter', Counter204*8),
    ('LastKeyUse', c_uint8*16),
    ('UserExtra', c_uint8),
    ('Selector', c_uint8),
    ('LockValue', c_uint8),
    ('LockConfig', c_uint8)]
```

## 21.102 cryptoauthlib.exceptions.BadArgumentError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.BadArgumentError:

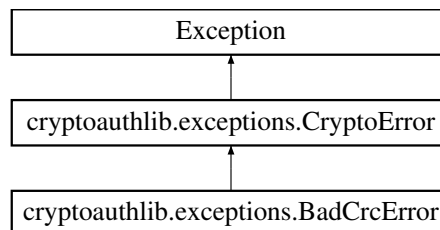


### 21.102.1 Detailed Description

bad argument (out of range, null pointer, etc.)

## 21.103 cryptoauthlib.exceptions.BadCrcError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.BadCrcError:

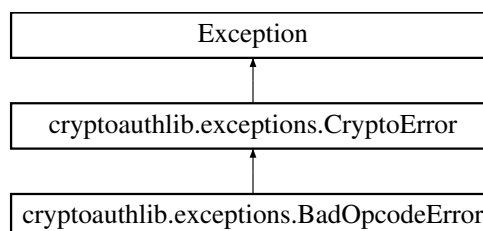


### 21.103.1 Detailed Description

incorrect CRC received

## 21.104 cryptoauthlib.exceptions.BadOpcodeError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.BadOpcodeError:



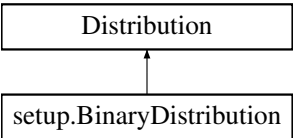


21.104.1 Detailed Description

Opcode is not supported by the device

21.105 setup.BinaryDistribution Class Reference

Inheritance diagram for setup.BinaryDistribution:



Public Member Functions

- def has\_ext\_modules (self)

21.106 cal\_buffer\_s Struct Reference

Data Fields

- size\_t len
- uint8\_t \* buf

21.106.1 Field Documentation

21.106.1.1 buf

uint8\_t\* cal\_buffer\_s::buf

Pointer to the actual buffer

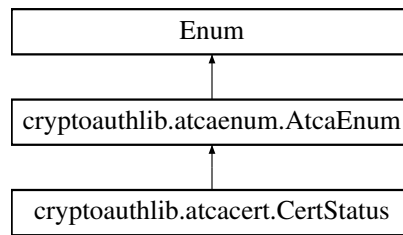
21.106.1.2 len

size\_t cal\_buffer\_s::len

Length of the provided buffer

## 21.107 cryptoauthlib.atcacert.CertStatus Class Reference

Inheritance diagram for cryptoauthlib.atcacert.CertStatus:



### Static Public Attributes

- int **ATCACERT\_E\_SUCCESS** = 0
- int **ATCACERT\_E\_ERROR** = 1
- int **ATCACERT\_E\_BAD\_PARAMS** = 2
- int **ATCACERT\_E\_BUFFER\_TOO\_SMALL** = 3
- int **ATCACERT\_E\_DECODING\_ERROR** = 4
- int **ATCACERT\_E\_INVALID\_DATE** = 5
- int **ATCACERT\_E\_UNIMPLEMENTED** = 6
- int **ATCACERT\_E\_UNEXPECTED\_ELEM\_SIZE** = 7
- int **ATCACERT\_E\_ELEM\_MISSING** = 8
- int **ATCACERT\_E\_ELEM\_OUT\_OF\_BOUNDS** = 9
- int **ATCACERT\_E\_BAD\_CERT** = 10
- int **ATCACERT\_E\_WRONG\_CERT\_DEF** = 11
- int **ATCACERT\_E\_VERIFY\_FAILED** = 12

### Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

- def **\_\_str\_\_** (self)
- def **\_\_eq\_\_** (self, other)
- def **\_\_ne\_\_** (self, other)
- def **\_\_int\_\_** (self)
- def **\_\_hash\_\_** (self)

Data Fields inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

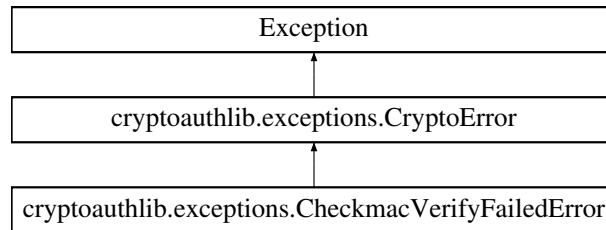
- **name**
- **value**

### 21.107.1 Detailed Description

Status codes returned from atcacert commands and their meanings. From atcacert.h

## 21.108 cryptauthlib.exceptions.CheckmacVerifyFailedError Class Reference

Inheritance diagram for cryptauthlib.exceptions.CheckmacVerifyFailedError:

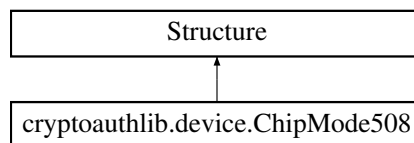


### 21.108.1 Detailed Description

response status byte indicates CheckMac failure (status byte = 0x01)

## 21.109 cryptauthlib.device.ChipMode508 Class Reference

Inheritance diagram for cryptauthlib.device.ChipMode508:



### Static Protected Attributes

- list [\\_fields\\_](#)
- int [\\_pack\\_](#) = 1

### 21.109.1 Detailed Description

ChipMode for 508 Field Definition

### 21.109.2 Field Documentation

#### 21.109.2.1 [\\_fields\\_](#)

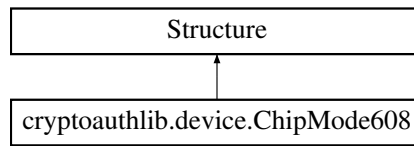
list cryptauthlib.device.ChipMode508.[\\_fields\\_](#) [static], [protected]

**Initial value:**

```
= [ ('UserExtraAdd', c_uint8, 1),
    ('TTLenable', c_uint8, 1),
    ('WatchdogDuration', c_uint8, 1)]
```

## 21.110 cryptauthlib.device.ChipMode608 Class Reference

Inheritance diagram for cryptauthlib.device.ChipMode608:



### Static Protected Attributes

- list [\\_fields\\_](#)
- int [\\_pack\\_](#) = 1

#### 21.110.1 Detailed Description

ChipMode for 608 Field Definition

#### 21.110.2 Field Documentation

##### 21.110.2.1 [\\_fields\\_](#)

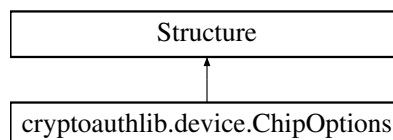
```
list cryptauthlib.device.ChipMode608._fields_ [static], [protected]
```

**Initial value:**

```
= [('UserExtraAdd', c_uint8, 1),  
    ('TTLenable', c_uint8, 1),  
    ('WatchdogDuration', c_uint8, 1),  
    ('ClockDivider', c_uint8, 5)]
```

## 21.111 cryptauthlib.device.ChipOptions Class Reference

Inheritance diagram for cryptauthlib.device.ChipOptions:



### Static Protected Attributes

- list [\\_fields\\_](#)
- int [\\_pack\\_](#) = 1

### 21.111.1 Detailed Description

ChipOptions Field Definition

### 21.111.2 Field Documentation

#### 21.111.2.1 `_fields_`

```
list cryptoauthlib.device.ChipOptions._fields_ [static], [protected]
```

**Initial value:**

```
= [ ('PowerOnSelfTest', c_uint16, 1),
    ('IoProtectionKeyEnable', c_uint16, 1),
    ('KdfAesEnable', c_uint16, 1),
    ('AutoClearFirstFail', c_uint16, 1),
    ('Reserved', c_uint16, 4),
    ('EcdhProtectionBits', c_uint16, 2),
    ('KdfProtectionBits', c_uint16, 2),
    ('IoProtectionKey', c_uint16, 4)]
```

## 21.112 CK\_AES\_CBC\_ENCRYPT\_DATA\_PARAMS Struct Reference

### Data Fields

- CK\_BYTE iv [16]
- CK\_BYTE\_PTR pData
- CK\_ULONG length

## 21.113 CK\_AES\_CCM\_PARAMS Struct Reference

### Data Fields

- CK\_ULONG ulDataLen
- CK\_BYTE\_PTR pNonce
- CK\_ULONG ulNonceLen
- CK\_BYTE\_PTR pAAD
- CK\_ULONG ulAADLen
- CK\_ULONG ulMACLen

## 21.114 CK\_AES\_CTR\_PARAMS Struct Reference

### Data Fields

- CK\_ULONG ulCounterBits
- CK\_BYTE cb [16]

## 21.115 CK\_AES\_GCM\_PARAMS Struct Reference

### Data Fields

- CK\_BYTE\_PTR **plv**
- CK\_ULONG **ulIvLen**
- CK\_ULONG **ulIvBits**
- CK\_BYTE\_PTR **pAAD**
- CK\_ULONG **ulAADLen**
- CK\_ULONG **ulTagBits**

## 21.116 CK\_ARIA\_CBC\_ENCRYPT\_DATA\_PARAMS Struct Reference

### Data Fields

- CK\_BYTE **iv** [16]
- CK\_BYTE\_PTR **pData**
- CK\_ULONG **length**

## 21.117 CK\_ATTRIBUTE Struct Reference

### Data Fields

- CK\_ATTRIBUTE\_TYPE **type**
- CK\_VOID\_PTR **pValue**
- CK\_ULONG **ulValueLen**

## 21.118 CK\_C\_INITIALIZE\_ARGS Struct Reference

### Data Fields

- CK\_CREATEMUTEX **CreateMutex**
- CK\_DESTROYMUTEX **DestroyMutex**
- CK\_LOCKMUTEX **LockMutex**
- CK\_UNLOCKMUTEX **UnlockMutex**
- CK\_FLAGS **flags**
- CK\_VOID\_PTR **pReserved**

## 21.119 CK\_CAMELLIA\_CBC\_ENCRYPT\_DATA\_PARAMS Struct Reference

### Data Fields

- CK\_BYTE **iv** [16]
- CK\_BYTE\_PTR **pData**
- CK\_ULONG **length**

## 21.120 CK\_CAMELLIA\_CTR\_PARAMS Struct Reference

### Data Fields

- CK\_ULONG **ulCounterBits**
- CK\_BYTE **cb** [16]

## 21.121 CK\_CCM\_PARAMS Struct Reference

### Data Fields

- CK\_ULONG **ulDataLen**
- CK\_BYTE\_PTR **pNonce**
- CK\_ULONG **ulNonceLen**
- CK\_BYTE\_PTR **pAAD**
- CK\_ULONG **ulAADLen**
- CK\_ULONG **ulMACLen**

## 21.122 CK\_CMS\_SIG\_PARAMS Struct Reference

### Data Fields

- CK\_OBJECT\_HANDLE **certificateHandle**
- CK\_MECHANISM\_PTR **pSigningMechanism**
- CK\_MECHANISM\_PTR **pDigestMechanism**
- CK\_UTF8CHAR\_PTR **pContentType**
- CK\_BYTE\_PTR **pRequestedAttributes**
- CK\_ULONG **ulRequestedAttributesLen**
- CK\_BYTE\_PTR **pRequiredAttributes**
- CK\_ULONG **ulRequiredAttributesLen**

## 21.123 CK\_DATE Struct Reference

### Data Fields

- CK\_CHAR **year** [4]
- CK\_CHAR **month** [2]
- CK\_CHAR **day** [2]

## 21.124 CK\_DES\_CBC\_ENCRYPT\_DATA\_PARAMS Struct Reference

### Data Fields

- CK\_BYTE **iv** [8]
- CK\_BYTE\_PTR **pData**
- CK\_ULONG **length**

## 21.125 CK\_DSA\_PARAMETER\_GEN\_PARAM Struct Reference

### Data Fields

- CK\_MECHANISM\_TYPE **hash**
- CK\_BYTE\_PTR **pSeed**
- CK\_ULONG **ulSeedLen**
- CK\_ULONG **ulIndex**

## 21.126 CK\_ECDH1\_DERIVE\_PARAMS Struct Reference

### Data Fields

- CK\_EC\_KDF\_TYPE **kdf**
- CK\_ULONG **ulSharedDataLen**
- CK\_BYTE\_PTR **pSharedData**
- CK\_ULONG **ulPublicDataLen**
- CK\_BYTE\_PTR **pPublicData**

## 21.127 CK\_ECDH2\_DERIVE\_PARAMS Struct Reference

### Data Fields

- CK\_EC\_KDF\_TYPE **kdf**
- CK\_ULONG **ulSharedDataLen**
- CK\_BYTE\_PTR **pSharedData**
- CK\_ULONG **ulPublicDataLen**
- CK\_BYTE\_PTR **pPublicData**
- CK\_ULONG **ulPrivateDataLen**
- CK\_OBJECT\_HANDLE **hPrivateData**
- CK\_ULONG **ulPublicDataLen2**
- CK\_BYTE\_PTR **pPublicData2**

## 21.128 CK\_ECDH\_AES\_KEY\_WRAP\_PARAMS Struct Reference

### Data Fields

- CK\_ULONG **ulAESKeyBits**
- CK\_EC\_KDF\_TYPE **kdf**
- CK\_ULONG **ulSharedDataLen**
- CK\_BYTE\_PTR **pSharedData**



## 21.129 CK\_ECMQV\_DERIVE\_PARAMS Struct Reference

### Data Fields

- CK\_EC\_KDF\_TYPE **kdf**
- CK\_ULONG **ulSharedDataLen**
- CK\_BYTE\_PTR **pSharedData**
- CK\_ULONG **ulPublicDataLen**
- CK\_BYTE\_PTR **pPublicData**
- CK\_ULONG **ulPrivateDataLen**
- CK\_OBJECT\_HANDLE **hPrivateData**
- CK\_ULONG **ulPublicDataLen2**
- CK\_BYTE\_PTR **pPublicData2**
- CK\_OBJECT\_HANDLE **publicKey**

## 21.130 CK\_FUNCTION\_LIST Struct Reference

### Data Fields

- [CK\\_VERSION](#) **version**

## 21.131 CK\_GCM\_PARAMS Struct Reference

### Data Fields

- CK\_BYTE\_PTR **pIv**
- CK\_ULONG **ulIvLen**
- CK\_ULONG **ulIvBits**
- CK\_BYTE\_PTR **pAAD**
- CK\_ULONG **ulAADLen**
- CK\_ULONG **ulTagBits**

## 21.132 CK\_GOSTR3410\_DERIVE\_PARAMS Struct Reference

### Data Fields

- CK\_EC\_KDF\_TYPE **kdf**
- CK\_BYTE\_PTR **pPublicData**
- CK\_ULONG **ulPublicDataLen**
- CK\_BYTE\_PTR **pUKM**
- CK\_ULONG **ulUKMLen**

## 21.133 CK\_GOSTR3410\_KEY\_WRAP\_PARAMS Struct Reference

### Data Fields

- CK\_BYTE\_PTR pWrapOID
- CK\_ULONG ulWrapOIDLen
- CK\_BYTE\_PTR pUKM
- CK\_ULONG ulUKMLen
- CK\_OBJECT\_HANDLE hKey

## 21.134 CK\_INFO Struct Reference

### Data Fields

- [CK\\_VERSION](#) cryptokiVersion
- CK\_UTF8CHAR manufacturerID [32]
- CK\_FLAGS flags
- CK\_UTF8CHAR libraryDescription [32]
- [CK\\_VERSION](#) libraryVersion

## 21.135 CK\_KEA\_DERIVE\_PARAMS Struct Reference

### Data Fields

- CK\_BBOOL isSender
- CK\_ULONG ulRandomLen
- CK\_BYTE\_PTR pRandomA
- CK\_BYTE\_PTR pRandomB
- CK\_ULONG ulPublicDataLen
- CK\_BYTE\_PTR pPublicData

## 21.136 CK\_KEY\_DERIVATION\_STRING\_DATA Struct Reference

### Data Fields

- CK\_BYTE\_PTR pData
- CK\_ULONG ulLen

## 21.137 CK\_KEY\_WRAP\_SET\_OAEP\_PARAMS Struct Reference

### Data Fields

- CK\_BYTE bBC
- CK\_BYTE\_PTR pX
- CK\_ULONG ulXLen

## 21.138 CK\_KIP\_PARAMS Struct Reference

### Data Fields

- CK\_MECHANISM\_PTR **pMechanism**
- CK\_OBJECT\_HANDLE **hKey**
- CK\_BYTE\_PTR **pSeed**
- CK\_ULONG **ulSeedLen**

## 21.139 CK\_MECHANISM Struct Reference

### Data Fields

- CK\_MECHANISM\_TYPE **mechanism**
- CK\_VOID\_PTR **pParameter**
- CK\_ULONG **ulParameterLen**

## 21.140 CK\_MECHANISM\_INFO Struct Reference

### Data Fields

- CK\_ULONG **ulMinKeySize**
- CK\_ULONG **ulMaxKeySize**
- CK\_FLAGS **flags**

## 21.141 CK\_OTP\_PARAM Struct Reference

### Data Fields

- CK\_OTP\_PARAM\_TYPE **type**
- CK\_VOID\_PTR **pValue**
- CK\_ULONG **ulValueLen**

## 21.142 CK\_OTP\_PARAMS Struct Reference

### Data Fields

- CK\_OTP\_PARAM\_PTR **pParams**
- CK\_ULONG **ulCount**

## 21.143 CK\_OTP\_SIGNATURE\_INFO Struct Reference

### Data Fields

- CK\_OTP\_PARAM\_PTR **pParams**
- CK\_ULONG **ulCount**

## 21.144 CK\_PBE\_PARAMS Struct Reference

### Data Fields

- CK\_BYTE\_PTR **pInitVector**
- CK\_UTF8CHAR\_PTR **pPassword**
- CK\_ULONG **ulPasswordLen**
- CK\_BYTE\_PTR **pSalt**
- CK\_ULONG **ulSaltLen**
- CK\_ULONG **ullIteration**

## 21.145 CK\_PKCS5\_PBKD2\_PARAMS Struct Reference

### Data Fields

- CK\_PKCS5\_PBKDF2\_SALT\_SOURCE\_TYPE **saltSource**
- CK\_VOID\_PTR **pSaltSourceData**
- CK\_ULONG **ulSaltSourceDataLen**
- CK\_ULONG **iterations**
- CK\_PKCS5\_PBKD2\_PSEUDO\_RANDOM\_FUNCTION\_TYPE **prf**
- CK\_VOID\_PTR **pPrfData**
- CK\_ULONG **ulPrfDataLen**
- CK\_UTF8CHAR\_PTR **pPassword**
- CK\_ULONG\_PTR **ulPasswordLen**

## 21.146 CK\_PKCS5\_PBKD2\_PARAMS2 Struct Reference

### Data Fields

- CK\_PKCS5\_PBKDF2\_SALT\_SOURCE\_TYPE **saltSource**
- CK\_VOID\_PTR **pSaltSourceData**
- CK\_ULONG **ulSaltSourceDataLen**
- CK\_ULONG **iterations**
- CK\_PKCS5\_PBKD2\_PSEUDO\_RANDOM\_FUNCTION\_TYPE **prf**
- CK\_VOID\_PTR **pPrfData**
- CK\_ULONG **ulPrfDataLen**
- CK\_UTF8CHAR\_PTR **pPassword**
- CK\_ULONG **ulPasswordLen**

## 21.147 CK\_RC2\_CBC\_PARAMS Struct Reference

### Data Fields

- CK\_ULONG **ulEffectiveBits**
- CK\_BYTE **iv** [8]

## 21.148 CK\_RC2\_MAC\_GENERAL\_PARAMS Struct Reference

### Data Fields

- CK\_ULONG **ulEffectiveBits**
- CK\_ULONG **ulMacLength**

## 21.149 CK\_RC5\_CBC\_PARAMS Struct Reference

### Data Fields

- CK\_ULONG **ulWordsize**
- CK\_ULONG **ulRounds**
- CK\_BYTE\_PTR **pIv**
- CK\_ULONG **ulIvLen**

## 21.150 CK\_RC5\_MAC\_GENERAL\_PARAMS Struct Reference

### Data Fields

- CK\_ULONG **ulWordsize**
- CK\_ULONG **ulRounds**
- CK\_ULONG **ulMacLength**

## 21.151 CK\_RC5\_PARAMS Struct Reference

### Data Fields

- CK\_ULONG **ulWordsize**
- CK\_ULONG **ulRounds**

## 21.152 CK\_RSA\_AES\_KEY\_WRAP\_PARAMS Struct Reference

### Data Fields

- CK\_ULONG **ulAESKeyBits**
- CK\_RSA\_PKCS\_OAEP\_PARAMS\_PTR **pOAEPParams**

## 21.153 CK\_RSA\_PKCS\_OAEP\_PARAMS Struct Reference

### Data Fields

- CK\_MECHANISM\_TYPE **hashAlg**
- CK\_RSA\_PKCS\_MGF\_TYPE **mgf**
- CK\_RSA\_PKCS\_OAEP\_SOURCE\_TYPE **source**
- CK\_VOID\_PTR **pSourceData**
- CK\_ULONG **ulSourceDataLen**

## 21.154 CK\_RSA\_PKCS\_PSS\_PARAMS Struct Reference

### Data Fields

- CK\_MECHANISM\_TYPE **hashAlg**
- CK\_RSA\_PKCS\_MGF\_TYPE **mgf**
- CK\_ULONG **sLen**

## 21.155 CK\_SEED\_CBC\_ENCRYPT\_DATA\_PARAMS Struct Reference

### Data Fields

- CK\_BYTE **iv** [16]
- CK\_BYTE\_PTR **pData**
- CK\_ULONG **length**

## 21.156 CK\_SESSION\_INFO Struct Reference

### Data Fields

- CK\_SLOT\_ID **slotID**
- CK\_STATE **state**
- CK\_FLAGS **flags**
- CK\_ULONG **ulDeviceError**

## 21.157 CK\_SKIPJACK\_PRIVATE\_WRAP\_PARAMS Struct Reference

### Data Fields

- CK\_ULONG **ulPasswordLen**
- CK\_BYTE\_PTR **pPassword**
- CK\_ULONG **ulPublicDataLen**
- CK\_BYTE\_PTR **pPublicData**
- CK\_ULONG **ulPAndGLen**
- CK\_ULONG **ulQLen**
- CK\_ULONG **ulRandomLen**
- CK\_BYTE\_PTR **pRandomA**
- CK\_BYTE\_PTR **pPrimeP**
- CK\_BYTE\_PTR **pBaseG**
- CK\_BYTE\_PTR **pSubprimeQ**

## 21.158 CK\_SKIPJACK\_RELAYX\_PARAMS Struct Reference

### Data Fields

- CK\_ULONG **ulOldWrappedXLen**
- CK\_BYTE\_PTR **pOldWrappedX**
- CK\_ULONG **ulOldPasswordLen**
- CK\_BYTE\_PTR **pOldPassword**
- CK\_ULONG **ulOldPublicDataLen**
- CK\_BYTE\_PTR **pOldPublicData**
- CK\_ULONG **ulOldRandomLen**
- CK\_BYTE\_PTR **pOldRandomA**
- CK\_ULONG **ulNewPasswordLen**
- CK\_BYTE\_PTR **pNewPassword**
- CK\_ULONG **ulNewPublicDataLen**
- CK\_BYTE\_PTR **pNewPublicData**
- CK\_ULONG **ulNewRandomLen**
- CK\_BYTE\_PTR **pNewRandomA**

## 21.159 CK\_SLOT\_INFO Struct Reference

### Data Fields

- CK\_UTF8CHAR **slotDescription** [64]
- CK\_UTF8CHAR **manufacturerID** [32]
- CK\_FLAGS **flags**
- [CK\\_VERSION](#) **hardwareVersion**
- [CK\\_VERSION](#) **firmwareVersion**

## 21.160 CK\_SSL3\_KEY\_MAT\_OUT Struct Reference

### Data Fields

- CK\_OBJECT\_HANDLE **hClientMacSecret**
- CK\_OBJECT\_HANDLE **hServerMacSecret**
- CK\_OBJECT\_HANDLE **hClientKey**
- CK\_OBJECT\_HANDLE **hServerKey**
- CK\_BYTE\_PTR **pIVClient**
- CK\_BYTE\_PTR **pIVServer**

## 21.161 CK\_SSL3\_KEY\_MAT\_PARAMS Struct Reference

### Data Fields

- CK\_ULONG **ulMacSizeInBits**
- CK\_ULONG **ulKeySizeInBits**
- CK\_ULONG **ulIVSizeInBits**
- CK\_BBOOL **blsExport**
- [CK\\_SSL3\\_RANDOM\\_DATA](#) **RandomInfo**
- CK\_SSL3\_KEY\_MAT\_OUT\_PTR **pReturnedKeyMaterial**

## 21.162 CK\_SSL3\_MASTER\_KEY\_DERIVE\_PARAMS Struct Reference

### Data Fields

- [CK\\_SSL3\\_RANDOM\\_DATA](#) RandomInfo
- CK\_VERSION\_PTR pVersion

## 21.163 CK\_SSL3\_RANDOM\_DATA Struct Reference

### Data Fields

- CK\_BYTE\_PTR pClientRandom
- CK\_ULONG ulClientRandomLen
- CK\_BYTE\_PTR pServerRandom
- CK\_ULONG ulServerRandomLen

## 21.164 CK\_TLS12\_KEY\_MAT\_PARAMS Struct Reference

### Data Fields

- CK\_ULONG ulMacSizeInBits
- CK\_ULONG ulKeySizeInBits
- CK\_ULONG ulIVSizeInBits
- CK\_BBOOL bIsExport
- [CK\\_SSL3\\_RANDOM\\_DATA](#) RandomInfo
- CK\_SSL3\_KEY\_MAT\_OUT\_PTR pReturnedKeyMaterial
- CK\_MECHANISM\_TYPE prfHashMechanism

## 21.165 CK\_TLS12\_MASTER\_KEY\_DERIVE\_PARAMS Struct Reference

### Data Fields

- [CK\\_SSL3\\_RANDOM\\_DATA](#) RandomInfo
- CK\_VERSION\_PTR pVersion
- CK\_MECHANISM\_TYPE prfHashMechanism

## 21.166 CK\_TLS\_KDF\_PARAMS Struct Reference

### Data Fields

- CK\_MECHANISM\_TYPE prfMechanism
- CK\_BYTE\_PTR pLabel
- CK\_ULONG ulLabelLength
- [CK\\_SSL3\\_RANDOM\\_DATA](#) RandomInfo
- CK\_BYTE\_PTR pContextData
- CK\_ULONG ulContextDataLength



## 21.167 CK\_TLS\_MAC\_PARAMS Struct Reference

### Data Fields

- CK\_MECHANISM\_TYPE **prfHashMechanism**
- CK\_ULONG **ulMacLength**
- CK\_ULONG **ulServerOrClient**

## 21.168 CK\_TLS\_PRF\_PARAMS Struct Reference

### Data Fields

- CK\_BYTE\_PTR **pSeed**
- CK\_ULONG **ulSeedLen**
- CK\_BYTE\_PTR **pLabel**
- CK\_ULONG **ulLabelLen**
- CK\_BYTE\_PTR **pOutput**
- CK\_ULONG\_PTR **pulOutputLen**

## 21.169 CK\_TOKEN\_INFO Struct Reference

### Data Fields

- CK\_UTF8CHAR **label** [32]
- CK\_UTF8CHAR **manufacturerID** [32]
- CK\_UTF8CHAR **model** [16]
- CK\_CHAR **serialNumber** [16]
- CK\_FLAGS **flags**
- CK\_ULONG **ulMaxSessionCount**
- CK\_ULONG **ulSessionCount**
- CK\_ULONG **ulMaxRwSessionCount**
- CK\_ULONG **ulRwSessionCount**
- CK\_ULONG **ulMaxPinLen**
- CK\_ULONG **ulMinPinLen**
- CK\_ULONG **ulTotalPublicMemory**
- CK\_ULONG **ulFreePublicMemory**
- CK\_ULONG **ulTotalPrivateMemory**
- CK\_ULONG **ulFreePrivateMemory**
- [CK\\_VERSION](#) **hardwareVersion**
- [CK\\_VERSION](#) **firmwareVersion**
- CK\_CHAR **utcTime** [16]

## 21.170 CK\_VERSION Struct Reference

### Data Fields

- CK\_BYTE **major**
- CK\_BYTE **minor**

## 21.171 CK\_WTLS\_KEY\_MAT\_OUT Struct Reference

### Data Fields

- CK\_OBJECT\_HANDLE **hMacSecret**
- CK\_OBJECT\_HANDLE **hKey**
- CK\_BYTE\_PTR **pIV**

## 21.172 CK\_WTLS\_KEY\_MAT\_PARAMS Struct Reference

### Data Fields

- CK\_MECHANISM\_TYPE **DigestMechanism**
- CK\_ULONG **ulMacSizeInBits**
- CK\_ULONG **ulKeySizeInBits**
- CK\_ULONG **ulIVSizeInBits**
- CK\_ULONG **ulSequenceNumber**
- CK\_BBOOL **blsExport**
- [CK\\_WTLS\\_RANDOM\\_DATA](#) **RandomInfo**
- CK\_WTLS\_KEY\_MAT\_OUT\_PTR **pReturnedKeyMaterial**

## 21.173 CK\_WTLS\_MASTER\_KEY\_DERIVE\_PARAMS Struct Reference

### Data Fields

- CK\_MECHANISM\_TYPE **DigestMechanism**
- [CK\\_WTLS\\_RANDOM\\_DATA](#) **RandomInfo**
- CK\_BYTE\_PTR **pVersion**

## 21.174 CK\_WTLS\_PRF\_PARAMS Struct Reference

### Data Fields

- CK\_MECHANISM\_TYPE **DigestMechanism**
- CK\_BYTE\_PTR **pSeed**
- CK\_ULONG **ulSeedLen**
- CK\_BYTE\_PTR **pLabel**
- CK\_ULONG **ulLabelLen**
- CK\_BYTE\_PTR **pOutput**
- CK\_ULONG\_PTR **pulOutputLen**

## 21.175 CK\_WTLS\_RANDOM\_DATA Struct Reference

### Data Fields

- CK\_BYTE\_PTR **pClientRandom**
- CK\_ULONG **ulClientRandomLen**
- CK\_BYTE\_PTR **pServerRandom**
- CK\_ULONG **ulServerRandomLen**

## 21.176 CK\_X9\_42\_DH1\_DERIVE\_PARAMS Struct Reference

### Data Fields

- CK\_X9\_42\_DH\_KDF\_TYPE **kdf**
- CK\_ULONG **ulOtherInfoLen**
- CK\_BYTE\_PTR **pOtherInfo**
- CK\_ULONG **ulPublicDataLen**
- CK\_BYTE\_PTR **pPublicData**

## 21.177 CK\_X9\_42\_DH2\_DERIVE\_PARAMS Struct Reference

### Data Fields

- CK\_X9\_42\_DH\_KDF\_TYPE **kdf**
- CK\_ULONG **ulOtherInfoLen**
- CK\_BYTE\_PTR **pOtherInfo**
- CK\_ULONG **ulPublicDataLen**
- CK\_BYTE\_PTR **pPublicData**
- CK\_ULONG **ulPrivateDataLen**
- CK\_OBJECT\_HANDLE **hPrivateData**
- CK\_ULONG **ulPublicDataLen2**
- CK\_BYTE\_PTR **pPublicData2**

## 21.178 CK\_X9\_42\_MQV\_DERIVE\_PARAMS Struct Reference

### Data Fields

- CK\_X9\_42\_DH\_KDF\_TYPE **kdf**
- CK\_ULONG **ulOtherInfoLen**
- CK\_BYTE\_PTR **pOtherInfo**
- CK\_ULONG **ulPublicDataLen**
- CK\_BYTE\_PTR **pPublicData**
- CK\_ULONG **ulPrivateDataLen**
- CK\_OBJECT\_HANDLE **hPrivateData**
- CK\_ULONG **ulPublicDataLen2**
- CK\_BYTE\_PTR **pPublicData2**
- CK\_OBJECT\_HANDLE **publicKey**

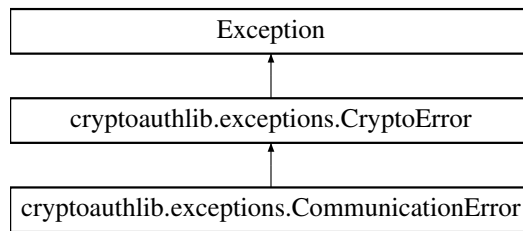
## 21.179 CL\_HashContext Struct Reference

### Data Fields

- uint32\_t **h** [20/4]
- uint32\_t **buf** [64/4]
- uint32\_t **byteCount**
- uint32\_t **byteCountHi**

## 21.180 cryptauthlib.exceptions.CommunicationError Class Reference

Inheritance diagram for cryptauthlib.exceptions.CommunicationError:

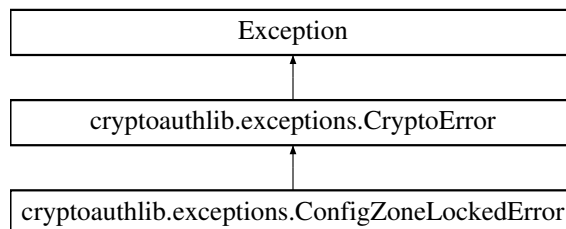


### 21.180.1 Detailed Description

Communication with device failed. Same as in hardware dependent modules.

## 21.181 cryptauthlib.exceptions.ConfigZoneLockedError Class Reference

Inheritance diagram for cryptauthlib.exceptions.ConfigZoneLockedError:

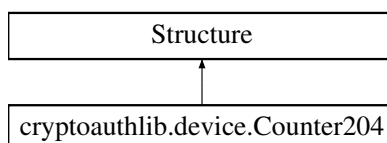


### 21.181.1 Detailed Description

Config Zone Locked

## 21.182 cryptauthlib.device.Counter204 Class Reference

Inheritance diagram for cryptauthlib.device.Counter204:



Static Protected Attributes

- list [\\_fields\\_](#)
- int `_pack_` = 1

21.182.1 Detailed Description

Counter Definition for SHA204

21.182.2 Field Documentation

21.182.2.1 `_fields_`

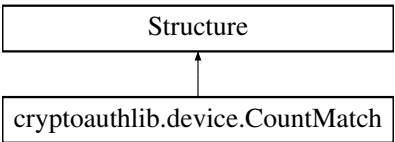
```
list cryptoauthlib.device.Counter204._fields_ [static], [protected]
```

Initial value:

```
= [ ('UseFlag', c_uint8),  
    ('UpdateCount', c_uint8)]
```

21.183 cryptoauthlib.device.CountMatch Class Reference

Inheritance diagram for cryptoauthlib.device.CountMatch:



Static Protected Attributes

- list [\\_fields\\_](#)
- int `_pack_` = 1

21.183.1 Detailed Description

CountMatch (608) Field Definition

21.183.2 Field Documentation

### 21.183.2.1 `_fields_`

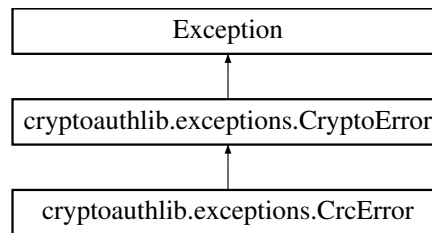
```
list cryptolib.device.CountMatch._fields_ [static], [protected]
```

#### Initial value:

```
= [ ('Enable', c_uint8, 1),  
    ('Reserved', c_uint8, 3),  
    ('CountMatchKey', c_uint8, 4)]
```

## 21.184 cryptolib.exceptions.CrcError Class Reference

Inheritance diagram for cryptolib.exceptions.CrcError:

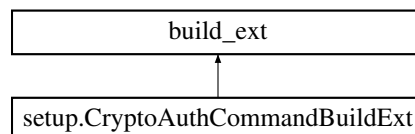


### 21.184.1 Detailed Description

response status byte indicates CRC error (status byte = 0xFF)

## 21.185 setup.CryptoAuthCommandBuildExt Class Reference

Inheritance diagram for setup.CryptoAuthCommandBuildExt:

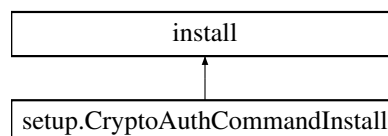


### Public Member Functions

- def **build\_extension** (self, ext)

## 21.186 setup.CryptoAuthCommandInstall Class Reference

Inheritance diagram for setup.CryptoAuthCommandInstall:

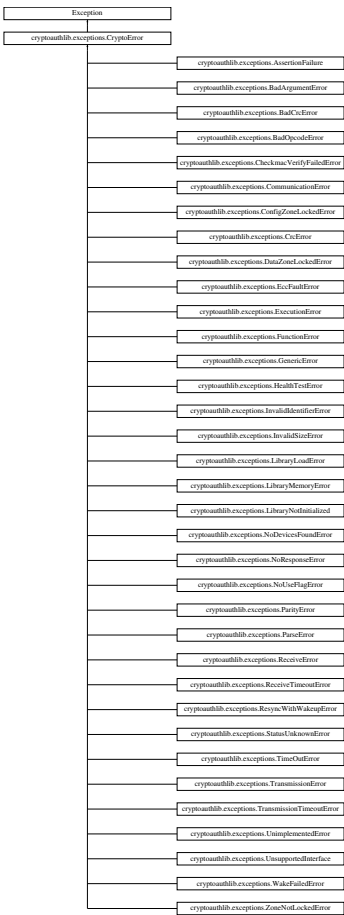


Public Member Functions

- def run (self)

21.187    cryptoauthlib.exceptions.CryptoError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.CryptoError:

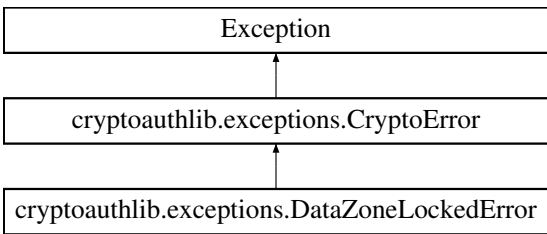


21.187.1    Detailed Description

Standard CryptoAuthLib Exceptions

21.188    cryptoauthlib.exceptions.DataZoneLockedError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.DataZoneLockedError:



### 21.188.1 Detailed Description

Configuration Enabled

## 21.189 device\_execution\_time\_t Struct Reference

Structure to hold the device execution time and the opcode for the corresponding command.

```
#include <lib/calib/calib_execution.h>
```

### Data Fields

- uint8\_t **opcode**
- uint16\_t **execution\_time\_msec**

### 21.189.1 Detailed Description

Structure to hold the device execution time and the opcode for the corresponding command.

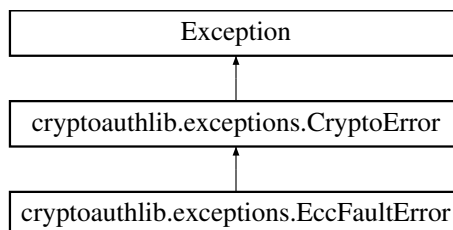
## 21.190 devtype\_names\_t Struct Reference

### Data Fields

- ATCADeviceType **devtype**
- const char \* **name**

## 21.191 cryptoauthlib.exceptions.EccFaultError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.EccFaultError:



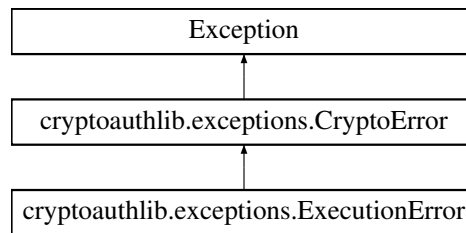
### 21.191.1 Detailed Description

response status byte is ECC fault (status byte = 0x05)



## 21.192 cryptoauthlib.exceptions.ExecutionError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.ExecutionError:

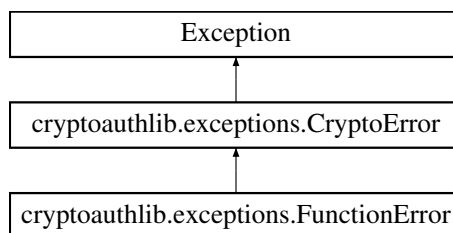


### 21.192.1 Detailed Description

chip was in a state where it could not execute the command, response status byte indicates command execution error (status byte = 0x0F)

## 21.193 cryptoauthlib.exceptions.FunctionError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.FunctionError:

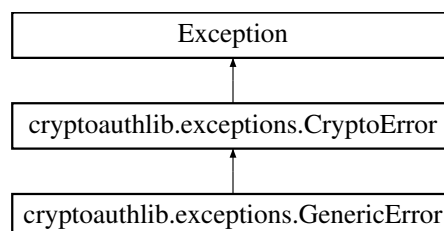


### 21.193.1 Detailed Description

Function could not execute due to incorrect condition / state.

## 21.194 cryptoauthlib.exceptions.GenericError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.GenericError:

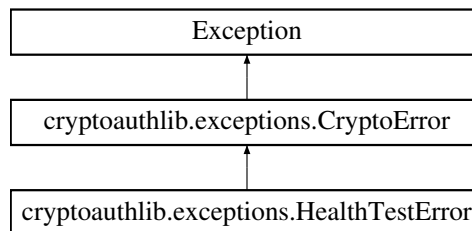


### 21.194.1 Detailed Description

`unspecified error`

## 21.195 `cryptoauthlib.exceptions.HealthTestError` Class Reference

Inheritance diagram for `cryptoauthlib.exceptions.HealthTestError`:

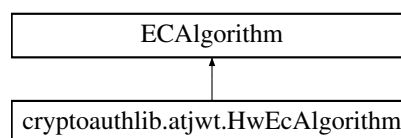


### 21.195.1 Detailed Description

`Random number generator health test error`

## 21.196 `cryptoauthlib.atjwt.HwEcAlgorithm` Class Reference

Inheritance diagram for `cryptoauthlib.atjwt.HwEcAlgorithm`:



### Public Member Functions

- `def __init__(self, hash_alg, slot, iface_cfg)`
- `def sign(self, msg, _)`

### Protected Attributes

- `_cfg`
- `_slot`

### 21.196.1 Detailed Description

`Extended Algorithm with hardware based elliptic curve support`

21.196.2 Member Function Documentation

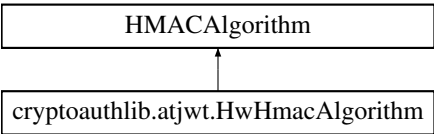
21.196.2.1 sign()

```
def cryptoauthlib.atjwt.HwEcAlgorithm.sign (
    self,
    msg,
    _ )
```

Return a signature of the JWT with hardware ECDSA

21.197 cryptoauthlib.atjwt.HwHmacAlgorithm Class Reference

Inheritance diagram for cryptoauthlib.atjwt.HwHmacAlgorithm:



Public Member Functions

- def `__init__` (self, hash\_alg, slot, iface\_cfg)
- def `sign` (self, msg, \_)
- def `verify` (self, msg, key, sig)

Protected Attributes

- `_cfg`
- `_slot`

21.197.1 Detailed Description

Extended Algorithm with hardware based HMAC support

21.197.2 Member Function Documentation

## 21.198 i2c\_sam0\_instance Struct Reference

---

### 21.197.2.1 sign()

```
def cryptoauthlib.atjwt.HwHmacAlgorithm.sign (
    self,
    msg,
    _ )
```

Return a signature of the JWT with hardware SHA256 HMAC and stored key

### 21.197.2.2 verify()

```
def cryptoauthlib.atjwt.HwHmacAlgorithm.verify (
    self,
    msg,
    key,
    sig )
```

Verify a signature using the software HMAC module

## 21.198 i2c\_sam0\_instance Struct Reference

### Data Fields

- struct i2c\_master\_module \* **i2c\_instance**
- sam0\_change\_baudrate **change\_baudrate**

## 21.199 i2c\_sam\_instance Struct Reference

### Data Fields

- Twi \* **i2c\_instance**
- sam\_change\_baudrate **change\_baudrate**

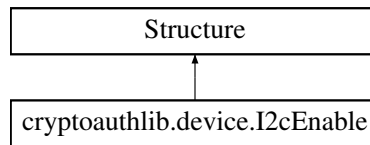
## 21.200 i2c\_start\_instance Struct Reference

### Data Fields

- struct i2c\_m\_sync\_desc \* **i2c\_descriptor**
- start\_change\_baudrate **change\_baudrate**

## 21.201 cryptauthlib.device.I2cEnable Class Reference

Inheritance diagram for cryptauthlib.device.I2cEnable:



### Static Protected Attributes

- list [\\_fields\\_](#)
- int [\\_pack\\_](#) = 1

#### 21.201.1 Detailed Description

I2C Enable Field Definition

#### 21.201.2 Field Documentation

##### 21.201.2.1 [\\_fields\\_](#)

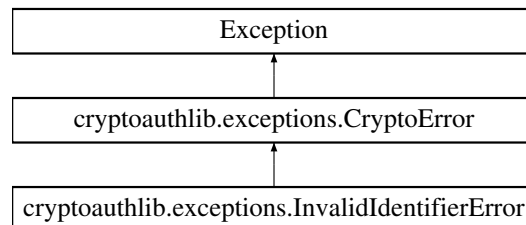
```
list cryptauthlib.device.I2cEnable._fields_ [static], [protected]
```

**Initial value:**

```
= [('Enable', c_uint8, 1),  
   ('Reserved', c_uint8, 6)]
```

## 21.202 cryptauthlib.exceptions.InvalidIdentifierError Class Reference

Inheritance diagram for cryptauthlib.exceptions.InvalidIdentifierError:

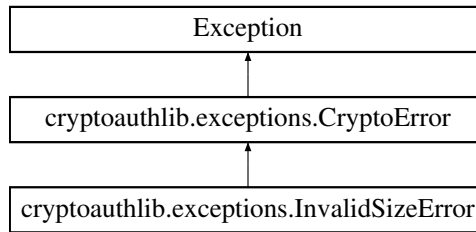


#### 21.202.1 Detailed Description

invalid device id, id not set

## 21.203 cryptauthlib.exceptions.InvalidSizeError Class Reference

Inheritance diagram for cryptauthlib.exceptions.InvalidSizeError:

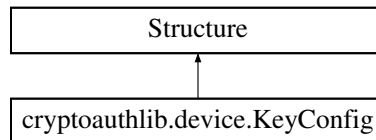


### 21.203.1 Detailed Description

Count value is out of range or greater than buffer size.

## 21.204 cryptauthlib.device.KeyConfig Class Reference

Inheritance diagram for cryptauthlib.device.KeyConfig:



### Static Protected Attributes

- list [\\_fields\\_](#)
- int [\\_pack\\_](#) = 1

### 21.204.1 Detailed Description

KeyConfig Field Definition

### 21.204.2 Field Documentation

21.204.2.1 `_fields_`

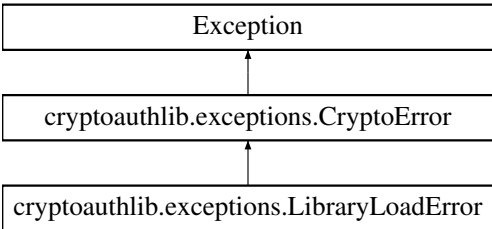
```
list cryptoauthlib.device.KeyConfig._fields_  [static], [protected]
```

Initial value:

```
=  [('Private', c_uint16, 1),
    ('PubInfo', c_uint16, 1),
    ('KeyType', c_uint16, 3),
    ('Lockable', c_uint16, 1),
    ('ReqRandom', c_uint16, 1),
    ('ReqAuth', c_uint16, 1),
    ('AuthKey', c_uint16, 4),
    ('PersistentDisable', c_uint16, 1),
    ('RFU', c_uint16, 1),
    ('X509id', c_uint16, 2)]
```

21.205 `cryptoauthlib.exceptions.LibraryLoadError` Class Reference

Inheritance diagram for `cryptoauthlib.exceptions.LibraryLoadError`:

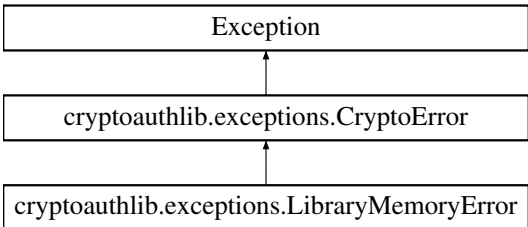


21.205.1 Detailed Description

```
CryptpAuthLib failed to Load
```

21.206 `cryptoauthlib.exceptions.LibraryMemoryError` Class Reference

Inheritance diagram for `cryptoauthlib.exceptions.LibraryMemoryError`:

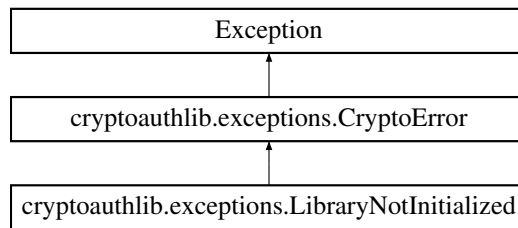


21.206.1 Detailed Description

```
CryptoAuthLib was unable to allocate memory
```

## 21.207 cryptoauthlib.exceptions.LibraryNotInitialized Class Reference

Inheritance diagram for cryptoauthlib.exceptions.LibraryNotInitialized:



### 21.207.1 Detailed Description

Indication that library or context was not initialized prior to an API call

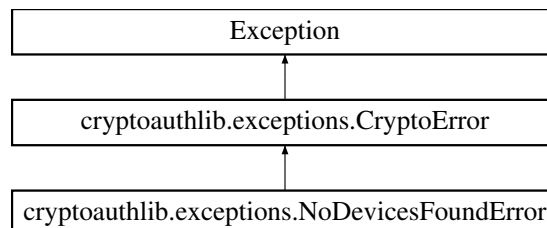
## 21.208 memory\_parameters Struct Reference

### Data Fields

- uint32\_t **start\_address**
- uint32\_t **memory\_size**
- uint32\_t **version\_info**
- uint8\_t **reserved** [52]
- uint8\_t **signature** [[ATCA\\_SIG\\_SIZE](#)]

## 21.209 cryptoauthlib.exceptions.NoDevicesFoundError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.NoDevicesFoundError:



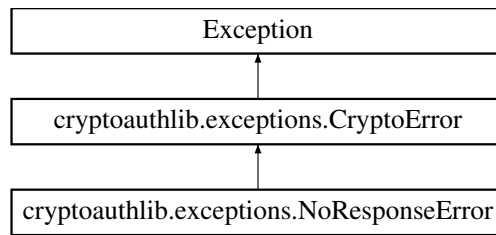
### 21.209.1 Detailed Description

For protocols that support device discovery (kit protocol), no devices were found



## 21.210 cryptoauthlib.exceptions.NoResponseError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.NoResponseError:

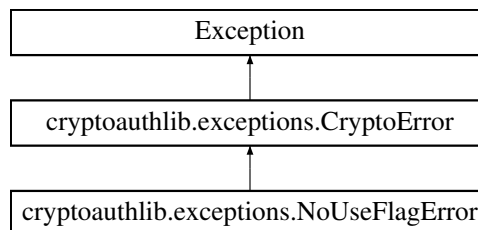


### 21.210.1 Detailed Description

error while the Command layer is polling for a command response.

## 21.211 cryptoauthlib.exceptions.NoUseFlagError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.NoUseFlagError:

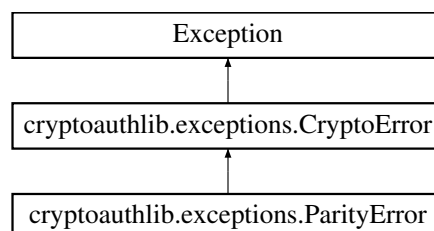


### 21.211.1 Detailed Description

Indication that no dk pk flag is available to perform

## 21.212 cryptoauthlib.exceptions.ParityError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.ParityError:

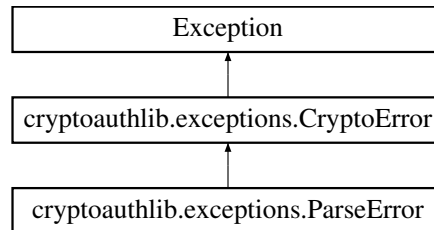


### 21.212.1 Detailed Description

`for protocols needing parity`

## 21.213 cryptoauthlib.exceptions.ParseError Class Reference

Inheritance diagram for `cryptoauthlib.exceptions.ParseError`:



### 21.213.1 Detailed Description

`response status byte indicates parsing error (status byte = 0x03)`

## 21.214 pkcs11\_mech\_table\_e Struct Reference

### Data Fields

- `CK_MECHANISM_TYPE` **type**
- `CK_MECHANISM_INFO` **info**

## 21.215 pkcs11\_attrib\_model\_s Struct Reference

### Data Fields

- `const CK_ATTRIBUTE_TYPE` **type**
- `const attrib_f` **func**

## 21.216 pkcs11\_conf\_filedata\_s Struct Reference

### Data Fields

- `bool` **initialized**
- `char` **filename** [MAX\_CONF\_FILE\_NAME\_SIZE]

## 21.217 `pkcs11_dev_ctx` Struct Reference

```
#include <lib/pkcs11/pkcs11_init.h>
```

### Data Fields

- `CK_SESSION_HANDLE session`

### 21.217.1 Detailed Description

Context Tracking Info

## 21.218 `pkcs11_dev_res` Struct Reference

```
#include <lib/pkcs11/pkcs11_init.h>
```

### Data Fields

- `pkcs11_dev_ctx contexts [(5u)]`

### 21.218.1 Detailed Description

Reservable Device Resources

## 21.219 `pkcs11_dev_state` Struct Reference

```
#include <lib/pkcs11/pkcs11_init.h>
```

### Data Fields

- `hal_mutex_t dev_lock`
- `pkcs11_dev_res resources [PKCS11_MAX_SLOTS_ALLOWED]`

### 21.219.1 Detailed Description

Device state tracker structure

### 21.219.2 Field Documentation

### 21.219.2.1 dev\_lock

`hal_mutex_t` `pkcs11_dev_state::dev_lock`

Lock to protect concurrent access to the device

### 21.219.2.2 resources

`pkcs11_dev_res` `pkcs11_dev_state::resources[PKCS11_MAX_SLOTS_ALLOWED]`

Track the usage of device resources

## 21.220 pkcs11\_ecc\_key\_info\_s Struct Reference

### Data Fields

- CK\_BYTE `ec_key_type`
- CK\_BYTE `oid_size`
- CK\_BYTE\_PTR `curve_oid`
- CK\_BYTE\_PTR `ec_asn1_header`
- CK\_BYTE\_PTR `ec_x962_asn1_header`
- uint16\_t `asn1_header_sz`
- CK\_ULONG `pubkey_sz`
- CK\_ULONG `min_msg_sz`
- CK\_ULONG `sig_sz`

## 21.221 pkcs11\_lib\_ctx\_s Struct Reference

```
#include <lib/pkcs11/pkcs11_init.h>
```

### Data Fields

- CK\_BBOOL `initialized`
- `CK_C_INITIALIZE_ARGS` `init_args`
- CK\_VOID\_PTR `lib_lock`
- `pkcs11_dev_state *` `dev_state`
- CK\_BBOOL `dev_lock_enabled`
- CK\_VOID\_PTR `slots`
- CK\_ULONG `slot_cnt`
- CK\_CHAR `config_path` [200]

### 21.221.1 Detailed Description

Library Context

## 21.221.2 Field Documentation

### 21.221.2.1 config\_path

```
CK_CHAR pkcs11_lib_ctx_s::config_path[200]
```

Filesystem path where the base config is located

### 21.221.2.2 dev\_lock\_enabled

```
CK_BBOOL pkcs11_lib_ctx_s::dev_lock_enabled
```

Flag to indicate if a device lock is enabled and configured

### 21.221.2.3 dev\_state

```
pkcs11_dev_state* pkcs11_lib_ctx_s::dev_state
```

Device State state and Lock (if configured)

### 21.221.2.4 init\_args

```
CK_C_INITIALIZE_ARGS pkcs11_lib_ctx_s::init_args
```

Arguments provided by the app for C\_Initialize

### 21.221.2.5 initialized

```
CK_BBOOL pkcs11_lib_ctx_s::initialized
```

Indicates that the library has been initialized

### 21.221.2.6 lib\_lock

```
CK_VOID_PTR pkcs11_lib_ctx_s::lib_lock
```

Application Lock for concurrent access to the library if the application will be using threads

### 21.221.2.7 slot\_cnt

```
CK_ULONG pkcs11_lib_ctx_s::slot_cnt
```

Number of configured slots

### 21.221.2.8 slots

`CK_VOID_PTR pkcs11_lib_ctx_s::slots`

Configured slots in the library

## 21.222 pkcs11\_object\_cache\_s Struct Reference

### Data Fields

- `CK_OBJECT_HANDLE` [handle](#)
- `CK_SLOT_ID` **slotid**
- `pkcs11_object_ptr` [object](#)

### 21.222.1 Field Documentation

#### 21.222.1.1 handle

`CK_OBJECT_HANDLE pkcs11_object_cache_s::handle`

Arbitrary (but unique) non-null identifier for an object

#### 21.222.1.2 object

`pkcs11_object_ptr pkcs11_object_cache_s::object`

The actual object

## 21.223 pkcs11\_object\_s Struct Reference

### Data Fields

- `CK_OBJECT_CLASS` [class\\_id](#)
- `CK_ULONG` [class\\_type](#)
- [pkcs11\\_attr\\_model](#) const \* [attributes](#)
- `CK_ULONG` [count](#)
- `CK_ULONG` **size**
- `uint16_t` **slot**
- `CK_FLAGS` **flags**
- `CK_UTF8CHAR` **name** [PKCS11\_MAX\_LABEL\_SIZE+1]
- `CK_VOID_PTR` **config**
- `CK_VOID_PTR` **data**
- `ta_element_attributes_t` **handle\_info**

## 21.223.1 Field Documentation

### 21.223.1.1 attributes

```
pkcs11_attrib_model const* pkcs11_object_s::attributes
```

List of attribute models this object possesses

### 21.223.1.2 class\_id

```
CK_OBJECT_CLASS pkcs11_object_s::class_id
```

The Class Identifier

### 21.223.1.3 class\_type

```
CK_ULONG pkcs11_object_s::class_type
```

The Class Type

### 21.223.1.4 count

```
CK_ULONG pkcs11_object_s::count
```

Count of attribute models

## 21.224 pkcs11\_session\_ctx\_s Struct Reference

```
#include <lib/pkcs11/pkcs11_session.h>
```

### Data Fields

- CK\_BBOOL **initialized**
- pkcs11\_slot\_ctx\_ptr **slot**
- CK\_SESSION\_HANDLE **handle**
- CK\_STATE **state**
- CK\_ULONG **error**
- CK\_ATTRIBUTE\_PTR **attrib\_list**
- CK\_ULONG **attrib\_count**
- CK\_ULONG **object\_index**
- CK\_ULONG **object\_count**
- CK\_OBJECT\_HANDLE **active\_object**
- CK\_MECHANISM\_TYPE **active\_mech**
- [pkcs11\\_session\\_mech\\_ctx](#) **active\_mech\_data**

### 21.224.1 Detailed Description

Session Context

## 21.225 pkcs11\_session\_mech\_ctx\_s Struct Reference

### Data Fields

- [atcac\\_hmac\\_ctx\\_t](#) **hmac**
- [atcac\\_sha2\\_256\\_ctx\\_t](#) **sha256**
- [atca\\_aes\\_cmac\\_ctx\\_t](#) **cmac**
- [atca\\_aes\\_cbc\\_ctx\\_t](#) **cbc**
- struct {  
    [atca\\_aes\\_gcm\\_ctx\\_t](#) **context**  
    CK\_BYTE **tag\_len**  
} **gcm**
- struct {  
    uint8\_t **iv** [TA\_AES\_GCM\_IV\_LENGTH]  
    uint8\_t **aad** [ATCA\_AES128\_BLOCK\_SIZE]  
    CK\_BYTE **aad\_len**  
} **gcm\_single**

## 21.226 pkcs11\_slot\_ctx\_s Struct Reference

```
#include <lib/pkcs11/pkcs11_slot.h>
```

### Data Fields

- CK\_BYTE **slot\_state**
- CK\_SLOT\_ID **slot\_id**
- [ATCADevice](#) **device\_ctx**
- [ATCAIfaceCfg](#) **interface\_config**
- CK\_SESSION\_HANDLE **session**
- [atecc608\\_config\\_t](#) **cfg\_zone**
- CK\_FLAGS **flags**
- uint16\_t **user\_pin\_handle**
- uint16\_t **so\_pin\_handle**
- CK\_UTF8CHAR **label** [PKCS11\_MAX\_LABEL\_SIZE+1]
- CK\_BBOOL **logged\_in**
- CK\_BYTE [read\\_key](#) [32]

### 21.226.1 Detailed Description

Slot Context



## 21.226.2 Field Documentation

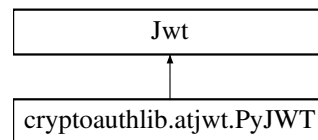
### 21.226.2.1 read\_key

`CK_BYTE pkcs11_slot_ctx_s::read_key[32]`

Accepted through C\_Login as the user pin

## 21.227 cryptoauthlib.atjwt.PyJWT Class Reference

Inheritance diagram for `cryptoauthlib.atjwt.PyJWT`:



### Public Member Functions

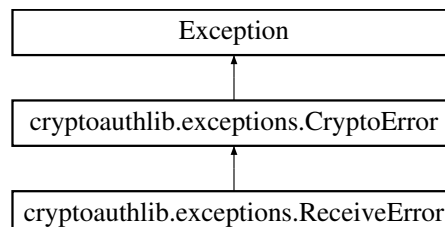
- `def __init__(self, slot=0, iface_cfg=None, options=None)`
- `def register_algorithm(self, alg_id, algorithm)`

### 21.227.1 Detailed Description

Extended PyJWT class from the pyjwt module

## 21.228 cryptoauthlib.exceptions.ReceiveError Class Reference

Inheritance diagram for `cryptoauthlib.exceptions.ReceiveError`:

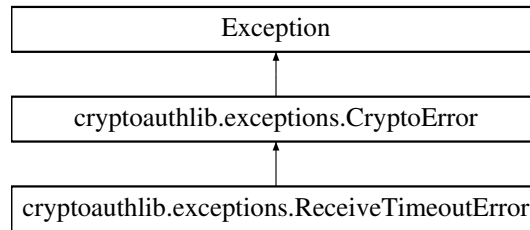


### 21.228.1 Detailed Description

Timed out while waiting for response. Number of bytes received is `> 0`.

## 21.229 cryptoauthlib.exceptions.ReceiveTimeoutError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.ReceiveTimeoutError:

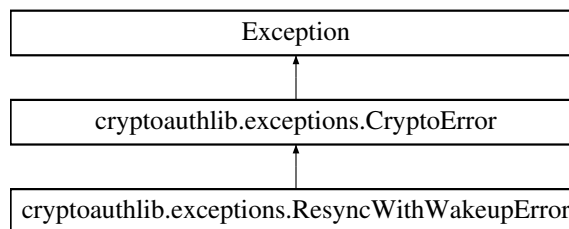


### 21.229.1 Detailed Description

for Microchip PHY protocol, timeout on receipt waiting for master

## 21.230 cryptoauthlib.exceptions.ResyncWithWakeupError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.ResyncWithWakeupError:



### 21.230.1 Detailed Description

Re-synchronization succeeded, but only after generating a Wake-up

## 21.231 secure\_boot\_config\_bits Struct Reference

### Data Fields

- uint16\_t **secure\_boot\_mode**: 2
- uint16\_t **secure\_boot\_reserved1**: 1
- uint16\_t **secure\_boot\_persistent\_enable**: 1
- uint16\_t **secure\_boot\_rand\_nonce**: 1
- uint16\_t **secure\_boot\_reserved2**: 3
- uint16\_t **secure\_boot\_sig\_dig**: 4
- uint16\_t **secure\_boot\_pub\_key**: 4

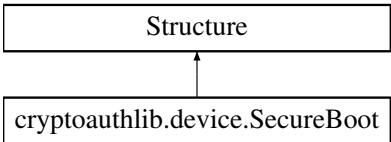
## 21.232 secure\_boot\_parameters Struct Reference

### Data Fields

- [memory\\_parameters](#) `memory_params`
- [atcac\\_sha2\\_256\\_ctx](#) `s_sha_context`
- `uint8_t app_digest` [ATCA\_SHA\_DIGEST\_SIZE]

## 21.233 cryptoauthlib.device.SecureBoot Class Reference

Inheritance diagram for `cryptoauthlib.device.SecureBoot`:



### Static Protected Attributes

- `list _fields_`
- `int _pack_ = 1`

### 21.233.1 Detailed Description

SecureBoot Field Definition

### 21.233.2 Field Documentation

#### 21.233.2.1 \_fields\_

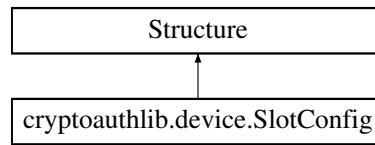
`list cryptoauthlib.device.SecureBoot._fields_ [static], [protected]`

**Initial value:**

```
= [ ('SecureBootMode', c_uint16, 2),
    ('Reserved0', c_uint16, 1),
    ('SecureBootPersistentEnable', c_uint16, 1),
    ('SecureBootRandNonce', c_uint16, 1),
    ('Reserved1', c_uint16, 3),
    ('SecureBootSigDig', c_uint16, 4),
    ('SecureBootPubKey', c_uint16, 4)]
```

## 21.234 cryptauthlib.device.SlotConfig Class Reference

Inheritance diagram for cryptauthlib.device.SlotConfig:



### Static Protected Attributes

- list `_fields_`
- int `_pack_` = 1

#### 21.234.1 Detailed Description

Slot Configuration Field Definition

#### 21.234.2 Field Documentation

##### 21.234.2.1 `_fields_`

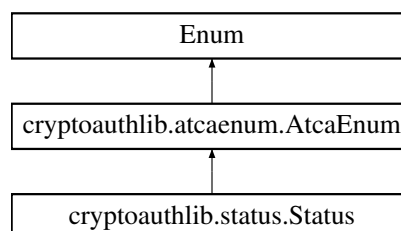
```
list cryptauthlib.device.SlotConfig._fields_ [static], [protected]
```

Initial value:

```
= [('ReadKey', c_uint16, 4),  
   ('NoMac', c_uint16, 1),  
   ('LimitedUse', c_uint16, 1),  
   ('EncryptRead', c_uint16, 1),  
   ('IsSecret', c_uint16, 1),  
   ('WriteKey', c_uint16, 4),  
   ('WriteConfig', c_uint16, 4)]
```

## 21.235 cryptauthlib.status.Status Class Reference

Inheritance diagram for cryptauthlib.status.Status:



## Static Public Attributes

- int **ATCA\_SUCCESS** = 0
- int **ATCA\_CONFIG\_ZONE\_LOCKED** = 0x01
- int **ATCA\_DATA\_ZONE\_LOCKED** = 0x02
- int **ATCA\_WAKE\_FAILED** = -48
- int **ATCA\_CHECKMAC\_VERIFY\_FAILED** = -47
- int **ATCA\_PARSE\_ERROR** = -46
- int **ATCA\_STATUS\_CRC** = -44
- int **ATCA\_STATUS\_UNKNOWN** = -43
- int **ATCA\_STATUS\_ECC** = -42
- int **ATCA\_STATUS\_SELFTEST\_ERROR** = -41
- int **ATCA\_FUNC\_FAIL** = -32
- int **ATCA\_GEN\_FAIL** = -31
- int **ATCA\_BAD\_PARAM** = -30
- int **ATCA\_INVALID\_ID** = -29
- int **ATCA\_INVALID\_SIZE** = -28
- int **ATCA\_BAD\_CRC** = -27
- int **ATCA\_RX\_FAIL** = -26
- int **ATCA\_RX\_NO\_RESPONSE** = -25
- int **ATCA\_RESYNC\_WITH\_WAKEUP** = -24
- int **ATCA\_PARITY\_ERROR** = -23
- int **ATCA\_TX\_TIMEOUT** = -22
- int **ATCA\_RX\_TIMEOUT** = -21
- int **ATCA\_COMM\_FAIL** = -16
- int **ATCA\_TIMEOUT** = -15
- int **ATCA\_BAD\_OPCODE** = -14
- int **ATCA\_WAKE\_SUCCESS** = -13
- int **ATCA\_EXECUTION\_ERROR** = -12
- int **ATCA\_UNIMPLEMENTED** = -11
- int **ATCA\_ASSERT\_FAILURE** = -10
- int **ATCA\_TX\_FAIL** = -9
- int **ATCA\_NOT\_LOCKED** = -8
- int **ATCA\_NO\_DEVICES** = -7
- int **ATCA\_HEALTH\_TEST\_ERROR** = -6
- int **ATCA\_ALLOC\_FAILURE** = -5
- int **ATCA\_USE\_FLAGS\_CONSUMED** = -4
- int **ATCA\_NOT\_INITIALIZED** = -3

## Additional Inherited Members

Public Member Functions inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

- def **\_\_str\_\_** (self)
- def **\_\_eq\_\_** (self, other)
- def **\_\_ne\_\_** (self, other)
- def **\_\_int\_\_** (self)
- def **\_\_hash\_\_** (self)

Data Fields inherited from [cryptoauthlib.atcaenum.AtcaEnum](#)

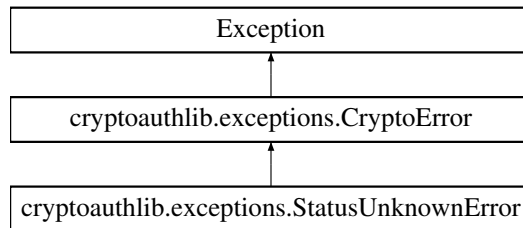
- **name**
- **value**

### 21.235.1 Detailed Description

Status codes returned from cryptoauthlib commands and their meanings. See `atca_status.h`

## 21.236 cryptoauthlib.exceptions.StatusUnknownError Class Reference

Inheritance diagram for `cryptoauthlib.exceptions.StatusUnknownError`:



### 21.236.1 Detailed Description

Response status byte is unknown

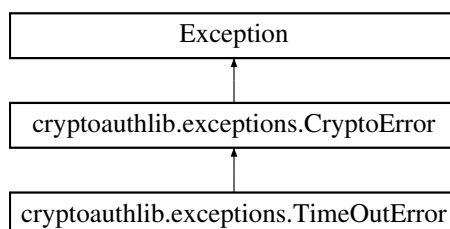
## 21.237 sw\_sha256\_ctx Struct Reference

### Data Fields

- `uint32_t total_msg_size`  
*Total number of message bytes processed.*
- `uint32_t block_size`  
*Number of bytes in current block.*
- `uint8_t block [(64) * 2]`  
*Unprocessed message storage.*
- `uint32_t hash [8]`  
*Hash state.*

## 21.238 cryptoauthlib.exceptions.TimeoutError Class Reference

Inheritance diagram for `cryptoauthlib.exceptions.TimeoutError`:



21.238.1 Detailed Description

Timed out while waiting for response. Number of bytes received is 0.

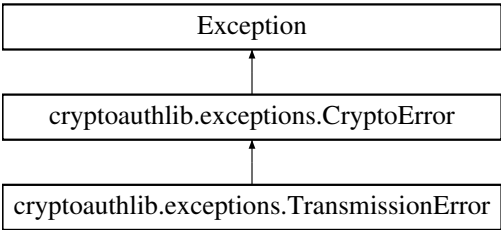
21.239 tng\_cert\_map\_element Struct Reference

Data Fields

- const char \* **otpcode**
- const [atcacert\\_def\\_t](#) \* **cert\_def**

21.240 cryptoauthlib.exceptions.TransmissionError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.TransmissionError:

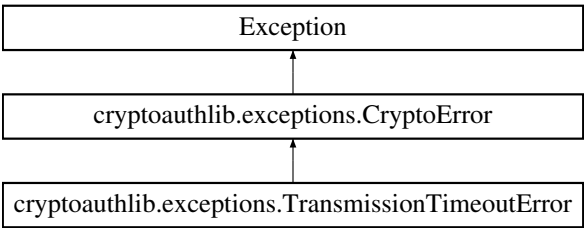


21.240.1 Detailed Description

Failed to write

21.241 cryptoauthlib.exceptions.TransmissionTimeoutError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.TransmissionTimeoutError:

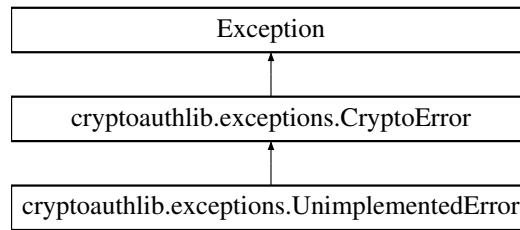


21.241.1 Detailed Description

for Microchip PHY protocol, timeout on transmission waiting for master

## 21.242 cryptoauthlib.exceptions.UnimplementedError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.UnimplementedError:

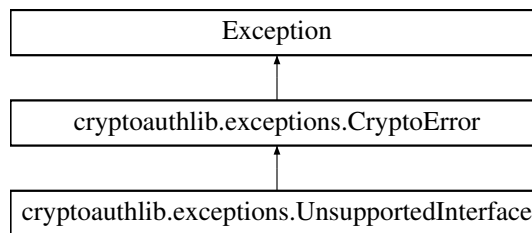


### 21.242.1 Detailed Description

Function or some element of it hasn't been implemented yet

## 21.243 cryptoauthlib.exceptions.UnsupportedInterface Class Reference

Inheritance diagram for cryptoauthlib.exceptions.UnsupportedInterface:

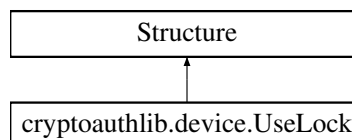


### 21.243.1 Detailed Description

"The selected interface is not supported by the library

## 21.244 cryptoauthlib.device.UseLock Class Reference

Inheritance diagram for cryptoauthlib.device.UseLock:



### Static Protected Attributes

- list `_fields_`
- int `_pack_` = 1



### 21.244.1 Detailed Description

UseLock Field Definition

### 21.244.2 Field Documentation

#### 21.244.2.1 `_fields_`

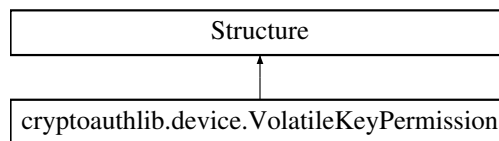
```
list cryptoauthlib.device.UseLock._fields_ [static], [protected]
```

**Initial value:**

```
= [ ('UseLockEnable', c_uint8, 4),  
    ('UseLockKey', c_uint8, 4)]
```

## 21.245 cryptoauthlib.device.VolatileKeyPermission Class Reference

Inheritance diagram for `cryptoauthlib.device.VolatileKeyPermission`:



### Static Protected Attributes

- list `_fields_`
- int `_pack_` = 1

### 21.245.1 Detailed Description

VolatileKeyPermission Field Definition

### 21.245.2 Field Documentation

#### 21.245.2.1 `_fields_`

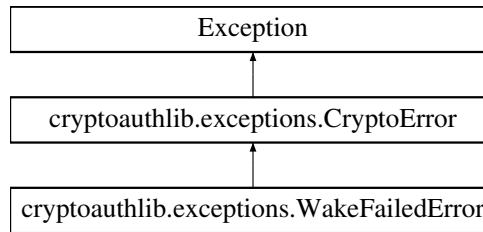
```
list cryptoauthlib.device.VolatileKeyPermission._fields_ [static], [protected]
```

**Initial value:**

```
= [ ('VolatileKeyPermitSlot', c_uint8, 4),  
    ('Reserved', c_uint8, 3),  
    ('VolatileKeyPermitEnable', c_uint8, 1)]
```

## 21.246 cryptauthlib.exceptions.WakeFailedError Class Reference

Inheritance diagram for cryptauthlib.exceptions.WakeFailedError:

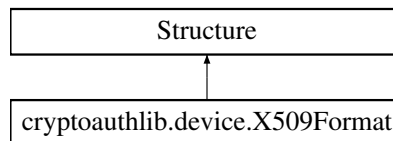


### 21.246.1 Detailed Description

Device Wake failed

## 21.247 cryptauthlib.device.X509Format Class Reference

Inheritance diagram for cryptauthlib.device.X509Format:



### Static Protected Attributes

- list [\\_fields\\_](#)
- int [\\_pack\\_](#) = 1

### 21.247.1 Detailed Description

X509Format Field Definition

### 21.247.2 Field Documentation

#### 21.247.2.1 [\\_fields\\_](#)

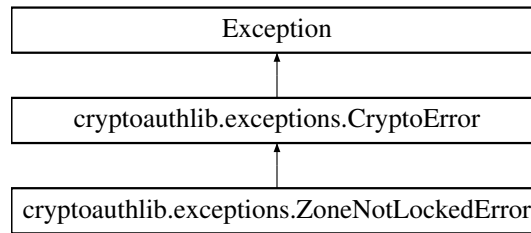
```
list cryptauthlib.device.X509Format._fields_ [static], [protected]
```

**Initial value:**

```
= [('PublicPosition', c_uint8, 4),  
   ('TemplateLength', c_uint8, 4)]
```

## 21.248 cryptoauthlib.exceptions.ZoneNotLockedError Class Reference

Inheritance diagram for cryptoauthlib.exceptions.ZoneNotLockedError:



### 21.248.1 Detailed Description

`required zone was not locked`

## Chapter 22

# File Documentation

### 22.1 api\_206a.c File Reference

Provides APIs to use with ATSHA206A device.

```
#include <stdlib.h>
#include <stdio.h>
#include "cryptoauthlib.h"
#include "api_206a.h"
```

#### Functions

- ATCA\_STATUS [sha206a\\_diversify\\_parent\\_key](#) (uint8\_t \*parent\_key, uint8\_t \*diversified\_key)  
*Computes the diversified key based on the parent key provided and device serial number.*
- ATCA\_STATUS [sha206a\\_generate\\_derive\\_key](#) (uint8\_t \*parent\_key, uint8\_t \*derived\_key, uint8\_t param1, uint16\_t param2)  
*Generates the derived key based on the parent key and other parameters provided.*
- ATCA\_STATUS [sha206a\\_generate\\_challenge\\_response\\_pair](#) (uint8\_t \*key, uint8\_t \*challenge, uint8\_t \*response)  
*Generates the response based on Key and Challenge provided.*
- ATCA\_STATUS [sha206a\\_authenticate](#) (uint8\_t \*challenge, uint8\_t \*expected\_response, uint8\_t \*is\_authenticated)  
*verifies the challenge and provided response using key in device*
- ATCA\_STATUS [sha206a\\_verify\\_device\\_consumption](#) (uint8\_t \*is\_consumed)  
*verifies the device is fully consumed or not based on Parent and Derived Key use flags.*
- ATCA\_STATUS [sha206a\\_check\\_dk\\_useflag\\_validity](#) (uint8\_t \*is\_consumed)  
*verifies Derived Key use flags for consumption*
- ATCA\_STATUS [sha206a\\_check\\_pk\\_useflag\\_validity](#) (uint8\_t \*is\_consumed)  
*verifies Parent Key use flags for consumption*
- ATCA\_STATUS [sha206a\\_get\\_dk\\_useflag\\_count](#) (uint8\_t \*dk\_available\_count)  
*calculates available Derived Key use counts*
- ATCA\_STATUS [sha206a\\_get\\_pk\\_useflag\\_count](#) (uint8\_t \*pk\_available\_count)  
*calculates available Parent Key use counts*
- ATCA\_STATUS [sha206a\\_get\\_dk\\_update\\_count](#) (uint8\_t \*dk\_update\_count)  
*Read Derived Key slot update count. It will be wraps around 256.*

- ATCA\_STATUS [sha206a\\_write\\_data\\_store](#) (uint8\_t slot, uint8\_t \*data, uint8\_t block, uint8\_t offset, uint8\_t len, bool lock\_after\_write)  
*Update the data store slot with user data and lock it if necessary.*
- ATCA\_STATUS [sha206a\\_read\\_data\\_store](#) (uint8\_t slot, uint8\_t \*data, uint8\_t offset, uint8\_t len)  
*Read the data stored in Data store.*
- ATCA\_STATUS [sha206a\\_get\\_data\\_store\\_lock\\_status](#) (uint8\_t slot, uint8\_t \*is\_locked)  
*Returns the lock status of the given data store.*

### 22.1.1 Detailed Description

Provides APIs to use with ATSHA206A device.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.1.2 Function Documentation

#### 22.1.2.1 sha206a\_authenticate()

```
ATCA_STATUS sha206a_authenticate (
    uint8_t * challenge,
    uint8_t * expected_response,
    uint8_t * is_authenticated )
```

verifies the challenge and provided response using key in device

#### Parameters

in	<i>challenge</i>	Challenge to be used in the response calculations
in	<i>expected_response</i>	Expected response from the device.
out	<i>is_authenticated</i>	result of expected of response and calcualted response

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 22.1.2.2 sha206a\_check\_dk\_useflag\_validity()

```
ATCA_STATUS sha206a_check_dk_useflag_validity (
    uint8_t * is_consumed )
```

verifies Derived Key use flags for consumption

## 22.1 api\_206a.c File Reference

---

### Parameters

out	<i>is_consumed</i>	indicates if DK is available for consumption.
-----	--------------------	---

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 22.1.2.3 sha206a\_check\_pk\_useflag\_validity()

```
ATCA_STATUS sha206a_check_pk_useflag_validity (
    uint8_t * is_consumed )
```

verifies Parent Key use flags for consumption

### Parameters

out	<i>is_consumed</i>	indicates if PK is available for consumption
-----	--------------------	--

### Returns

ATCA\_SUCCESS on success, otherwise an error code

### 22.1.2.4 sha206a\_diversify\_parent\_key()

```
ATCA_STATUS sha206a_diversify_parent_key (
    uint8_t * parent_key,
    uint8_t * diversified_key )
```

Computes the diversified key based on the parent key provided and device serial number.

### Parameters

in	<i>parent_key</i>	parent key to be diversified
out	<i>diversified_key</i>	diversified parent key

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 22.1.2.5 sha206a\_generate\_challenge\_response\_pair()

```
ATCA_STATUS sha206a_generate_challenge_response_pair (
    uint8_t * key,
    uint8_t * challenge,
    uint8_t * response )
```

Generates the response based on Key and Challenge provided.

#### Parameters

in	<i>key</i>	Input data contains device's key
in	<i>challenge</i>	Input data to be used in challenge response calculation
out	<i>response</i>	response derived from key and challenge

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 22.1.2.6 sha206a\_generate\_derive\_key()

```
ATCA_STATUS sha206a_generate_derive_key (
    uint8_t * parent_key,
    uint8_t * derived_key,
    uint8_t param1,
    uint16_t param2 )
```

Generates the derived key based on the parent key and other parameters provided.

#### Parameters

in	<i>parent_key</i>	Input data contains device's parent key
out	<i>derived_key</i>	Output data derived from parent key
in	<i>param1</i>	Input data to be used in derive key calculation
in	<i>param2</i>	Input data to be used in derive key calculation

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 22.1.2.7 sha206a\_get\_data\_store\_lock\_status()

```
ATCA_STATUS sha206a_get_data_store_lock_status (
    uint8_t slot,
    uint8_t * is_locked )
```

Returns the lock status of the given data store.

Parameters

in	slot	Slot number of the data store
out	is_locked	lock status of the data store

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.1.2.8 sha206a\_get\_dk\_update\_count()

```
ATCA_STATUS sha206a_get_dk_update_count (
    uint8_t * dk_update_count )
```

Read Derived Key slot update count. It will be wraps around 256.

Parameters

out	dk_update_count	returns number of times the slot has been updated with derived key
-----	-----------------	--

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.1.2.9 sha206a\_get\_dk\_useflag\_count()

```
ATCA_STATUS sha206a_get_dk_useflag_count (
    uint8_t * dk_available_count )
```

calculates available Derived Key use counts

Parameters

out	dk_available_count	counts available bit's as 1
-----	--------------------	-----------------------------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.1.2.10 sha206a\_get\_pk\_useflag\_count()

```
ATCA_STATUS sha206a_get_pk_useflag_count (
    uint8_t * pk_available_count )
```



calculates available Parent Key use counts

#### Parameters

out	<i>pk_available_count</i>	counts available bit's as 1
-----	---------------------------	-----------------------------

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 22.1.2.11 sha206a\_read\_data\_store()

```
ATCA_STATUS sha206a_read_data_store (
    uint8_t slot,
    uint8_t * data,
    uint8_t offset,
    uint8_t len )
```

Read the data stored in Data store.

#### Parameters

in	<i>slot</i>	Slot number to read from
in	<i>data</i>	Pointer to hold slot data data
in	<i>offset</i>	Byte offset within the zone to read from.
in	<i>len</i>	data length

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 22.1.2.12 sha206a\_verify\_device\_consumption()

```
ATCA_STATUS sha206a_verify_device_consumption (
    uint8_t * is_consumed )
```

verifies the device is fully consumed or not based on Parent and Derived Key use flags.

#### Parameters

out	<i>is_consumed</i>	result of device consumption
-----	--------------------	------------------------------

22.2 api\_206a.h File Reference

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.1.2.13 sha206a\_write\_data\_store()

```
ATCA_STATUS sha206a_write_data_store (
    uint8_t slot,
    uint8_t * data,
    uint8_t block,
    uint8_t offset,
    uint8_t len,
    bool lock_after_write )
```

Update the data store slot with user data and lock it if necessary.

Parameters

in	slot	Slot number to be written with data
in	data	Pointer that holds the data
in	block	32-byte block to write to.
in	offset	4-byte word within the specified block to write to. If performing a 32-byte write, this should be 0.
in	len	data length
in	lock_after_write	set 1 to lock slot after write, otherwise 0

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.2 api\_206a.h File Reference

Provides api interfaces to use with ATSHA206A device.

```
#include "atca_status.h"
```

Macros

- #define ATCA\_SHA206A\_ZONE\_WRITE\_LOCK 0x20u
- #define ATCA\_SHA206A\_DKEY\_CONSUMPTION\_MASK 0x01u
- #define ATCA\_SHA206A\_PKEY\_CONSUMPTION\_MASK 0x02u
- #define ATCA\_SHA206A\_SYMMETRIC\_KEY\_ID\_SLOT 0x07u

Enumerations

- enum { SHA206A\_DATA\_STORE0 =8 , SHA206A\_DATA\_STORE1 , SHA206A\_DATA\_STORE2 }

## Functions

- ATCA\_STATUS [sha206a\\_diversify\\_parent\\_key](#) (uint8\_t \*parent\_key, uint8\_t \*diversified\_key)  
*Computes the diversified key based on the parent key provided and device serial number.*
- ATCA\_STATUS [sha206a\\_generate\\_derive\\_key](#) (uint8\_t \*parent\_key, uint8\_t \*derived\_key, uint8\_t param1, uint16\_t param2)  
*Generates the derived key based on the parent key and other parameters provided.*
- ATCA\_STATUS [sha206a\\_generate\\_challenge\\_response\\_pair](#) (uint8\_t \*key, uint8\_t \*challenge, uint8\_t \*response)  
*Generates the response based on Key and Challenge provided.*
- ATCA\_STATUS [sha206a\\_authenticate](#) (uint8\_t \*challenge, uint8\_t \*expected\_response, uint8\_t \*is\_authenticated)  
*verifies the challenge and provided response using key in device*
- ATCA\_STATUS [sha206a\\_verify\\_device\\_consumption](#) (uint8\_t \*is\_consumed)  
*verifies the device is fully consumed or not based on Parent and Derived Key use flags.*
- ATCA\_STATUS [sha206a\\_check\\_dk\\_useflag\\_validity](#) (uint8\_t \*is\_consumed)  
*verifies Derived Key use flags for consumption*
- ATCA\_STATUS [sha206a\\_check\\_pk\\_useflag\\_validity](#) (uint8\_t \*is\_consumed)  
*verifies Parent Key use flags for consumption*
- ATCA\_STATUS [sha206a\\_get\\_dk\\_useflag\\_count](#) (uint8\_t \*dk\_available\_count)  
*calculates available Derived Key use counts*
- ATCA\_STATUS [sha206a\\_get\\_pk\\_useflag\\_count](#) (uint8\_t \*pk\_available\_count)  
*calculates available Parent Key use counts*
- ATCA\_STATUS [sha206a\\_get\\_dk\\_update\\_count](#) (uint8\_t \*dk\_update\_count)  
*Read Derived Key slot update count. It will be wraps around 256.*
- ATCA\_STATUS [sha206a\\_write\\_data\\_store](#) (uint8\_t slot, uint8\_t \*data, uint8\_t block, uint8\_t offset, uint8\_t len, bool lock\_after\_write)  
*Update the data store slot with user data and lock it if necessary.*
- ATCA\_STATUS [sha206a\\_read\\_data\\_store](#) (uint8\_t slot, uint8\_t \*data, uint8\_t offset, uint8\_t len)  
*Read the data stored in Data store.*
- ATCA\_STATUS [sha206a\\_get\\_data\\_store\\_lock\\_status](#) (uint8\_t slot, uint8\_t \*is\_locked)  
*Returns the lock status of the given data store.*

### 22.2.1 Detailed Description

Provides api interfaces to use with ATSHA206A device.

Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.2.2 Function Documentation

#### 22.2.2.1 sha206a\_authenticate()

```
ATCA_STATUS sha206a_authenticate (
    uint8_t * challenge,
    uint8_t * expected_response,
    uint8_t * is_authenticated )
```

verifies the challenge and provided response using key in device

### Parameters

in	<i>challenge</i>	Challenge to be used in the response calculations
in	<i>expected_response</i>	Expected response from the device.
out	<i>is_authenticated</i>	result of expected of response and calcaulted response

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 22.2.2.2 sha206a\_check\_dk\_useflag\_validity()

```
ATCA_STATUS sha206a_check_dk_useflag_validity (
    uint8_t * is_consumed )
```

verifies Derived Key use flags for consumption

### Parameters

out	<i>is_consumed</i>	indicates if DK is available for consumption.
-----	--------------------	---

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 22.2.2.3 sha206a\_check\_pk\_useflag\_validity()

```
ATCA_STATUS sha206a_check_pk_useflag_validity (
    uint8_t * is_consumed )
```

verifies Parent Key use flags for consumption

### Parameters

out	<i>is_consumed</i>	indicates if PK is available for consumption
-----	--------------------	--

### Returns

ATCA\_SUCCESS on success, otherwise an error code

#### 22.2.2.4 sha206a\_diversify\_parent\_key()

```
ATCA_STATUS sha206a_diversify_parent_key (
    uint8_t * parent_key,
    uint8_t * diversified_key )
```

Computes the diversified key based on the parent key provided and device serial number.

##### Parameters

in	<i>parent_key</i>	parent key to be diversified
out	<i>diversified_key</i>	diversified parent key

##### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 22.2.2.5 sha206a\_generate\_challenge\_response\_pair()

```
ATCA_STATUS sha206a_generate_challenge_response_pair (
    uint8_t * key,
    uint8_t * challenge,
    uint8_t * response )
```

Generates the response based on Key and Challenge provided.

##### Parameters

in	<i>key</i>	Input data contains device's key
in	<i>challenge</i>	Input data to be used in challenge response calculation
out	<i>response</i>	response derived from key and challenge

##### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 22.2.2.6 sha206a\_generate\_derive\_key()

```
ATCA_STATUS sha206a_generate_derive_key (
    uint8_t * parent_key,
    uint8_t * derived_key,
    uint8_t param1,
    uint16_t param2 )
```

Generates the derived key based on the parent key and other parameters provided.

### Parameters

in	<i>parent_key</i>	Input data contains device's parent key
out	<i>derived_key</i>	Output data derived from parent key
in	<i>param1</i>	Input data to be used in derive key calculation
in	<i>param2</i>	Input data to be used in derive key calculation

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 22.2.2.7 sha206a\_get\_data\_store\_lock\_status()

```
ATCA_STATUS sha206a_get_data_store_lock_status (
    uint8_t slot,
    uint8_t * is_locked )
```

Returns the lock status of the given data store.

### Parameters

in	<i>slot</i>	Slot number of the data store
out	<i>is_locked</i>	lock status of the data store

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 22.2.2.8 sha206a\_get\_dk\_update\_count()

```
ATCA_STATUS sha206a_get_dk_update_count (
    uint8_t * dk_update_count )
```

Read Derived Key slot update count. It will be wraps around 256.

### Parameters

out	<i>dk_update_count</i>	returns number of times the slot has been updated with derived key
-----	------------------------	--

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 22.2.2.9 sha206a\_get\_dk\_useflag\_count()

```
ATCA_STATUS sha206a_get_dk_useflag_count (
    uint8_t * dk_available_count )
```

calculates available Derived Key use counts

Parameters

out	<i>dk_available_count</i>	counts available bit's as 1
-----	---------------------------	-----------------------------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 22.2.2.10 sha206a\_get\_pk\_useflag\_count()

```
ATCA_STATUS sha206a_get_pk_useflag_count (
    uint8_t * pk_available_count )
```

calculates available Parent Key use counts

Parameters

out	<i>pk_available_count</i>	counts available bit's as 1
-----	---------------------------	-----------------------------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 22.2.2.11 sha206a\_read\_data\_store()

```
ATCA_STATUS sha206a_read_data_store (
    uint8_t slot,
    uint8_t * data,
    uint8_t offset,
    uint8_t len )
```

Read the data stored in Data store.

Parameters

in	<i>slot</i>	Slot number to read from
in	<i>data</i>	Pointer to hold slot data data
in	<i>offset</i>	Byte offset within the zone to read from.
in	<i>len</i>	data length

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.2.2.12 sha206a\_verify\_device\_consumption()

```
ATCA_STATUS sha206a_verify_device_consumption (
    uint8_t * is_consumed )
```

verifies the device is fully consumed or not based on Parent and Derived Key use flags.

Parameters

out	<i>is_consumed</i>	result of device consumption
-----	--------------------	------------------------------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.2.2.13 sha206a\_write\_data\_store()

```
ATCA_STATUS sha206a_write_data_store (
    uint8_t slot,
    uint8_t * data,
    uint8_t block,
    uint8_t offset,
    uint8_t len,
    bool lock_after_write )
```

Update the data store slot with user data and lock it if necessary.

Parameters

in	<i>slot</i>	Slot number to be written with data
in	<i>data</i>	Pointer that holds the data
in	<i>block</i>	32-byte block to write to.
in	<i>offset</i>	4-byte word within the specified block to write to. If performing a 32-byte write, this should be 0.
in	<i>len</i>	data length
in	<i>lock_after_write</i>	set 1 to lock slot after write, otherwise 0

Returns

ATCA\_SUCCESS on success, otherwise an error code.



## 22.3 symmetric\_authentication.c File Reference

Contains API for performing the symmetric Authentication between the Host and the device.

```
#include "cryptoauthlib.h"
#include "host/atca_host.h"
#include "symmetric_authentication.h"
```

### Functions

- ATCA\_STATUS [symmetric\\_authenticate](#) (uint8\_t slot, const uint8\_t \*master\_key, const uint8\_t \*rand\_↵number)  
*Function which does the authentication between the host and device.*

### 22.3.1 Detailed Description

Contains API for performing the symmetric Authentication between the Host and the device.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.3.2 Function Documentation

#### 22.3.2.1 symmetric\_authenticate()

```
ATCA_STATUS symmetric_authenticate (
    uint8_t slot,
    const uint8_t * master_key,
    const uint8_t * rand_number )
```

Function which does the authentication between the host and device.

#### Parameters

in	<i>slot</i>	The slot number used for the symmetric authentication.
in	<i>master_key</i>	The master key used for the calculating the symmetric key.
in	<i>rand_number</i>	The 20 byte rand_number from the host.

Returns

ATCA\_SUCCESS on successful authentication, otherwise an error code.

22.4 symmetric\_authentication.h File Reference

Contains API for performing the symmetric Authentication between the Host and the device.

```
#include "cryptoauthlib.h"
```

Functions

- ATCA\_STATUS [symmetric\\_authenticate](#) (uint8\_t slot, const uint8\_t \*master\_key, const uint8\_t \*rand\_↵  
number)

*Function which does the authentication between the host and device.*

22.4.1 Detailed Description

Contains API for performing the symmetric Authentication between the Host and the device.

Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

22.4.2 Function Documentation

22.4.2.1 symmetric\_authenticate()

```
ATCA_STATUS symmetric_authenticate (  
    uint8_t slot,  
    const uint8_t * master_key,  
    const uint8_t * rand_number )
```

Function which does the authentication between the host and device.

Parameters

in	<i>slot</i>	The slot number used for the symmetric authentication.
in	<i>master_key</i>	The master key used for the calculating the symmetric key.
in	<i>rand_number</i>	The 20 byte rand_number from the host.

### Returns

ATCA\_SUCCESS on successful authentication, otherwise an error code.

## 22.5 ascii\_kit\_host.c File Reference

KIT protocol interpreter.

```
#include <ctype.h>
#include "ascii_kit_host.h"
#include "hal/kit_protocol.h"
#include "talib/talib_fce.h"
```

### Functions

- ATCA\_STATUS [kit\\_host\\_init\\_phy](#) ([atca\\_hal\\_kit\\_phy\\_t](#) \*phy, [ATCAIface](#) iface)  
*Initializes a phy structure with a cryptoauthlib hal adapter.*
- ATCA\_STATUS [kit\\_host\\_init](#) ([ascii\\_kit\\_host\\_context\\_t](#) \*ctx, [ATCAIfaceCfg](#) \*iface[], const size\_t iface\_count, const [atca\\_hal\\_kit\\_phy\\_t](#) \*phy, const uint32\_t flags)  
*Initializes the kit protocol parser context.*
- size\_t [kit\\_host\\_format\\_response](#) (uint8\_t \*response, size\_t rlen, ATCA\_STATUS status, uint8\_t \*data, size\_t dlen)  
*Format the status and data into the kit protocol response format.*
- ATCA\_STATUS [kit\\_host\\_process\\_cmd](#) ([ascii\\_kit\\_host\\_context\\_t](#) \*ctx, const [kit\\_host\\_map\\_entry\\_t](#) \*cmd↵\_list, int argc, char \*argv[], uint8\_t \*response, size\_t \*rlen)  
*Iterate through a command list to match the given command and then will execute it.*
- ATCA\_STATUS [kit\\_host\\_process\\_ta](#) ([ascii\\_kit\\_host\\_context\\_t](#) \*ctx, int argc, char \*argv[], uint8\_t↵ \*response, size\_t \*rlen)
- ATCA\_STATUS [kit\\_host\\_process\\_line](#) ([ascii\\_kit\\_host\\_context\\_t](#) \*ctx, uint8\_t \*input\_line, size\_t ilen, uint8\_t \*response, size\_t \*rlen)  
*Parse a line as a kit protocol command. The kit protocol is printable ascii and each line ends with a newline character.*
- void [kit\\_host\\_task](#) ([ascii\\_kit\\_host\\_context\\_t](#) \*ctx)  
*Non returning kit protocol runner using the configured physical interface that was provided when the context was initialized.*

### 22.5.1 Detailed Description

KIT protocol interpreter.

#### Copyright

(c) 2018 Microchip Technology Inc. and its subsidiaries. You may use this software and any derivatives exclusively with Microchip products.

### 22.5.2 Function Documentation

22.5.2.1 kit\_host\_init()

```
ATCA_STATUS kit_host_init (
    ascii_kit_host_context_t * ctx,
    ATCAIfaceCfg * iface[],
    const size_t iface_count,
    const atca_hal_kit_phy_t * phy,
    const uint32_t flags )
```

Initializes the kit protocol parser context.

Returns

ATCA\_SUCCESS on success, otherwise an error code

Parameters

<i>ctx</i>	Kit protocol parser context
<i>iface</i>	List of device configurations which will be used
<i>iface_count</i>	Number of configurations provided
<i>phy</i>	Kit protocol physical adapter
<i>flags</i>	Option Flags

22.5.2.2 kit\_host\_init\_phy()

```
ATCA_STATUS kit_host_init_phy (
    atca_hal_kit_phy_t * phy,
    ATCAIface iface )
```

Initializes a phy structure with a cryptoauthlib hal adapter.

Returns

ATCA\_SUCCESS on success, otherwise an error code

22.6 ascii\_kit\_host.h File Reference

KIT protocol interpreter.

```
#include "cryptoauthlib.h"
```

Data Structures

- struct [\\_ascii\\_kit\\_host\\_context](#)
- struct [\\_kit\\_host\\_map\\_entry](#)

## Macros

- `#define KIT_LAYER_DELIMITER ':'`
- `#define KIT_DATA_BEGIN_DELIMITER '('`
- `#define KIT_DATA_END_DELIMITER ')'`
- `#define KIT_MESSAGE_DELIMITER '\n'`
- `#define KIT_MESSAGE_SIZE_MAX (2500)`  
*The Kit Protocol maximum message size.*
- `#define KIT_SECTION_NAME_SIZE_MAX KIT_MESSAGE_SIZE_MAX`
- `#define KIT_VERSION_SIZE_MAX (32)`
- `#define KIT_FIRMWARE_SIZE_MAX (32)`

## Typedefs

- `typedef struct _ascii_kit_host_context ascii_kit_host_context_t`
- `typedef struct _kit_host_map_entry kit_host_map_entry_t`

## Functions

- `ATCA_STATUS kit_host_init_phy (atca_hal_kit_phy_t *phy, ATCAIface iface)`  
*Initializes a phy structure with a cryptoauthlib hal adapter.*
- `ATCA_STATUS kit_host_init (ascii_kit_host_context_t *ctx, ATCAIfaceCfg *iface[], const size_t iface_count, const atca_hal_kit_phy_t *phy, const uint32_t flags)`  
*Initializes the kit protocol parser context.*
- `size_t kit_host_format_response (uint8_t *response, size_t rlen, ATCA_STATUS status, uint8_t *data, size_t dlen)`  
*Format the status and data into the kit protocol response format.*
- `ATCA_STATUS kit_host_process_cmd (ascii_kit_host_context_t *ctx, const kit_host_map_entry_t *cmd↵_list, int argc, char *argv[], uint8_t *response, size_t *rlen)`  
*Iterate through a command list to match the given command and then will execute it.*
- `ATCA_STATUS kit_host_process_line (ascii_kit_host_context_t *ctx, uint8_t *input_line, size_t ilen, uint8_t *response, size_t *rlen)`  
*Parse a line as a kit protocol command. The kit protocol is printable ascii and each line ends with a newline character.*
- `void kit_host_task (ascii_kit_host_context_t *ctx)`  
*Non returning kit protocol runner using the configured physical interface that was provided when the context was initialized.*

### 22.6.1 Detailed Description

KIT protocol interpreter.

#### Copyright

(c) 2018 Microchip Technology Inc. and its subsidiaries. You may use this software and any derivatives exclusively with Microchip products.

### 22.6.2 Macro Definition Documentation

22.6.2.1 `KIT_MESSAGE_SIZE_MAX`

```
#define KIT_MESSAGE_SIZE_MAX (2500)
```

The Kit Protocol maximum message size.

Note

Send: <target>:<command>(optional hex bytes to send)  
Receive: <status hex byte>(optional hex bytes of response)

22.6.3 Typedef Documentation

22.6.3.1 `kit_host_map_entry_t`

```
typedef struct _kit_host_map_entry kit_host_map_entry_t
```

Used to create command tables for the kit host parser

22.6.4 Function Documentation

22.6.4.1 `kit_host_init()`

```
ATCA_STATUS kit_host_init (
    ascii_kit_host_context_t * ctx,
    ATCAIfaceCfg * iface[],
    const size_t iface_count,
    const atca_hal_kit_phy_t * phy,
    const uint32_t flags )
```

Initializes the kit protocol parser context.

Returns

`ATCA_SUCCESS` on success, otherwise an error code

Parameters

<i>ctx</i>	Kit protocol parser context
<i>iface</i>	List of device configurations which will be used
<i>iface_count</i>	Number of configurations provided
<i>phy</i>	Kit protocol physical adapter
<i>flags</i>	Option Flags

#### 22.6.4.2 kit\_host\_init\_phy()

```
ATCA_STATUS kit_host_init_phy (
    atca_hal_kit_phy_t * phy,
    ATCAIface iface )
```

Initializes a phy structure with a cryptoauthlib hal adapter.

##### Returns

ATCA\_SUCCESS on success, otherwise an error code

## 22.7 trust\_pkcs11\_config.c File Reference

PKCS11 Trust Platform Configuration.

```
#include "cryptoauthlib.h"
#include "pkcs11_config.h"
#include "pkcs11/pkcs11_object.h"
#include "pkcs11/pkcs11_slot.h"
```

### 22.7.1 Detailed Description

PKCS11 Trust Platform Configuration.

##### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.8 io\_protection\_key.h File Reference

Provides required interface to access IO protection key.

```
#include "atca_status.h"
```

### Functions

- ATCA\_STATUS **io\_protection\_get\_key** (uint8\_t \*io\_key)
- ATCA\_STATUS **io\_protection\_set\_key** (uint8\_t \*io\_key)

### 22.8.1 Detailed Description

Provides required interface to access IO protection key.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.9 secure\_boot.c File Reference

Provides required APIs to manage secure boot under various scenarios.

```
#include <string.h>
#include "secure_boot.h"
#include "io_protection_key.h"
#include "basic/atca_basic.h"
```

### Functions

- ATCA\_STATUS [secure\\_boot\\_process](#) (void)  
*Handles secure boot functionality through initialization, execution, and de-initialization.*
- ATCA\_STATUS [bind\\_host\\_and\\_secure\\_element\\_with\\_io\\_protection](#) (uint16\_t slot)  
*Binds host MCU and Secure element with IO protection key.*

### 22.9.1 Detailed Description

Provides required APIs to manage secure boot under various scenarios.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.9.2 Function Documentation

#### 22.9.2.1 bind\_host\_and\_secure\_element\_with\_io\_protection()

```
ATCA_STATUS bind_host_and_secure_element_with_io_protection (
    uint16_t slot )
```

Binds host MCU and Secure element with IO protection key.



Parameters

<code>in</code>	<code>slot</code>	The slot number of IO protection Key.
-----------------	-------------------	---------------------------------------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 22.9.2.2 secure\_boot\_process()

```
ATCA_STATUS secure_boot_process (
    void )
```

Handles secure boot functionality through initialization, execution, and de-initialization.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

## 22.10 secure\_boot.h File Reference

Provides required APIs to manage secure boot under various scenarios.

```
#include "atca_status.h"
#include "secure_boot_memory.h"
#include "atca_command.h"
#include "crypto/atca_crypto_sw_sha2.h"
```

### Data Structures

- struct [secure\\_boot\\_config\\_bits](#)
- struct [secure\\_boot\\_parameters](#)

### Macros

- #define **SECURE\_BOOT\_CONFIG\_DISABLE** 0
- #define **SECURE\_BOOT\_CONFIG\_FULL\_BOTH** 1
- #define **SECURE\_BOOT\_CONFIG\_FULL\_SIGN** 2
- #define **SECURE\_BOOT\_CONFIG\_FULL\_DIG** 3
- #define **SECURE\_BOOT\_CONFIGURATION** SECURE\_BOOT\_CONFIG\_FULL\_DIG
- #define **SECURE\_BOOT\_DIGEST\_ENCRYPT\_ENABLED** true
- #define **SECURE\_BOOT\_UPGRADE\_SUPPORT** true

Functions

- ATCA\_STATUS [secure\\_boot\\_process](#) (void)  
*Handles secure boot functionality through initialization, execution, and de-initialization.*
- ATCA\_STATUS [bind\\_host\\_and\\_secure\\_element\\_with\\_io\\_protection](#) (uint16\_t slot)  
*Binds host MCU and Secure element with IO protection key.*
- ATCA\_STATUS [host\\_generate\\_random\\_number](#) (uint8\_t \*rand)

22.10.1 Detailed Description

Provides required APIs to manage secure boot under various scenarios.

Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

22.10.2 Function Documentation

22.10.2.1 [bind\\_host\\_and\\_secure\\_element\\_with\\_io\\_protection\(\)](#)

```
ATCA_STATUS bind_host_and_secure_element_with_io_protection (
    uint16_t slot )
```

Binds host MCU and Secure element with IO protection key.

Parameters

in	slot	The slot number of IO protection Key.
----	------	---------------------------------------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.10.2.2 [secure\\_boot\\_process\(\)](#)

```
ATCA_STATUS secure_boot_process (
    void )
```

Handles secure boot functionality through initialization, execution, and de-initialization.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

## 22.11 secure\_boot\_memory.h File Reference

Provides interface to memory component for the secure boot.

```
#include "atca_status.h"
#include "atca_command.h"
```

### Data Structures

- struct [memory\\_parameters](#)

### Functions

- ATCA\_STATUS **secure\_boot\_init\_memory** ([memory\\_parameters](#) \*memory\_params)
- ATCA\_STATUS **secure\_boot\_read\_memory** (uint8\_t \*pu8\_data, uint32\_t \*pu32\_target\_length)
- ATCA\_STATUS **secure\_boot\_write\_memory** (uint8\_t \*pu8\_data, uint32\_t \*pu32\_target\_length)
- void **secure\_boot\_deinit\_memory** ([memory\\_parameters](#) \*memory\_params)
- ATCA\_STATUS **secure\_boot\_mark\_full\_copy\_completion** (void)
- bool **secure\_boot\_check\_full\_copy\_completion** (void)

#### 22.11.1 Detailed Description

Provides interface to memory component for the secure boot.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.12 tflxtls\_cert\_def\_4\_device.c File Reference

TNG TLS device certificate definition.

```
#include "atcacert/atcacert_def.h"
#include "tngtls_cert_def_1_signer.h"
#include "tflxtls_cert_def_4_device.h"
```

### Variables

- const uint8\_t **g\_tflxtls\_cert\_template\_4\_device** [500]
- const [atcacert\\_cert\\_element\\_t](#) **g\_tflxtls\_cert\_elements\_4\_device** []
- const [atcacert\\_def\\_t](#) **g\_tflxtls\_cert\_def\_4\_device**

### 22.12.1 Detailed Description

TNG TLS device certificate definition.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.13 tflxtls\_cert\_def\_4\_device.h File Reference

TNG TLS device certificate definition.

```
#include "atcacert/atcacert_def.h"
```

### Variables

- const uint8\_t **g\_tflxtls\_cert\_template\_4\_device** [500]
- const [atcacert\\_def\\_t](#) **g\_tflxtls\_cert\_def\_4\_device**
- const [atcacert\\_cert\\_element\\_t](#) **g\_tflxtls\_cert\_elements\_4\_device** []

### 22.13.1 Detailed Description

TNG TLS device certificate definition.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.14 tng\_atca.c File Reference

TNG Helper Functions.

```
#include <string.h>
#include "cryptoauthlib.h"
#include "tng_atca.h"
#include "tnglora_cert_def_2_device.h"
#include "tnglora_cert_def_4_device.h"
#include "tngtls_cert_def_2_device.h"
#include "tngtls_cert_def_3_device.h"
#include "tflxtls_cert_def_4_device.h"
#include "atcacert/atcacert_def.h"
```

## Data Structures

- struct [tng\\_cert\\_map\\_element](#)

## Functions

- const [atcacert\\_def\\_t](#) \* [tng\\_map\\_get\\_device\\_cert\\_def](#) (int index)  
*Helper function to iterate through all trust cert definitions.*
- ATCA\_STATUS [tng\\_get\\_device\\_cert\\_def\\_ext](#) (ATCADevice device, const [atcacert\\_def\\_t](#) \*\*cert\_def)  
*Get the TNG device certificate definition.*
- ATCA\_STATUS [tng\\_get\\_device\\_cert\\_def](#) (const [atcacert\\_def\\_t](#) \*\*cert\_def)  
*Get the TNG device certificate definition.*
- ATCA\_STATUS [tng\\_get\\_device\\_pubkey](#) (uint8\_t \*public\_key)  
*Uses GenKey command to calculate the public key from the primary device public key.*

### 22.14.1 Detailed Description

TNG Helper Functions.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.15 tng\_atca.h File Reference

TNG Helper Functions.

```
#include "atca_basic.h"
#include "atcacert/atcacert_def.h"
```

## Macros

- #define **ATCA\_OTP\_CODE\_SIZE** (8u)

## Functions

- const [atcacert\\_def\\_t](#) \* [tng\\_map\\_get\\_device\\_cert\\_def](#) (int index)  
*Helper function to iterate through all trust cert definitions.*
- ATCA\_STATUS [tng\\_get\\_device\\_cert\\_def](#) (const [atcacert\\_def\\_t](#) \*\*cert\_def)  
*Get the TNG device certificate definition.*
- ATCA\_STATUS [tng\\_get\\_device\\_cert\\_def\\_ext](#) (ATCADevice device, const [atcacert\\_def\\_t](#) \*\*cert\_def)  
*Get the TNG device certificate definition.*
- ATCA\_STATUS [tng\\_get\\_device\\_pubkey](#) (uint8\_t \*public\_key)  
*Uses GenKey command to calculate the public key from the primary device public key.*

### 22.15.1 Detailed Description

TNG Helper Functions.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.16 tng\_atcacert\_client.c File Reference

Client side certificate I/O functions for TNG devices.

```
#include "tng_atca.h"
#include "atcacert/atcacert_client.h"
#include "tng_atcacert_client.h"
#include "tngtls_cert_def_1_signer.h"
#include "tng_root_cert.h"
#include <limits.h>
```

### Functions

- int [tng\\_atcacert\\_max\\_device\\_cert\\_size](#) (size\_t \*max\_cert\_size)  
*Return the maximum possible certificate size in bytes for a TNG device certificate. Certificate can be variable size, so this gives an appropriate buffer size when reading the certificate.*
- int [tng\\_atcacert\\_read\\_device\\_cert](#) (uint8\_t \*cert, size\_t \*cert\_size, const uint8\_t \*signer\_cert)  
*Reads the device certificate for a TNG device.*
- int [tng\\_atcacert\\_device\\_public\\_key](#) (uint8\_t \*public\_key, uint8\_t \*cert)  
*Reads the device public key.*
- int [tng\\_atcacert\\_max\\_signer\\_cert\\_size](#) (size\_t \*max\_cert\_size)  
*Return the maximum possible certificate size in bytes for a TNG signer certificate. Certificate can be variable size, so this gives an appropriate buffer size when reading the certificate.*
- int [tng\\_atcacert\\_read\\_signer\\_cert](#) (uint8\_t \*cert, size\_t \*cert\_size)  
*Reads the signer certificate for a TNG device.*
- int [tng\\_atcacert\\_signer\\_public\\_key](#) (uint8\_t \*public\_key, uint8\_t \*cert)  
*Reads the signer public key.*
- int [tng\\_atcacert\\_root\\_cert\\_size](#) (size\_t \*cert\_size)  
*Get the size of the TNG root cert.*
- int [tng\\_atcacert\\_root\\_cert](#) (uint8\_t \*cert, size\_t \*cert\_size)  
*Get the TNG root cert.*
- int [tng\\_atcacert\\_root\\_public\\_key](#) (uint8\_t \*public\_key)  
*Gets the root public key.*

### 22.16.1 Detailed Description

Client side certificate I/O functions for TNG devices.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.16.2 Function Documentation

### 22.16.2.1 tng\_atcacert\_device\_public\_key()

```
int tng_atcacert_device_public_key (
    uint8_t * public_key,
    uint8_t * cert )
```

Reads the device public key.

#### Parameters

out	<i>public_key</i>	Public key will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve.
in	<i>cert</i>	If supplied, the device public key is used from this certificate. If set to NULL, the device public key is read from the device.

#### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 22.16.2.2 tng\_atcacert\_max\_signer\_cert\_size()

```
int tng_atcacert_max_signer_cert_size (
    size_t * max_cert_size )
```

Return the maximum possible certificate size in bytes for a TNG signer certificate. Certificate can be variable size, so this gives an appropriate buffer size when reading the certificate.

#### Parameters

out	<i>max_cert_size</i>	Maximum certificate size will be returned here in bytes.
-----	----------------------	--

#### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 22.16.2.3 tng\_atcacert\_read\_device\_cert()

```
int tng_atcacert_read_device_cert (
    uint8_t * cert,
    size_t * cert_size,
    const uint8_t * signer_cert )
```

Reads the device certificate for a TNG device.

## 22.16 tng\_atcacert\_client.c File Reference

---

### Parameters

out	<i>cert</i>	Buffer to received the certificate (DER format).
in, out	<i>cert_size</i>	As input, the size of the cert buffer in bytes. As output, the size of the certificate returned in cert in bytes.
in	<i>signer_cert</i>	If supplied, the signer public key is used from this certificate. If set to NULL, the signer public key is read from the device.

### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 22.16.2.4 tng\_atcacert\_read\_signer\_cert()

```
int tng_atcacert_read_signer_cert (
    uint8_t * cert,
    size_t * cert_size )
```

Reads the signer certificate for a TNG device.

### Parameters

out	<i>cert</i>	Buffer to received the certificate (DER format).
in, out	<i>cert_size</i>	As input, the size of the cert buffer in bytes. As output, the size of the certificate returned in cert in bytes.

### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

### 22.16.2.5 tng\_atcacert\_root\_cert()

```
int tng_atcacert_root_cert (
    uint8_t * cert,
    size_t * cert_size )
```

Get the TNG root cert.

### Parameters

out	<i>cert</i>	Buffer to received the certificate (DER format).
in, out	<i>cert_size</i>	As input, the size of the cert buffer in bytes. As output, the size of the certificate returned in cert in bytes.



Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

22.16.2.6 tng\_atcacert\_root\_cert\_size()

```
int tng_atcacert_root_cert_size (
    size_t * cert_size )
```

Get the size of the TNG root cert.

Parameters

out	cert_size	Certificate size will be returned here in bytes.
-----	-----------	--

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

22.16.2.7 tng\_atcacert\_root\_public\_key()

```
int tng_atcacert_root_public_key (
    uint8_t * public_key )
```

Gets the root public key.

Parameters

out	public_key	Public key will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve.
-----	------------	--

Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

22.16.2.8 tng\_atcacert\_signer\_public\_key()

```
int tng_atcacert_signer_public_key (
    uint8_t * public_key,
    uint8_t * cert )
```

Reads the signer public key.

## 22.17 tng\_atcacert\_client.h File Reference

---

### Parameters

out	public_key	Public key will be returned here. Format will be the X and Y integers in big-endian format. 64 bytes for P256 curve.
in	cert	If supplied, the signer public key is used from this certificate. If set to NULL, the signer public key is read from the device.

### Returns

ATCACERT\_E\_SUCCESS on success, otherwise an error code.

## 22.17 tng\_atcacert\_client.h File Reference

Client side certificate I/O functions for TNG devices.

```
#include <stdint.h>
#include "atcacert/atcacert.h"
```

### Functions

- int [tng\\_atcacert\\_max\\_device\\_cert\\_size](#) (size\_t \*max\_cert\_size)  
*Return the maximum possible certificate size in bytes for a TNG device certificate. Certificate can be variable size, so this gives an appropriate buffer size when reading the certificate.*
- int [tng\\_atcacert\\_read\\_device\\_cert](#) (uint8\_t \*cert, size\_t \*cert\_size, const uint8\_t \*signer\_cert)  
*Reads the device certificate for a TNG device.*
- int [tng\\_atcacert\\_device\\_public\\_key](#) (uint8\_t \*public\_key, uint8\_t \*cert)  
*Reads the device public key.*
- int [tng\\_atcacert\\_max\\_signer\\_cert\\_size](#) (size\_t \*max\_cert\_size)  
*Return the maximum possible certificate size in bytes for a TNG signer certificate. Certificate can be variable size, so this gives an appropriate buffer size when reading the certificate.*
- int [tng\\_atcacert\\_read\\_signer\\_cert](#) (uint8\_t \*cert, size\_t \*cert\_size)  
*Reads the signer certificate for a TNG device.*
- int [tng\\_atcacert\\_signer\\_public\\_key](#) (uint8\_t \*public\_key, uint8\_t \*cert)  
*Reads the signer public key.*
- int [tng\\_atcacert\\_root\\_cert\\_size](#) (size\_t \*cert\_size)  
*Get the size of the TNG root cert.*
- int [tng\\_atcacert\\_root\\_cert](#) (uint8\_t \*cert, size\_t \*cert\_size)  
*Get the TNG root cert.*
- int [tng\\_atcacert\\_root\\_public\\_key](#) (uint8\_t \*public\_key)  
*Gets the root public key.*

### 22.17.1 Detailed Description

Client side certificate I/O functions for TNG devices.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.18 tng\_root\_cert.c File Reference

TNG root certificate (DER)

```
#include <stdint.h>
#include <stddef.h>
#include "tng_root_cert.h"
```

### Variables

- const uint8\_t **g\_cryptoauth\_root\_ca\_002\_cert** [501]
- const size\_t **g\_cryptoauth\_root\_ca\_002\_cert\_size** = sizeof(g\_cryptoauth\_root\_ca\_002\_cert)

### 22.18.1 Detailed Description

TNG root certificate (DER)

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.19 tng\_root\_cert.h File Reference

TNG root certificate (DER)

```
#include <stdint.h>
```

- #define **CRYPTOAUTH\_ROOT\_CA\_002\_PUBLIC\_KEY\_OFFSET** 266
- const uint8\_t **g\_cryptoauth\_root\_ca\_002\_cert** []
- const size\_t **g\_cryptoauth\_root\_ca\_002\_cert\_size**

### 22.19.1 Detailed Description

TNG root certificate (DER)

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.20 tnglora\_cert\_def\_1\_signer.c File Reference

TNG LORA signer certificate definition.

```
#include "atcacert/atcacert_def.h"
#include "tngtls_cert_def_1_signer.h"
#include "tnglora_cert_def_1_signer.h"
```

### Variables

- SHARED\_LIB\_EXPORT const [atcacert\\_def\\_t](#) g\_tnglora\_cert\_def\_1\_signer

### 22.20.1 Detailed Description

TNG LORA signer certificate definition.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.21 tnglora\_cert\_def\_1\_signer.h File Reference

TNG LORA signer certificate definition.

```
#include "atcacert/atcacert_def.h"
```

### Variables

- ATCA\_DLL const [atcacert\\_def\\_t](#) g\_tnglora\_cert\_def\_1\_signer

### 22.21.1 Detailed Description

TNG LORA signer certificate definition.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.22 tnglora\_cert\_def\_2\_device.c File Reference

TNG LORA device certificate definition.

```
#include "atcacert/atcacert_def.h"  
#include "tngtls_cert_def_2_device.h"  
#include "tngtls_cert_def_1_signer.h"  
#include "tnglora_cert_def_1_signer.h"  
#include "tnglora_cert_def_2_device.h"
```

## Variables

- SHARED\_LIB\_EXPORT const [atcacert\\_def\\_t](#) **g\_tnqlora\_cert\_def\_2\_device**

### 22.22.1 Detailed Description

TNG LORA device certificate definition.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.23 tnqlora\_cert\_def\_2\_device.h File Reference

TNG LORA device certificate definition.

```
#include "atcacert/atcacert_def.h"
```

## Variables

- ATCA\_DLL const [atcacert\\_def\\_t](#) **g\_tnqlora\_cert\_def\_2\_device**

### 22.23.1 Detailed Description

TNG LORA device certificate definition.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.24 tnqlora\_cert\_def\_4\_device.c File Reference

TNG LORA device certificate definition.

```
#include "atcacert/atcacert_def.h"  
#include "tnqlora_cert_def_4_device.h"  
#include "tnqlora_cert_def_1_signer.h"
```

## Variables

- SHARED\_LIB\_EXPORT const uint8\_t **g\_tnqlora\_cert\_template\_4\_device** [552]
- SHARED\_LIB\_EXPORT const [atcacert\\_cert\\_element\\_t](#) **g\_tnqlora\_cert\_elements\_4\_device** []
- SHARED\_LIB\_EXPORT const [atcacert\\_def\\_t](#) **g\_tnqlora\_cert\_def\_4\_device**

### 22.24.1 Detailed Description

TNG LORA device certificate definition.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.25 tnglora\_cert\_def\_4\_device.h File Reference

TNG LORA device certificate definition.

```
#include "atcacert/atcacert_def.h"
```

- #define **TNGLORA\_CERT\_TEMPLATE\_4\_DEVICE\_SIZE** 552
- ATCA\_DLL const [atcacert\\_def\\_t](#) **g\_tnglora\_cert\_def\_4\_device**
- SHARED\_LIB\_EXPORT const uint8\_t **g\_tnglora\_cert\_template\_4\_device** []
- SHARED\_LIB\_EXPORT const [atcacert\\_cert\\_element\\_t](#) **g\_tnglora\_cert\_elements\_4\_device** []

### 22.25.1 Detailed Description

TNG LORA device certificate definition.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.26 tngtls\_cert\_def\_1\_signer.c File Reference

TNG TLS signer certificate definition.

```
#include "atcacert/atcacert_def.h"  
#include "tngtls_cert_def_1_signer.h"
```

### Variables

- SHARED\_LIB\_EXPORT const uint8\_t **g\_tngtls\_cert\_template\_1\_signer** [520]
- SHARED\_LIB\_EXPORT const [atcacert\\_cert\\_element\\_t](#) **g\_tngtls\_cert\_elements\_1\_signer** []
- SHARED\_LIB\_EXPORT const [atcacert\\_def\\_t](#) **g\_tngtls\_cert\_def\_1\_signer**

### 22.26.1 Detailed Description

TNG TLS signer certificate definition.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.26.2 Variable Documentation

### 22.26.2.1 g\_tngtls\_cert\_elements\_1\_signer

```
SHARED_LIB_EXPORT const atcacert_cert_element_t g_tngtls_cert_elements_1_signer[]
```

#### Initial value:

```
= {
    {
        .id = "subject",
        .device_loc = {
            .zone = DEVZONE_NONE,
        },
        .cert_loc = {
            .offset = 158,
            .count = 81
        }
    }
}
```

## 22.27 tngtls\_cert\_def\_1\_signer.h File Reference

TNG TLS signer certificate definition.

```
#include "atcacert/atcacert_def.h"
```

- #define TNGTLS\_CERT\_TEMPLATE\_1\_SIGNER\_SIZE 520
- ATCA\_DLL const atcacert\_def\_t g\_tngtls\_cert\_def\_1\_signer
- SHARED\_LIB\_EXPORT const uint8\_t g\_tngtls\_cert\_template\_1\_signer []
- SHARED\_LIB\_EXPORT const atcacert\_cert\_element\_t g\_tngtls\_cert\_elements\_1\_signer []

### 22.27.1 Detailed Description

TNG TLS signer certificate definition.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.28 tngtls\_cert\_def\_2\_device.c File Reference

TNG TLS device certificate definition.

```
#include "atcacert/atcacert_def.h"
#include "tngtls_cert_def_2_device.h"
#include "tngtls_cert_def_1_signer.h"
```

### Variables

- SHARED\_LIB\_EXPORT const uint8\_t **g\_tngtls\_cert\_template\_2\_device** [505]
- SHARED\_LIB\_EXPORT const [atcacert\\_cert\\_element\\_t](#) **g\_tngtls\_cert\_elements\_2\_device** [2]
- SHARED\_LIB\_EXPORT const [atcacert\\_def\\_t](#) **g\_tngtls\_cert\_def\_2\_device**

### 22.28.1 Detailed Description

TNG TLS device certificate definition.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.29 tngtls\_cert\_def\_2\_device.h File Reference

TNG TLS device certificate definition.

```
#include "atcacert/atcacert_def.h"
```

- #define **TNGTLS\_CERT\_TEMPLATE\_2\_DEVICE\_SIZE** 505
- #define **TNGTLS\_CERT\_ELEMENTS\_2\_DEVICE\_COUNT** 2
- ATCA\_DLL const [atcacert\\_def\\_t](#) **g\_tngtls\_cert\_def\_2\_device**
- SHARED\_LIB\_EXPORT const uint8\_t **g\_tngtls\_cert\_template\_2\_device** []
- SHARED\_LIB\_EXPORT const [atcacert\\_cert\\_element\\_t](#) **g\_tngtls\_cert\_elements\_2\_device** []

### 22.29.1 Detailed Description

TNG TLS device certificate definition.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.30 tngtls\_cert\_def\_3\_device.c File Reference

TNG TLS device certificate definition.

```
#include "atcacert/atcacert_def.h"  
#include "tngtls_cert_def_3_device.h"  
#include "tngtls_cert_def_1_signer.h"
```



## Variables

- SHARED\_LIB\_EXPORT const uint8\_t **g\_tngtls\_cert\_template\_3\_device** [546]
- SHARED\_LIB\_EXPORT const [atcacert\\_cert\\_element\\_t](#) **g\_tngtls\_cert\_elements\_3\_device** []
- SHARED\_LIB\_EXPORT const [atcacert\\_def\\_t](#) **g\_tngtls\_cert\_def\_3\_device**

### 22.30.1 Detailed Description

TNG TLS device certificate definition.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.31 tngtls\_cert\_def\_3\_device.h File Reference

TNG TLS device certificate definition.

```
#include "atcacert/atcacert_def.h"
```

- #define **TNGTLS\_CERT\_TEMPLATE\_3\_DEVICE\_SIZE** 546
- ATCA\_DLL const [atcacert\\_def\\_t](#) **g\_tngtls\_cert\_def\_3\_device**
- ATCA\_DLL const uint8\_t **g\_tngtls\_cert\_template\_3\_device** []
- ATCA\_DLL const [atcacert\\_cert\\_element\\_t](#) **g\_tngtls\_cert\_elements\_3\_device** []

### 22.31.1 Detailed Description

TNG TLS device certificate definition.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.32 wpc\_apis.c File Reference

Provides api interfaces for WPC authentication.

```
#include "cryptoauthlib.h"
#include "wpc_apis.h"
#include "wpccert_client.h"
#include "atcacert/atcacert_client.h"
```

### 22.32.1 Detailed Description

Provides api interfaces for WPC authentication.

#### Copyright

(c) 2015-2021 Microchip Technology Inc. and its subsidiaries.

## 22.33 wpc\_apis.h File Reference

Provides api interfaces for WPC authentication.

```
#include "wpc_check_config.h"
```

### Macros

- `#define WPC_PROTOCOL_VERSION 0x01`
- `#define WPC_PROTOCOL_MAX_VERSION 0x01`
- `#define WPC_TBS_AUTH_PREFIX 0x41`
- `#define WPC_CONST_N_RH ATCA_SHA256_DIGEST_SIZE`
- `#define WPC_CONST_OS_MC (2 + WPC_CONST_N_RH)`
- `#define WPC_HEADER(x) ((WPC_PROTOCOL_VERSION << 4) | x)`
- `#define WPC_GET_DIGESTS_TYPE 0x09`
- `#define WPC_GET_DIGESTS_HEADER WPC_HEADER(WPC_GET_DIGESTS_TYPE)`
- `#define WPC_GET_DIGESTS_LENGTH (2)`
- `#define WPC_GET_CERTIFICATE_TYPE 0x0A`
- `#define WPC_GET_CERTIFICATE_HEADER WPC_HEADER(WPC_GET_CERTIFICATE_TYPE)`
- `#define WPC_GET_CERTIFICATE_LENGTH (4)`
- `#define WPC_CHALLENGE_TYPE 0x0B`
- `#define WPC_CHALLENGE_HEADER WPC_HEADER(WPC_CHALLENGE_TYPE)`
- `#define WPC_CHALLENGE_NONCE_LENGTH (16)`
- `#define WPC_CHALLENGE_LENGTH (2 + WPC_CHALLENGE_NONCE_LENGTH)`
- `#define WPC_DIGESTS_TYPE 0x01`
- `#define WPC_DIGESTS_HEADER WPC_HEADER(WPC_DIGESTS_TYPE)`
- `#define WPC_DIGESTS_LENGTH(x) (2 + (ATCA_SHA256_DIGEST_SIZE * x))`
- `#define WPC_CERTIFICATE_TYPE 0x02`
- `#define WPC_CERTIFICATE_HEADER WPC_HEADER(WPC_CERTIFICATE_TYPE)`
- `#define WPC_CERTIFICATE_LENGTH(x) (1 + x)`
- `#define WPC_CHALLENGE_AUTH_TYPE 0x03`
- `#define WPC_CHALLENGE_AUTH_HEADER WPC_HEADER(WPC_CHALLENGE_AUTH_TYPE)`
- `#define WPC_CHALLENGE_AUTH_LENGTH (67)`
- `#define WPC_ERROR_TYPE 0x07`
- `#define WPC_ERROR_HEADER WPC_HEADER(WPC_ERROR_TYPE)`
- `#define WPC_ERROR_LENGTH (3)`
- `#define WPC_ERROR_INVALID_REQUEST (0x01)`
- `#define WPC_ERROR_UNSUPPORTED_PROTOCOL (0x02)`
- `#define WPC_ERROR_BUSY (0x03)`
- `#define WPC_ERROR_UNSPECIFIED (0x04)`

## Variables

- `const uint8_t g_root_ca_digest []`

### 22.33.1 Detailed Description

Provides api interfaces for WPC authentication.

#### Copyright

(c) 2015-2021 Microchip Technology Inc. and its subsidiaries.

## 22.34 wpccert\_client.c File Reference

Provides api interfaces for accessing WPC certificates from device.

```
#include "wpc_check_config.h"
#include "wpccert_client.h"
#include "atcacert/atcacert_def.h"
#include "atcacert/atcacert_der.h"
#include "atcacert/atcacert_client.h"
#include "atca_basic.h"
```

## Functions

- ATCA\_STATUS `wpccert_read_cert` ([ATCADevice](#) device, const [atcacert\\_def\\_t](#) \*cert\_def, uint8\_t \*cert, size\_t \*cert\_size)  
*WPC API -.*
- ATCA\_STATUS `wpccert_read_pdu_cert` ([ATCADevice](#) device, uint8\_t \*cert, size\_t \*cert\_size, uint8\_t slot)
- ATCA\_STATUS `wpccert_read_mfg_cert` ([ATCADevice](#) device, uint8\_t \*cert, size\_t \*cert\_size, uint8\_t slot)
- ATCA\_STATUS `wpccert_public_key` (const [atcacert\\_def\\_t](#) \*cert\_def, uint8\_t \*public\_key, uint8\_t \*cert)

### 22.34.1 Detailed Description

Provides api interfaces for accessing WPC certificates from device.

#### Copyright

(c) 2015-2021 Microchip Technology Inc. and its subsidiaries.

### 22.34.2 Function Documentation

### 22.34.2.1 wpccert\_read\_cert()

```
ATCA_STATUS wpccert_read_cert (
    ATCADevice device,
    const atcacert_def_t * cert_def,
    uint8_t * cert,
    size_t * cert_size )
```

WPC API -.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

## 22.35 wpccert\_client.h File Reference

Provides api interfaces for accessing WPC certificates from device.

```
#include "cryptoauthlib.h"
#include "atcacert/atcacert_def.h"
```

### Functions

- uint8\_t **wpccert\_get\_slots\_populated** (void)
- uint8\_t **wpccert\_get\_slot\_count** (void)
- ATCA\_STATUS **wpccert\_get\_slot\_info** (uint16\_t \*dig\_handle, const atcacert\_def\_t \*\*def, uint8\_t slot)
- ATCA\_STATUS **wpccert\_read\_cert** (ATCADevice device, const atcacert\_def\_t \*cert\_def, uint8\_t \*cert, size\_t \*cert\_size)  
WPC API -.
- ATCA\_STATUS **wpccert\_write\_cert** (ATCADevice device, const atcacert\_def\_t \*cert\_def, const uint8\_t \*cert, size\_t cert\_size)
- ATCA\_STATUS **wpccert\_read\_pdu\_cert** (ATCADevice device, uint8\_t \*cert, size\_t \*cert\_size, uint8\_t slot)
- ATCA\_STATUS **wpccert\_read\_mfg\_cert** (ATCADevice device, uint8\_t \*cert, size\_t \*cert\_size, uint8\_t slot)
- ATCA\_STATUS **wpccert\_public\_key** (const atcacert\_def\_t \*cert\_def, uint8\_t \*public\_key, uint8\_t \*cert)

### 22.35.1 Detailed Description

Provides api interfaces for accessing WPC certificates from device.

#### Copyright

(c) 2015-2021 Microchip Technology Inc. and its subsidiaries.

### 22.35.2 Function Documentation

### 22.35.2.1 wpccert\_read\_cert()

```
ATCA_STATUS wpccert_read_cert (
    ATCADevice device,
    const atcacert_def_t * cert_def,
    uint8_t * cert,
    size_t * cert_size )
```

WPC API -.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

## 22.36 atca\_basic.c File Reference

CryptoAuthLib Basic API methods. These methods provide a simpler way to access the core crypto methods.

```
#include "atca_basic.h"
#include "atca_version.h"
```

### Functions

- ATCA\_STATUS [atcab\\_version](#) (char \*ver\_str)  
*basic API methods are all prefixed with atcab\_ (CryptoAuthLib Basic) the fundamental premise of the basic API is it is based on a single interface instance and that instance is global, so all basic API commands assume that one global device is the one to operate on.*
- ATCA\_STATUS [atcab\\_init\\_ext](#) (ATCADevice \*device, ATCAIfaceCfg \*cfg)  
*Creates and initializes a ATCADevice context.*
- ATCA\_STATUS [atcab\\_init](#) (ATCAIfaceCfg \*cfg)  
*Creates a global ATCADevice object used by Basic API.*
- ATCA\_STATUS [atcab\\_init\\_device](#) (ATCADevice ca\_device)  
*Initialize the global ATCADevice object to point to one of your choosing for use with all the atcab\_ basic API.*
- ATCA\_STATUS [atcab\\_release\\_ext](#) (ATCADevice \*device)  
*release (free) the an ATCADevice instance.*
- ATCA\_STATUS [atcab\\_release](#) (void)  
*release (free) the global ATCADevice instance. This must be called in order to release or free up the interface.*
- [ATCADevice atcab\\_get\\_device](#) (void)  
*Get the global device object.*
- ATCADeviceType [atcab\\_get\\_device\\_type\\_ext](#) (ATCADevice device)  
*Get the selected device type of rthe device context.*
- ATCADeviceType [atcab\\_get\\_device\\_type](#) (void)  
*Get the current device type configured for the global ATCADevice.*
- uint8\_t [atcab\\_get\\_device\\_address](#) (ATCADevice device)  
*Get the current device address based on the configured device and interface.*
- bool [atcab\\_is\\_ca\\_device](#) (ATCADeviceType dev\_type)  
*Check whether the device is cryptoauth device.*
- bool [atcab\\_is\\_ca2\\_device](#) (ATCADeviceType dev\_type)  
*Check whether the device is cryptoauth device.*

- bool [atcab\\_is\\_ta\\_device](#) (ATCADeviceType dev\_type)  
*Check whether the device is Trust Anchor device.*
- ATCA\_STATUS [atcab\\_wakeup](#) (void)  
*wakeup the CryptoAuth device*
- ATCA\_STATUS [atcab\\_idle](#) (void)  
*idle the CryptoAuth device*
- ATCA\_STATUS [atcab\\_sleep](#) (void)  
*invoke sleep on the CryptoAuth device*
- ATCA\_STATUS [atcab\\_get\\_zone\\_size\\_ext](#) (ATCADevice device, uint8\_t zone, uint16\_t slot, size\_t \*size)  
*Gets the size of the specified zone in bytes.*
- ATCA\_STATUS [atcab\\_get\\_zone\\_size](#) (uint8\_t zone, uint16\_t slot, size\_t \*size)  
*Gets the size of the specified zone in bytes.*
- ATCA\_STATUS [atcab\\_aes](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*aes\_in, uint8\_t \*aes\_out)  
*Compute the AES-128 encrypt, decrypt, or GFM calculation.*
- ATCA\_STATUS [atcab\\_aes\\_encrypt\\_ext](#) (ATCADevice device, uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*plaintext, uint8\_t \*ciphertext)  
*Perform an AES-128 encrypt operation with a key in the device.*
- ATCA\_STATUS [atcab\\_aes\\_encrypt](#) (uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*plaintext, uint8\_t \*ciphertext)  
*Perform an AES-128 encrypt operation with a key in the device.*
- ATCA\_STATUS [atcab\\_aes\\_decrypt\\_ext](#) (ATCADevice device, uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*ciphertext, uint8\_t \*plaintext)  
*Perform an AES-128 decrypt operation with a key in the device.*
- ATCA\_STATUS [atcab\\_aes\\_decrypt](#) (uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*ciphertext, uint8\_t \*plaintext)  
*Perform an AES-128 decrypt operation with a key in the device.*
- ATCA\_STATUS [atcab\\_aes\\_gfm](#) (const uint8\_t \*h, const uint8\_t \*input, uint8\_t \*output)  
*Perform a Galois Field Multiply (GFM) operation.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_init\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*iv, size\_t iv\_size)  
*Initialize context for AES GCM operation with an existing IV, which is common when starting a decrypt operation.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_init](#) (atca\_aes\_gcm\_ctx\_t \*ctx, uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*iv, size\_t iv\_size)  
*Initialize context for AES GCM operation with an existing IV, which is common when starting a decrypt operation.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_init\\_rand](#) (atca\_aes\_gcm\_ctx\_t \*ctx, uint16\_t key\_id, uint8\_t key\_block, size\_t rand\_size, const uint8\_t \*free\_field, size\_t free\_field\_size, uint8\_t \*iv)  
*Initialize context for AES GCM operation with a IV composed of a random and optional fixed(free) field, which is common when starting an encrypt operation.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_aad\\_update\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*aad, uint32\_t aad\_size)  
*Process Additional Authenticated Data (AAD) using GCM mode and a key within the ATECC608 device.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_aad\\_update](#) (atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*aad, uint32\_t aad\_size)  
*Process Additional Authenticated Data (AAD) using GCM mode and a key within the ATECC608 device.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_encrypt\\_update\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*plaintext, uint32\_t plaintext\_size, uint8\_t \*ciphertext)  
*Encrypt data using GCM mode and a key within the ATECC608 device. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_encrypt\\_update](#) (atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*plaintext, uint32\_t plaintext\_size, uint8\_t \*ciphertext)  
*Encrypt data using GCM mode and a key within the ATECC608 device. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function.*

- ATCA\_STATUS [atcab\\_aes\\_gcm\\_encrypt\\_finish\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, uint8\_t \*tag, size\_t tag\_size)  
*Complete a GCM encrypt operation returning the authentication tag.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_encrypt\\_finish](#) (atca\_aes\_gcm\_ctx\_t \*ctx, uint8\_t \*tag, size\_t tag\_size)  
*Complete a GCM encrypt operation returning the authentication tag.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_decrypt\\_update\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*ciphertext, uint32\_t ciphertext\_size, uint8\_t \*plaintext)  
*Decrypt data using GCM mode and a key within the ATECC608 device. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_decrypt\\_update](#) (atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*ciphertext, uint32\_t ciphertext\_size, uint8\_t \*plaintext)  
*Decrypt data using GCM mode and a key within the ATECC608 device. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_decrypt\\_finish\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*tag, size\_t tag\_size, bool \*is\_verified)  
*Complete a GCM decrypt operation verifying the authentication tag.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_decrypt\\_finish](#) (atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*tag, size\_t tag\_size, bool \*is\_verified)  
*Complete a GCM decrypt operation verifying the authentication tag.*
- ATCA\_STATUS [atcab\\_checkmac](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*challenge, const uint8\_t \*response, const uint8\_t \*other\_data)  
*Compares a MAC response with input values.*
- ATCA\_STATUS [atcab\\_checkmac\\_with\\_response\\_mac](#) (uint8\_t mode, const uint8\_t \*challenge, const uint8\_t \*response, const uint8\_t \*other\_data, uint8\_t \*mac)  
*Compares a MAC response with input values. SHA105 device can generate optional mac Output response mac mode only supports in SHA105 device.*
- ATCA\_STATUS [atcab\\_counter](#) (uint8\_t mode, uint16\_t counter\_id, uint32\_t \*counter\_value)  
*Compute the Counter functions.*
- ATCA\_STATUS [atcab\\_counter\\_increment](#) (uint16\_t counter\_id, uint32\_t \*counter\_value)  
*Increments one of the device's monotonic counters.*
- ATCA\_STATUS [atcab\\_counter\\_read](#) (uint16\_t counter\_id, uint32\_t \*counter\_value)  
*Read one of the device's monotonic counters.*
- ATCA\_STATUS [atcab\\_derivekey\\_ext](#) (ATCADevice device, uint8\_t mode, uint16\_t key\_id, const uint8\_t \*mac)  
*Executes the DeviveKey command for deriving a new key from a nonce (TempKey) and an existing key.*
- ATCA\_STATUS [atcab\\_derivekey](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*mac)  
*Executes the DeviveKey command for deriving a new key from a nonce (TempKey) and an existing key.*
- ATCA\_STATUS [atcab\\_ecdh\\_base](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*public\_key, uint8\_t \*pms, uint8\_t \*out\_nonce)  
*Base function for generating premaster secret key using ECDH.*
- ATCA\_STATUS [atcab\\_ecdh](#) (uint16\_t key\_id, const uint8\_t \*public\_key, uint8\_t \*pms)  
*ECDH command with a private key in a slot and the premaster secret is returned in the clear.*
- ATCA\_STATUS [atcab\\_ecdh\\_enc](#) (uint16\_t key\_id, const uint8\_t \*public\_key, uint8\_t \*pms, const uint8\_t \*read\_key, uint16\_t read\_key\_id, const uint8\_t num\_in[(20)])  
*ECDH command with a private key in a slot and the premaster secret is read from the next slot.*
- ATCA\_STATUS [atcab\\_ecdh\\_ioenc](#) (uint16\_t key\_id, const uint8\_t \*public\_key, uint8\_t \*pms, const uint8\_t \*io\_key)  
*ECDH command with a private key in a slot and the premaster secret is returned encrypted using the IO protection key.*
- ATCA\_STATUS [atcab\\_ecdh\\_tempkey](#) (const uint8\_t \*public\_key, uint8\_t \*pms)  
*ECDH command with a private key in TempKey and the premaster secret is returned in the clear.*
- ATCA\_STATUS [atcab\\_ecdh\\_tempkey\\_ioenc](#) (const uint8\_t \*public\_key, uint8\_t \*pms, const uint8\_t \*io\_key)  
*ECDH command with a private key in TempKey and the premaster secret is returned encrypted using the IO protection key.*

- ATCA\_STATUS [atcab\\_gendig](#) (uint8\_t zone, uint16\_t key\_id, const uint8\_t \*other\_data, uint8\_t other\_data\_size)
 

*Issues a GenDig command, which performs a SHA256 hash on the source data indicated by zone with the contents of TempKey. See the CryptoAuth datasheet for your chip to see what the values of zone correspond to.*
- ATCA\_STATUS [atcab\\_gendivkey](#) (const uint8\_t \*other\_data)
 

*Issues a GenDivKey command to generate the equivalent diversified key as that programmed into the client side device.*
- ATCA\_STATUS [atcab\\_genkey\\_base](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*other\_data, uint8\_t \*public\_key)
 

*Issues GenKey command, which can generate a private key, compute a public key, and/or compute a digest of a public key.*
- ATCA\_STATUS [atcab\\_genkey\\_ext](#) (ATCADevice device, uint16\_t key\_id, uint8\_t \*public\_key)
 

*Issues GenKey command, which generates a new random private key in slot/handle and returns the public key.*
- ATCA\_STATUS [atcab\\_genkey](#) (uint16\_t key\_id, uint8\_t \*public\_key)
 

*Issues GenKey command, which generates a new random private key in slot/handle and returns the public key.*
- ATCA\_STATUS [atcab\\_get\\_pubkey\\_ext](#) (ATCADevice device, uint16\_t key\_id, uint8\_t \*public\_key)
 

*Uses GenKey command to calculate the public key from an existing private key in a slot.*
- ATCA\_STATUS [atcab\\_get\\_pubkey](#) (uint16\_t key\_id, uint8\_t \*public\_key)
 

*Uses GenKey command to calculate the public key from an existing private key in a slot.*
- ATCA\_STATUS [atcab\\_hmac](#) (uint8\_t mode, uint16\_t key\_id, uint8\_t \*digest)
 

*Issues a HMAC command, which computes an HMAC/SHA-256 digest of a key stored in the device, a challenge, and other information on the device.*
- ATCA\_STATUS [atcab\\_info\\_base](#) (uint8\_t mode, uint16\_t param2, uint8\_t \*out\_data)
 

*Issues an Info command, which return internal device information and can control GPIO and the persistent latch.*
- ATCA\_STATUS [atcab\\_info\\_ext](#) (ATCADevice device, uint8\_t \*revision)
 

*Use the Info command to get the device revision (DevRev).*
- ATCA\_STATUS [atcab\\_info](#) (uint8\_t \*revision)
 

*Use the Info command to get the device revision (DevRev).*
- ATCA\_STATUS [atcab\\_info\\_lock\\_status](#) (uint16\_t param2, uint8\_t \*is\_locked)
 

*Use the Info command to get the lock status.*
- ATCA\_STATUS [atcab\\_info\\_chip\\_status](#) (uint8\_t \*chip\_status)
 

*Use the Info command to get the chip status.*
- ATCA\_STATUS [atcab\\_info\\_set\\_latch](#) (bool state)
 

*Use the Info command to set the persistent latch state for an ATECC608 device.*
- ATCA\_STATUS [atcab\\_info\\_get\\_latch](#) (bool \*state)
 

*Use the Info command to get the persistent latch current state for an ATECC608 device.*
- ATCA\_STATUS [atcab\\_kdf](#) (uint8\_t mode, uint16\_t key\_id, const uint32\_t details, const uint8\_t \*message, uint8\_t \*out\_data, uint8\_t \*out\_nonce)
 

*Executes the KDF command, which derives a new key in PRF, AES, or HKDF modes.*
- ATCA\_STATUS [atcab\\_lock](#) (uint8\_t mode, uint16\_t summary\_crc)
 

*The Lock command prevents future modifications of the Configuration and/or Data and OTP zones. If the device is so configured, then this command can be used to lock individual data slots. This command fails if the designated area is already locked.*
- ATCA\_STATUS [atcab\\_lock\\_config\\_zone\\_ext](#) (ATCADevice device)
 

*Unconditionally (no CRC required) lock the config zone.*
- ATCA\_STATUS [atcab\\_lock\\_config\\_zone](#) (void)
 

*Unconditionally (no CRC required) lock the config zone.*
- ATCA\_STATUS [atcab\\_lock\\_config\\_zone\\_crc](#) (uint16\_t summary\_crc)
 

*Lock the config zone with summary CRC.*
- ATCA\_STATUS [atcab\\_lock\\_data\\_zone\\_ext](#) (ATCADevice device)
 

*Unconditionally (no CRC required) lock the data zone (slots and OTP). for CryptoAuth devices and lock the setup for Trust Anchor device.*



- ATCA\_STATUS [atcab\\_lock\\_data\\_zone](#) (void)  
*Unconditionally (no CRC required) lock the data zone (slots and OTP). for CryptoAuth devices and lock the setup for Trust Anchor device.*
- ATCA\_STATUS [atcab\\_lock\\_data\\_zone\\_crc](#) (uint16\_t summary\_crc)  
*Lock the data zone (slots and OTP) with summary CRC.*
- ATCA\_STATUS [atcab\\_lock\\_data\\_slot\\_ext](#) (ATCADevice device, uint16\_t slot)  
*Lock an individual slot in the data zone on an ATECC device. Not available for ATSHA devices. Slot must be configured to be slot lockable (KeyConfig.Lockable=1) (for cryptoauth devices) or Lock an individual handle in shared data element on an Trust Anchor device (for Trust Anchor devices).*
- ATCA\_STATUS [atcab\\_lock\\_data\\_slot](#) (uint16\_t slot)  
*Lock an individual slot in the data zone on an ATECC device. Not available for ATSHA devices. Slot must be configured to be slot lockable (KeyConfig.Lockable=1) (for cryptoauth devices) or Lock an individual handle in shared data element on an Trust Anchor device (for Trust Anchor devices).*
- ATCA\_STATUS [atcab\\_mac](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*challenge, uint8\_t \*digest)  
*Executes MAC command, which computes a SHA-256 digest of a key stored in the device, a challenge, and other information on the device.*
- ATCA\_STATUS [atcab\\_nonce\\_base](#) (uint8\_t mode, uint16\_t zero, const uint8\_t \*num\_in, uint8\_t \*rand\_out)  
*Executes Nonce command, which loads a random or fixed nonce/data into the device for use by subsequent commands.*
- ATCA\_STATUS [atcab\\_nonce](#) (const uint8\_t \*num\_in)  
*Execute a Nonce command in pass-through mode to initialize TempKey to a specified value.*
- ATCA\_STATUS [atcab\\_nonce\\_load](#) (uint8\_t target, const uint8\_t \*num\_in, uint16\_t num\_in\_size)  
*Execute a Nonce command in pass-through mode to load one of the device's internal buffers with a fixed value.*
- ATCA\_STATUS [atcab\\_nonce\\_rand\\_ext](#) (ATCADevice device, const uint8\_t \*num\_in, uint8\_t \*rand\_out)  
*Execute a Nonce command to generate a random nonce combining a host nonce (num\_in) and a device random number.*
- ATCA\_STATUS [atcab\\_nonce\\_rand](#) (const uint8\_t \*num\_in, uint8\_t \*rand\_out)  
*Execute a Nonce command to generate a random nonce combining a host nonce (num\_in) and a device random number.*
- ATCA\_STATUS [atcab\\_challenge](#) (const uint8\_t \*num\_in)  
*Execute a Nonce command in pass-through mode to initialize TempKey to a specified value.*
- ATCA\_STATUS [atcab\\_challenge\\_seed\\_update](#) (const uint8\_t \*num\_in, uint8\_t \*rand\_out)  
*Execute a Nonce command to generate a random challenge combining a host nonce (num\_in) and a device random number.*
- ATCA\_STATUS [atcab\\_priv\\_write](#) (uint16\_t key\_id, const uint8\_t priv\_key[36], uint16\_t write\_key\_id, const uint8\_t write\_key[32], const uint8\_t num\_in[(20)])  
*Executes PrivWrite command, to write externally generated ECC private keys into the device.*
- ATCA\_STATUS [atcab\\_random\\_ext](#) (ATCADevice device, uint8\_t \*rand\_out)  
*Executes Random command, which generates a 32 byte random number from the device.*
- ATCA\_STATUS [atcab\\_random](#) (uint8\_t \*rand\_out)  
*Executes Random command, which generates a 32 byte random number from the device.*
- ATCA\_STATUS [atcab\\_read\\_zone\\_ext](#) (ATCADevice device, uint8\_t zone, uint16\_t slot, uint8\_t block, uint8\_t offset, uint8\_t \*data, uint8\_t len)  
*Executes Read command, which reads either 4 or 32 bytes of data from a given slot, configuration zone, or the OTP zone.*
- ATCA\_STATUS [atcab\\_read\\_zone](#) (uint8\_t zone, uint16\_t slot, uint8\_t block, uint8\_t offset, uint8\_t \*data, uint8\_t len)  
*Executes Read command, which reads either 4 or 32 bytes of data from a given slot, configuration zone, or the OTP zone.*
- ATCA\_STATUS [atcab\\_is\\_locked](#) (uint8\_t zone, bool \*is\_locked)  
*Executes Read command, which reads the configuration zone to see if the specified zone is locked.*
- ATCA\_STATUS [atcab\\_is\\_config\\_locked\\_ext](#) (ATCADevice device, bool \*is\_locked)  
*This function check whether configuration zone is locked or not.*

- ATCA\_STATUS [atcab\\_is\\_config\\_locked](#) (bool \*is\_locked)  
*This function check whether configuration zone is locked or not.*
- ATCA\_STATUS [atcab\\_is\\_data\\_locked\\_ext](#) (ATCADevice device, bool \*is\_locked)  
*This function check whether data/setup zone is locked or not.*
- ATCA\_STATUS [atcab\\_is\\_data\\_locked](#) (bool \*is\_locked)  
*This function check whether data/setup zone is locked or not.*
- ATCA\_STATUS [atcab\\_is\\_slot\\_locked\\_ext](#) (ATCADevice device, uint16\_t slot, bool \*is\_locked)  
*This function check whether slot/handle is locked or not.*
- ATCA\_STATUS [atcab\\_is\\_slot\\_locked](#) (uint16\_t slot, bool \*is\_locked)  
*This function check whether slot/handle is locked or not.*
- ATCA\_STATUS [atcab\\_is\\_private\\_ext](#) (ATCADevice device, uint16\_t slot, bool \*is\_private)  
*Check to see if the key is a private key or not.*
- ATCA\_STATUS [atcab\\_is\\_private](#) (uint16\_t slot, bool \*is\_private)
- ATCA\_STATUS [atcab\\_read\\_bytes\\_zone\\_ext](#) (ATCADevice device, uint8\_t zone, uint16\_t slot, size\_t offset, uint8\_t \*data, size\_t length)
- ATCA\_STATUS [atcab\\_read\\_bytes\\_zone](#) (uint8\_t zone, uint16\_t slot, size\_t offset, uint8\_t \*data, size\_t length)  
*Used to read an arbitrary number of bytes from any zone configured for clear reads.*
- ATCA\_STATUS [atcab\\_read\\_serial\\_number\\_ext](#) (ATCADevice device, uint8\_t \*serial\_number)  
*This function returns serial number of the device.*
- ATCA\_STATUS [atcab\\_read\\_serial\\_number](#) (uint8\_t \*serial\_number)  
*This function returns serial number of the device.*
- ATCA\_STATUS [atcab\\_read\\_pubkey\\_ext](#) (ATCADevice device, uint16\_t slot, uint8\_t \*public\_key)  
*Executes Read command to read an ECC P256 public key from a slot configured for clear reads.*
- ATCA\_STATUS [atcab\\_read\\_pubkey](#) (uint16\_t slot, uint8\_t \*public\_key)  
*Executes Read command to read an ECC P256 public key from a slot configured for clear reads.*
- ATCA\_STATUS [atcab\\_read\\_sig](#) (uint16\_t slot, uint8\_t \*sig)  
*Executes Read command to read a 64 byte ECDSA P256 signature from a slot configured for clear reads.*
- ATCA\_STATUS [atcab\\_read\\_config\\_zone\\_ext](#) (ATCADevice device, uint8\_t \*config\_data)  
*Executes Read command to read the complete device configuration zone.*
- ATCA\_STATUS [atcab\\_read\\_config\\_zone](#) (uint8\_t \*config\_data)  
*Executes Read command to read the complete device configuration zone.*
- ATCA\_STATUS [atcab\\_cmp\\_config\\_zone](#) (uint8\_t \*config\_data, bool \*same\_config)  
*Compares a specified configuration zone with the configuration zone currently on the device.*
- ATCA\_STATUS [atcab\\_read\\_enc](#) (uint16\_t key\_id, uint8\_t block, uint8\_t \*data, const uint8\_t \*enc\_key, const uint16\_t enc\_key\_id, const uint8\_t num\_in[(20)])  
*Executes Read command on a slot configured for encrypted reads and decrypts the data to return it as plaintext.*
- ATCA\_STATUS [atcab\\_secureboot](#) (uint8\_t mode, uint16\_t param2, const uint8\_t \*digest, const uint8\_t \*signature, uint8\_t \*mac)  
*Executes Secure Boot command, which provides support for secure boot of an external MCU or MPU.*
- ATCA\_STATUS [atcab\\_secureboot\\_mac](#) (uint8\_t mode, const uint8\_t \*digest, const uint8\_t \*signature, const uint8\_t \*num\_in, const uint8\_t \*io\_key, bool \*is\_verified)  
*Executes Secure Boot command with encrypted digest and validated MAC response using the IO protection key.*
- ATCA\_STATUS [atcab\\_selftest](#) (uint8\_t mode, uint16\_t param2, uint8\_t \*result)  
*Executes the SelfTest command, which performs a test of one or more of the cryptographic engines within the ATECC608 chip.*
- ATCA\_STATUS [atcab\\_sha\\_base](#) (uint8\_t mode, uint16\_t length, const uint8\_t \*data\_in, uint8\_t \*data\_out, uint16\_t \*data\_out\_size)  
*Executes SHA command, which computes a SHA-256 or HMAC/SHA-256 digest for general purpose use by the host system.*
- ATCA\_STATUS [atcab\\_sha\\_start](#) (void)  
*Executes SHA command to initialize SHA-256 calculation engine.*
- ATCA\_STATUS [atcab\\_sha\\_update](#) (const uint8\_t \*message)

- Executes SHA command to add 64 bytes of message data to the current context.*

  - ATCA\_STATUS [atcab\\_sha\\_end](#) (uint8\_t \*digest, uint16\_t length, const uint8\_t \*message)
- Executes SHA command to complete SHA-256 or HMAC/SHA-256 operation.*

  - ATCA\_STATUS [atcab\\_sha\\_read\\_context](#) (uint8\_t \*context, uint16\_t \*context\_size)

*Executes SHA command to read the SHA-256 context back. Only for ATECC608 with SHA-256 contexts. HMAC not supported.*
- ATCA\_STATUS [atcab\\_sha\\_write\\_context](#) (const uint8\_t \*context, uint16\_t context\_size)

*Executes SHA command to write (restore) a SHA-256 context into the the device. Only supported for ATECC608 with SHA-256 contexts.*
- ATCA\_STATUS [atcab\\_sha](#) (uint16\_t length, const uint8\_t \*message, uint8\_t \*digest)

*Use the SHA command to compute a SHA-256 digest.*
- ATCA\_STATUS [atcab\\_hw\\_sha2\\_256](#) (const uint8\_t \*data, size\_t data\_size, uint8\_t \*digest)

*Use the SHA command to compute a SHA-256 digest.*
- ATCA\_STATUS [atcab\\_hw\\_sha2\\_256\\_init](#) (atca\_sha256\_ctx\_t \*ctx)

*Initialize a SHA context for performing a hardware SHA-256 operation on a device. Note that only one SHA operation can be run at a time.*
- ATCA\_STATUS [atcab\\_hw\\_sha2\\_256\\_update](#) (atca\_sha256\_ctx\_t \*ctx, const uint8\_t \*data, size\_t data\_size)

*Add message data to a SHA context for performing a hardware SHA-256 operation on a device.*
- ATCA\_STATUS [atcab\\_hw\\_sha2\\_256\\_finish](#) (atca\_sha256\_ctx\_t \*ctx, uint8\_t \*digest)

*Finish SHA-256 digest for a SHA context for performing a hardware SHA-256 operation on a device.*
- ATCA\_STATUS [atcab\\_sha\\_hmac\\_init](#) (atca\_hmac\_sha256\_ctx\_t \*ctx, uint16\_t key\_slot)

*Executes SHA command to start an HMAC/SHA-256 operation.*
- ATCA\_STATUS [atcab\\_sha\\_hmac\\_update](#) (atca\_hmac\_sha256\_ctx\_t \*ctx, const uint8\_t \*data, size\_t data\_size)

*Executes SHA command to add an arbitrary amount of message data to a HMAC/SHA-256 operation.*
- ATCA\_STATUS [atcab\\_sha\\_hmac\\_finish](#) (atca\_hmac\_sha256\_ctx\_t \*ctx, uint8\_t \*digest, uint8\_t target)

*Executes SHA command to complete a HMAC/SHA-256 operation.*
- ATCA\_STATUS [atcab\\_sha\\_hmac\\_ext](#) (ATCADevice device, const uint8\_t \*data, size\_t data\_size, uint16\_t key\_slot, uint8\_t \*digest, uint8\_t target)

*Use the SHA command to compute an HMAC/SHA-256 operation.*
- ATCA\_STATUS [atcab\\_sha\\_hmac](#) (const uint8\_t \*data, size\_t data\_size, uint16\_t key\_slot, uint8\_t \*digest, uint8\_t target)

*Use the SHA command to compute an HMAC/SHA-256 operation.*
- ATCA\_STATUS [atcab\\_sign\\_base](#) (uint8\_t mode, uint16\_t key\_id, uint8\_t \*signature)

*Executes the Sign command, which generates a signature using the ECDSA algorithm.*
- ATCA\_STATUS [atcab\\_sign\\_ext](#) (ATCADevice device, uint16\_t key\_id, const uint8\_t \*msg, uint8\_t \*signature)

*Executes Sign command, to sign a 32-byte external message using the private key in the specified slot. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
- ATCA\_STATUS [atcab\\_sign](#) (uint16\_t key\_id, const uint8\_t \*msg, uint8\_t \*signature)

*Executes Sign command, to sign a 32-byte external message using the private key in the specified slot. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
- ATCA\_STATUS [atcab\\_sign\\_internal](#) (uint16\_t key\_id, bool is\_invalidate, bool is\_full\_sn, uint8\_t \*signature)

*Executes Sign command to sign an internally generated message.*
- ATCA\_STATUS [atcab\\_updateextra](#) (uint8\_t mode, uint16\_t new\_value)

*Executes UpdateExtra command to update the values of the two extra bytes within the Configuration zone (bytes 84 and 85).*
- ATCA\_STATUS [atcab\\_verify](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*signature, const uint8\_t \*public\_key, const uint8\_t \*other\_data, uint8\_t \*mac)

*Executes the Verify command, which takes an ECDSA [R,S] signature and verifies that it is correctly generated from a given message and public key. In all cases, the signature is an input to the command.*
- ATCA\_STATUS [atcab\\_verify\\_extern\\_ext](#) (ATCADevice device, const uint8\_t \*message, const uint8\_t \*signature, const uint8\_t \*public\_key, bool \*is\_verified)

- Executes the Verify command, which verifies a signature (ECDSA verify operation) with all components (message, signature, and public key) supplied. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
- ATCA\_STATUS [atcab\\_verify\\_extern](#) (const uint8\_t \*message, const uint8\_t \*signature, const uint8\_t \*public\_key, bool \*is\_verified)  
*Executes the Verify command, which verifies a signature (ECDSA verify operation) with all components (message, signature, and public key) supplied. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
  - ATCA\_STATUS [atcab\\_verify\\_extern\\_mac](#) (const uint8\_t \*message, const uint8\_t \*signature, const uint8\_t \*public\_key, const uint8\_t \*num\_in, const uint8\_t \*io\_key, bool \*is\_verified)  
*Executes the Verify command with verification MAC, which verifies a signature (ECDSA verify operation) with all components (message, signature, and public key) supplied. This function is only available on the ATECC608.*
  - ATCA\_STATUS [atcab\\_verify\\_stored\\_ext](#) (ATCADevice device, const uint8\_t \*message, const uint8\_t \*signature, uint16\_t key\_id, bool \*is\_verified)  
*Executes the Verify command, which verifies a signature (ECDSA verify operation) with a public key stored in the device. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
  - ATCA\_STATUS [atcab\\_verify\\_stored](#) (const uint8\_t \*message, const uint8\_t \*signature, uint16\_t key\_id, bool \*is\_verified)  
*Executes the Verify command, which verifies a signature (ECDSA verify operation) with a public key stored in the device. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
  - ATCA\_STATUS [atcab\\_verify\\_stored\\_with\\_tempkey](#) (const uint8\_t \*signature, uint16\_t key\_id, bool \*is\_verified)  
*Executes the Verify command, which verifies a signature (ECDSA verify operation) with a public key stored in the device. keyConfig.reqrandom bit should be set and the message to be signed should be already loaded into TempKey for all devices.*
  - ATCA\_STATUS [atcab\\_verify\\_stored\\_mac](#) (const uint8\_t \*message, const uint8\_t \*signature, uint16\_t key\_id, const uint8\_t \*num\_in, const uint8\_t \*io\_key, bool \*is\_verified)  
*Executes the Verify command with verification MAC, which verifies a signature (ECDSA verify operation) with a public key stored in the device. This function is only available on the ATECC608.*
  - ATCA\_STATUS [atcab\\_verify\\_validate](#) (uint16\_t key\_id, const uint8\_t \*signature, const uint8\_t \*other\_data, bool \*is\_verified)  
*Executes the Verify command in Validate mode to validate a public key stored in a slot.*
  - ATCA\_STATUS [atcab\\_verify\\_invalidate](#) (uint16\_t key\_id, const uint8\_t \*signature, const uint8\_t \*other\_data, bool \*is\_verified)  
*Executes the Verify command in Invalidate mode which invalidates a previously validated public key stored in a slot.*
  - ATCA\_STATUS [atcab\\_write](#) (uint8\_t zone, uint16\_t address, const uint8\_t \*value, const uint8\_t \*mac)  
*Executes the Write command, which writes either one four byte word or a 32-byte block to one of the EEPROM zones on the device. Depending upon the value of the WriteConfig byte for this slot, the data may be required to be encrypted by the system prior to being sent to the device. This command cannot be used to write slots configured as ECC private keys.*
  - ATCA\_STATUS [atcab\\_write\\_zone\\_ext](#) (ATCADevice device, uint8\_t zone, uint16\_t slot, uint8\_t block, uint8\_t offset, const uint8\_t \*data, uint8\_t len)  
*Executes the Write command, which writes either 4 or 32 bytes of data into a device zone.*
  - ATCA\_STATUS [atcab\\_write\\_zone](#) (uint8\_t zone, uint16\_t slot, uint8\_t block, uint8\_t offset, const uint8\_t \*data, uint8\_t len)  
*Executes the Write command, which writes either 4 or 32 bytes of data into a device zone.*
  - ATCA\_STATUS [atcab\\_write\\_bytes\\_zone\\_ext](#) (ATCADevice device, uint8\_t zone, uint16\_t slot, size\_t offset\_bytes, const uint8\_t \*data, size\_t length)  
*Executes the Write command, which writes data into the configuration, otp, or data zones with a given byte offset and length. Offset and length must be multiples of a word (4 bytes).*
  - ATCA\_STATUS [atcab\\_write\\_bytes\\_zone](#) (uint8\_t zone, uint16\_t slot, size\_t offset\_bytes, const uint8\_t \*data, size\_t length)  
*Executes the Write command, which writes data into the configuration, otp, or data zones with a given byte offset and length. Offset and length must be multiples of a word (4 bytes).*
  - ATCA\_STATUS [atcab\\_write\\_pubkey\\_ext](#) (ATCADevice device, uint16\_t slot, const uint8\_t \*public\_key)  
*Uses the write command to write a public key to a slot in the proper format.*

- ATCA\_STATUS [atcab\\_write\\_pubkey](#) (uint16\_t slot, const uint8\_t \*public\_key)  
*Uses the write command to write a public key to a slot in the proper format.*
- ATCA\_STATUS [atcab\\_write\\_config\\_zone\\_ext](#) (ATCADevice device, const uint8\_t \*config\_data)  
*Executes the Write command, which writes the configuration zone.*
- ATCA\_STATUS [atcab\\_write\\_config\\_zone](#) (const uint8\_t \*config\_data)  
*Executes the Write command, which writes the configuration zone.*
- ATCA\_STATUS [atcab\\_write\\_enc](#) (uint16\_t key\_id, uint8\_t block, const uint8\_t \*data, const uint8\_t \*enc\_key, const uint16\_t enc\_key\_id, const uint8\_t num\_in[(20)])  
*Executes the Write command, which performs an encrypted write of a 32 byte block into given slot.*
- ATCA\_STATUS [atcab\\_write\\_config\\_counter](#) (uint16\_t counter\_id, uint32\_t counter\_value)  
*Initialize one of the monotonic counters in device with a specific value.*

## Variables

- [ATCADevice](#) [g\\_atcab\\_device\\_ptr](#) = NULL

### 22.36.1 Detailed Description

CryptoAuthLib Basic API methods. These methods provide a simpler way to access the core crypto methods.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.37 atca\_basic.h File Reference

CryptoAuthLib Basic API methods - a simple crypto authentication API. These methods manage a global ATCADevice object behind the scenes. They also manage the wake/idle state transitions so callers don't need to.

```
#include "cryptoauthlib.h"
#include "crypto/atca_crypto_sw_sha2.h"
#include "crypto/atca_crypto_hw_aes.h"
```

## Macros

- #define [atcab\\_get\\_addr](#)(...) [calib\\_get\\_addr](#)(\_\_VA\_ARGS\_\_)
- #define [atca\\_execute\\_command](#)(...) [calib\\_execute\\_command](#)(\_\_VA\_ARGS\_\_)
- #define [SHA\\_CONTEXT\\_MAX\\_SIZE](#) (109)

## Functions

- ATCA\_STATUS [atcab\\_version](#) (char \*ver\_str)  
*basic API methods are all prefixed with atcab\_ (CryptoAuthLib Basic) the fundamental premise of the basic API is it is based on a single interface instance and that instance is global, so all basic API commands assume that one global device is the one to operate on.*
- ATCA\_STATUS [atcab\\_init\\_ext](#) (ATCADevice \*device, ATCAIfaceCfg \*cfg)  
*Creates and initializes a ATCADevice context.*
- ATCA\_STATUS [atcab\\_init](#) (ATCAIfaceCfg \*cfg)  
*Creates a global ATCADevice object used by Basic API.*
- ATCA\_STATUS [atcab\\_init\\_device](#) (ATCADevice ca\_device)  
*Initialize the global ATCADevice object to point to one of your choosing for use with all the atcab\_ basic API.*
- ATCA\_STATUS [atcab\\_release\\_ext](#) (ATCADevice \*device)  
*release (free) the an ATCADevice instance.*
- ATCA\_STATUS [atcab\\_release](#) (void)  
*release (free) the global ATCADevice instance. This must be called in order to release or free up the interface.*
- ATCADevice [atcab\\_get\\_device](#) (void)  
*Get the global device object.*
- ATCADeviceType [atcab\\_get\\_device\\_type\\_ext](#) (ATCADevice device)  
*Get the selected device type of rthe device context.*
- ATCADeviceType [atcab\\_get\\_device\\_type](#) (void)  
*Get the current device type configured for the global ATCADevice.*
- uint8\_t [atcab\\_get\\_device\\_address](#) (ATCADevice device)  
*Get the current device address based on the configured device and interface.*
- bool [atcab\\_is\\_ca\\_device](#) (ATCADeviceType dev\_type)  
*Check whether the device is cryptoauth device.*
- bool [atcab\\_is\\_ca2\\_device](#) (ATCADeviceType dev\_type)  
*Check whether the device is cryptoauth device.*
- bool [atcab\\_is\\_ta\\_device](#) (ATCADeviceType dev\_type)  
*Check whether the device is Trust Anchor device.*
- ATCA\_STATUS [atcab\\_pbkdf2\\_sha256\\_ext](#) (ATCADevice device, const uint32\_t iter, const uint16\_t slot, const uint8\_t \*salt, const size\_t salt\_len, uint8\_t \*result, size\_t result\_len)
- ATCA\_STATUS [atcab\\_pbkdf2\\_sha256](#) (const uint32\_t iter, const uint16\_t slot, const uint8\_t \*salt, const size\_t salt\_len, uint8\_t \*result, size\_t result\_len)
- ATCA\_STATUS [atcab\\_wakeup](#) (void)  
*wakeup the CryptoAuth device*
- ATCA\_STATUS [atcab\\_idle](#) (void)  
*idle the CryptoAuth device*
- ATCA\_STATUS [atcab\\_sleep](#) (void)  
*invoke sleep on the CryptoAuth device*
- ATCA\_STATUS [atcab\\_get\\_zone\\_size](#) (uint8\_t zone, uint16\_t slot, size\_t \*size)  
*Gets the size of the specified zone in bytes.*
- ATCA\_STATUS [atcab\\_get\\_zone\\_size\\_ext](#) (ATCADevice device, uint8\_t zone, uint16\_t slot, size\_t \*size)  
*Gets the size of the specified zone in bytes.*
- ATCA\_STATUS [atcab\\_aes](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*aes\_in, uint8\_t \*aes\_out)  
*Compute the AES-128 encrypt, decrypt, or GFM calculation.*
- ATCA\_STATUS [atcab\\_aes\\_encrypt](#) (uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*plaintext, uint8\_t \*ciphertext)  
*Perform an AES-128 encrypt operation with a key in the device.*
- ATCA\_STATUS [atcab\\_aes\\_encrypt\\_ext](#) (ATCADevice device, uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*plaintext, uint8\_t \*ciphertext)  
*Perform an AES-128 encrypt operation with a key in the device.*



- ATCA\_STATUS [atcab\\_aes\\_decrypt](#) (uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*ciphertext, uint8\_t \*plaintext)  
*Perform an AES-128 decrypt operation with a key in the device.*
- ATCA\_STATUS [atcab\\_aes\\_decrypt\\_ext](#) (ATCADevice device, uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*ciphertext, uint8\_t \*plaintext)  
*Perform an AES-128 decrypt operation with a key in the device.*
- ATCA\_STATUS [atcab\\_aes\\_gfm](#) (const uint8\_t \*h, const uint8\_t \*input, uint8\_t \*output)  
*Perform a Galois Field Multiply (GFM) operation.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_init](#) (atca\_aes\_gcm\_ctx\_t \*ctx, uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*iv, size\_t iv\_size)  
*Initialize context for AES GCM operation with an existing IV, which is common when starting a decrypt operation.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_init\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, uint16\_t key\_id, uint8\_t key\_block, const uint8\_t \*iv, size\_t iv\_size)  
*Initialize context for AES GCM operation with an existing IV, which is common when starting a decrypt operation.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_init\\_rand](#) (atca\_aes\_gcm\_ctx\_t \*ctx, uint16\_t key\_id, uint8\_t key\_block, size\_t rand\_size, const uint8\_t \*free\_field, size\_t free\_field\_size, uint8\_t \*iv)  
*Initialize context for AES GCM operation with a IV composed of a random and optional fixed(free) field, which is common when starting an encrypt operation.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_aad\\_update](#) (atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*aad, uint32\_t aad\_size)  
*Process Additional Authenticated Data (AAD) using GCM mode and a key within the ATECC608 device.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_aad\\_update\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*aad, uint32\_t aad\_size)  
*Process Additional Authenticated Data (AAD) using GCM mode and a key within the ATECC608 device.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_encrypt\\_update](#) (atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*plaintext, uint32\_t plaintext\_size, uint8\_t \*ciphertext)  
*Encrypt data using GCM mode and a key within the ATECC608 device. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_encrypt\\_update\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*plaintext, uint32\_t plaintext\_size, uint8\_t \*ciphertext)  
*Encrypt data using GCM mode and a key within the ATECC608 device. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_encrypt\\_finish](#) (atca\_aes\_gcm\_ctx\_t \*ctx, uint8\_t \*tag, size\_t tag\_size)  
*Complete a GCM encrypt operation returning the authentication tag.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_encrypt\\_finish\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, uint8\_t \*tag, size\_t tag\_size)  
*Complete a GCM encrypt operation returning the authentication tag.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_decrypt\\_update](#) (atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*ciphertext, uint32\_t ciphertext\_size, uint8\_t \*plaintext)  
*Decrypt data using GCM mode and a key within the ATECC608 device. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_decrypt\\_update\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*ciphertext, uint32\_t ciphertext\_size, uint8\_t \*plaintext)  
*Decrypt data using GCM mode and a key within the ATECC608 device. [atcab\\_aes\\_gcm\\_init\(\)](#) or [atcab\\_aes\\_gcm\\_init\\_rand\(\)](#) should be called before the first use of this function.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_decrypt\\_finish](#) (atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*tag, size\_t tag\_size, bool \*is\_verified)  
*Complete a GCM decrypt operation verifying the authentication tag.*
- ATCA\_STATUS [atcab\\_aes\\_gcm\\_decrypt\\_finish\\_ext](#) (ATCADevice device, atca\_aes\_gcm\_ctx\_t \*ctx, const uint8\_t \*tag, size\_t tag\_size, bool \*is\_verified)  
*Complete a GCM decrypt operation verifying the authentication tag.*
- ATCA\_STATUS [atcab\\_checkmac](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*challenge, const uint8\_t \*response, const uint8\_t \*other\_data)  
*Compares a MAC response with input values.*

- ATCA\_STATUS [atcab\\_checkmac\\_with\\_response\\_mac](#) (uint8\_t mode, const uint8\_t \*challenge, const uint8\_t \*response, const uint8\_t \*other\_data, uint8\_t \*mac)  
*Compares a MAC response with input values. SHA105 device can generate optional mac Output response mac mode only supports in SHA105 device.*
- ATCA\_STATUS [atcab\\_counter](#) (uint8\_t mode, uint16\_t counter\_id, uint32\_t \*counter\_value)  
*Compute the Counter functions.*
- ATCA\_STATUS [atcab\\_counter\\_increment](#) (uint16\_t counter\_id, uint32\_t \*counter\_value)  
*Increments one of the device's monotonic counters.*
- ATCA\_STATUS [atcab\\_counter\\_read](#) (uint16\_t counter\_id, uint32\_t \*counter\_value)  
*Read one of the device's monotonic counters.*
- ATCA\_STATUS [atcab\\_derivekey](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*mac)  
*Executes the DeviveKey command for deriving a new key from a nonce (TempKey) and an existing key.*
- ATCA\_STATUS [atcab\\_derivekey\\_ext](#) (ATCADevice device, uint8\_t mode, uint16\_t key\_id, const uint8\_t \*mac)  
*Executes the DeviveKey command for deriving a new key from a nonce (TempKey) and an existing key.*
- ATCA\_STATUS [atcab\\_ecdh\\_base](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*public\_key, uint8\_t \*pms, uint8\_t \*out\_nonce)  
*Base function for generating premaster secret key using ECDH.*
- ATCA\_STATUS [atcab\\_ecdh](#) (uint16\_t key\_id, const uint8\_t \*public\_key, uint8\_t \*pms)  
*ECDH command with a private key in a slot and the premaster secret is returned in the clear.*
- ATCA\_STATUS [atcab\\_ecdh\\_enc](#) (uint16\_t key\_id, const uint8\_t \*public\_key, uint8\_t \*pms, const uint8\_t \*read\_key, uint16\_t read\_key\_id, const uint8\_t num\_in[(20)])  
*ECDH command with a private key in a slot and the premaster secret is read from the next slot.*
- ATCA\_STATUS [atcab\\_ecdh\\_ioenc](#) (uint16\_t key\_id, const uint8\_t \*public\_key, uint8\_t \*pms, const uint8\_t \*io\_key)  
*ECDH command with a private key in a slot and the premaster secret is returned encrypted using the IO protection key.*
- ATCA\_STATUS [atcab\\_ecdh\\_tempkey](#) (const uint8\_t \*public\_key, uint8\_t \*pms)  
*ECDH command with a private key in TempKey and the premaster secret is returned in the clear.*
- ATCA\_STATUS [atcab\\_ecdh\\_tempkey\\_ioenc](#) (const uint8\_t \*public\_key, uint8\_t \*pms, const uint8\_t \*io\_key)  
*ECDH command with a private key in TempKey and the premaster secret is returned encrypted using the IO protection key.*
- ATCA\_STATUS [atcab\\_gendig](#) (uint8\_t zone, uint16\_t key\_id, const uint8\_t \*other\_data, uint8\_t other\_data\_size)  
*Issues a GenDig command, which performs a SHA256 hash on the source data indicated by zone with the contents of TempKey. See the CryptoAuth datasheet for your chip to see what the values of zone correspond to.*
- ATCA\_STATUS [atcab\\_gendivkey](#) (const uint8\_t \*other\_data)  
*Issues a GenDivKey command to generate the equivalent diversified key as that programmed into the client side device.*
- ATCA\_STATUS [atcab\\_genkey\\_base](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*other\_data, uint8\_t \*public\_key)  
*Issues GenKey command, which can generate a private key, compute a public key, nd/or compute a digest of a public key.*
- ATCA\_STATUS [atcab\\_genkey](#) (uint16\_t key\_id, uint8\_t \*public\_key)  
*Issues GenKey command, which generates a new random private key in slot/handle and returns the public key.*
- ATCA\_STATUS [atcab\\_genkey\\_ext](#) (ATCADevice device, uint16\_t key\_id, uint8\_t \*public\_key)  
*Issues GenKey command, which generates a new random private key in slot/handle and returns the public key.*
- ATCA\_STATUS [atcab\\_get\\_pubkey](#) (uint16\_t key\_id, uint8\_t \*public\_key)  
*Uses GenKey command to calculate the public key from an existing private key in a slot.*
- ATCA\_STATUS [atcab\\_get\\_pubkey\\_ext](#) (ATCADevice device, uint16\_t key\_id, uint8\_t \*public\_key)  
*Uses GenKey command to calculate the public key from an existing private key in a slot.*
- ATCA\_STATUS [atcab\\_hmac](#) (uint8\_t mode, uint16\_t key\_id, uint8\_t \*digest)  
*Issues a HMAC command, which computes an HMAC/SHA-256 digest of a key stored in the device, a challenge, and other information on the device.*



- ATCA\_STATUS [atcab\\_info\\_base](#) (uint8\_t mode, uint16\_t param2, uint8\_t \*out\_data)  
*Issues an Info command, which return internal device information and can control GPIO and the persistent latch.*
- ATCA\_STATUS [atcab\\_info](#) (uint8\_t \*revision)  
*Use the Info command to get the device revision (DevRev).*
- ATCA\_STATUS [atcab\\_info\\_ext](#) (ATCADevice device, uint8\_t \*revision)  
*Use the Info command to get the device revision (DevRev).*
- ATCA\_STATUS [atcab\\_info\\_lock\\_status](#) (uint16\_t param2, uint8\_t \*is\_locked)  
*Use the Info command to get the lock status.*
- ATCA\_STATUS [atcab\\_info\\_chip\\_status](#) (uint8\_t \*chip\_status)  
*Use the Info command to get the chip status.*
- ATCA\_STATUS [atcab\\_info\\_set\\_latch](#) (bool state)  
*Use the Info command to set the persistent latch state for an ATECC608 device.*
- ATCA\_STATUS [atcab\\_info\\_get\\_latch](#) (bool \*state)  
*Use the Info command to get the persistent latch current state for an ATECC608 device.*
- ATCA\_STATUS [atcab\\_kdf](#) (uint8\_t mode, uint16\_t key\_id, const uint32\_t details, const uint8\_t \*message, uint8\_t \*out\_data, uint8\_t \*out\_nonce)  
*Executes the KDF command, which derives a new key in PRF, AES, or HKDF modes.*
- ATCA\_STATUS [atcab\\_lock](#) (uint8\_t mode, uint16\_t summary\_crc)  
*The Lock command prevents future modifications of the Configuration and/or Data and OTP zones. If the device is so configured, then this command can be used to lock individual data slots. This command fails if the designated area is already locked.*
- ATCA\_STATUS [atcab\\_lock\\_config\\_zone](#) (void)  
*Unconditionally (no CRC required) lock the config zone.*
- ATCA\_STATUS [atcab\\_lock\\_config\\_zone\\_ext](#) (ATCADevice device)  
*Unconditionally (no CRC required) lock the config zone.*
- ATCA\_STATUS [atcab\\_lock\\_config\\_zone\\_crc](#) (uint16\_t summary\_crc)  
*Lock the config zone with summary CRC.*
- ATCA\_STATUS [atcab\\_lock\\_data\\_zone](#) (void)  
*Unconditionally (no CRC required) lock the data zone (slots and OTP). for CryptoAuth devices and lock the setup for Trust Anchor device.*
- ATCA\_STATUS [atcab\\_lock\\_data\\_zone\\_ext](#) (ATCADevice device)  
*Unconditionally (no CRC required) lock the data zone (slots and OTP). for CryptoAuth devices and lock the setup for Trust Anchor device.*
- ATCA\_STATUS [atcab\\_lock\\_data\\_zone\\_crc](#) (uint16\_t summary\_crc)  
*Lock the data zone (slots and OTP) with summary CRC.*
- ATCA\_STATUS [atcab\\_lock\\_data\\_slot](#) (uint16\_t slot)  
*Lock an individual slot in the data zone on an ATECC device. Not available for ATSHA devices. Slot must be configured to be slot lockable (KeyConfig.Lockable=1) (for cryptoauth devices) or Lock an individual handle in shared data element on an Trust Anchor device (for Trust Anchor devices).*
- ATCA\_STATUS [atcab\\_lock\\_data\\_slot\\_ext](#) (ATCADevice device, uint16\_t slot)  
*Lock an individual slot in the data zone on an ATECC device. Not available for ATSHA devices. Slot must be configured to be slot lockable (KeyConfig.Lockable=1) (for cryptoauth devices) or Lock an individual handle in shared data element on an Trust Anchor device (for Trust Anchor devices).*
- ATCA\_STATUS [atcab\\_mac](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*challenge, uint8\_t \*digest)  
*Executes MAC command, which computes a SHA-256 digest of a key stored in the device, a challenge, and other information on the device.*
- ATCA\_STATUS [atcab\\_nonce\\_base](#) (uint8\_t mode, uint16\_t zero, const uint8\_t \*num\_in, uint8\_t \*rand\_out)  
*Executes Nonce command, which loads a random or fixed nonce/data into the device for use by subsequent commands.*
- ATCA\_STATUS [atcab\\_nonce](#) (const uint8\_t \*num\_in)  
*Execute a Nonce command in pass-through mode to initialize TempKey to a specified value.*
- ATCA\_STATUS [atcab\\_nonce\\_load](#) (uint8\_t target, const uint8\_t \*num\_in, uint16\_t num\_in\_size)  
*Execute a Nonce command in pass-through mode to load one of the device's internal buffers with a fixed value.*

- ATCA\_STATUS [atcab\\_nonce\\_rand](#) (const uint8\_t \*num\_in, uint8\_t \*rand\_out)  
*Execute a Nonce command to generate a random nonce combining a host nonce (num\_in) and a device random number.*
- ATCA\_STATUS [atcab\\_nonce\\_rand\\_ext](#) (ATCADevice device, const uint8\_t \*num\_in, uint8\_t \*rand\_out)  
*Execute a Nonce command to generate a random nonce combining a host nonce (num\_in) and a device random number.*
- ATCA\_STATUS [atcab\\_challenge](#) (const uint8\_t \*num\_in)  
*Execute a Nonce command in pass-through mode to initialize TempKey to a specified value.*
- ATCA\_STATUS [atcab\\_challenge\\_seed\\_update](#) (const uint8\_t \*num\_in, uint8\_t \*rand\_out)  
*Execute a Nonce command to generate a random challenge combining a host nonce (num\_in) and a device random number.*
- ATCA\_STATUS [atcab\\_priv\\_write](#) (uint16\_t key\_id, const uint8\_t priv\_key[36], uint16\_t write\_key\_id, const uint8\_t write\_key[32], const uint8\_t num\_in[(20)])  
*Executes PrivWrite command, to write externally generated ECC private keys into the device.*
- ATCA\_STATUS [atcab\\_random](#) (uint8\_t \*rand\_out)  
*Executes Random command, which generates a 32 byte random number from the device.*
- ATCA\_STATUS [atcab\\_random\\_ext](#) (ATCADevice device, uint8\_t \*rand\_out)  
*Executes Random command, which generates a 32 byte random number from the device.*
- ATCA\_STATUS [atcab\\_read\\_zone](#) (uint8\_t zone, uint16\_t slot, uint8\_t block, uint8\_t offset, uint8\_t \*data, uint8\_t len)  
*Executes Read command, which reads either 4 or 32 bytes of data from a given slot, configuration zone, or the OTP zone.*
- ATCA\_STATUS [atcab\\_read\\_zone\\_ext](#) (ATCADevice device, uint8\_t zone, uint16\_t slot, uint8\_t block, uint8\_t offset, uint8\_t \*data, uint8\_t len)  
*Executes Read command, which reads either 4 or 32 bytes of data from a given slot, configuration zone, or the OTP zone.*
- ATCA\_STATUS [atcab\\_is\\_locked](#) (uint8\_t zone, bool \*is\_locked)  
*Executes Read command, which reads the configuration zone to see if the specified zone is locked.*
- ATCA\_STATUS [atcab\\_is\\_config\\_locked](#) (bool \*is\_locked)  
*This function check whether configuration zone is locked or not.*
- ATCA\_STATUS [atcab\\_is\\_config\\_locked\\_ext](#) (ATCADevice device, bool \*is\_locked)  
*This function check whether configuration zone is locked or not.*
- ATCA\_STATUS [atcab\\_is\\_data\\_locked](#) (bool \*is\_locked)  
*This function check whether data/setup zone is locked or not.*
- ATCA\_STATUS [atcab\\_is\\_data\\_locked\\_ext](#) (ATCADevice device, bool \*is\_locked)  
*This function check whether data/setup zone is locked or not.*
- ATCA\_STATUS [atcab\\_is\\_slot\\_locked](#) (uint16\_t slot, bool \*is\_locked)  
*This function check whether slot/handle is locked or not.*
- ATCA\_STATUS [atcab\\_is\\_slot\\_locked\\_ext](#) (ATCADevice device, uint16\_t slot, bool \*is\_locked)  
*This function check whether slot/handle is locked or not.*
- ATCA\_STATUS [atcab\\_is\\_private\\_ext](#) (ATCADevice device, uint16\_t slot, bool \*is\_private)  
*Check to see if the key is a private key or not.*
- ATCA\_STATUS [atcab\\_is\\_private](#) (uint16\_t slot, bool \*is\_private)
- ATCA\_STATUS [atcab\\_read\\_bytes\\_zone\\_ext](#) (ATCADevice device, uint8\_t zone, uint16\_t slot, size\_t offset, uint8\_t \*data, size\_t length)
- ATCA\_STATUS [atcab\\_read\\_bytes\\_zone](#) (uint8\_t zone, uint16\_t slot, size\_t offset, uint8\_t \*data, size\_t length)  
*Used to read an arbitrary number of bytes from any zone configured for clear reads.*
- ATCA\_STATUS [atcab\\_read\\_serial\\_number](#) (uint8\_t \*serial\_number)  
*This function returns serial number of the device.*
- ATCA\_STATUS [atcab\\_read\\_serial\\_number\\_ext](#) (ATCADevice device, uint8\_t \*serial\_number)  
*This function returns serial number of the device.*
- ATCA\_STATUS [atcab\\_read\\_pubkey](#) (uint16\_t slot, uint8\_t \*public\_key)

- Executes Read command to read an ECC P256 public key from a slot configured for clear reads.*

  - ATCA\_STATUS [atcab\\_read\\_pubkey\\_ext](#) (ATCADevice device, uint16\_t slot, uint8\_t \*public\_key)
- Executes Read command to read an ECC P256 public key from a slot configured for clear reads.*

  - ATCA\_STATUS [atcab\\_read\\_sig](#) (uint16\_t slot, uint8\_t \*sig)
- Executes Read command to read a 64 byte ECDSA P256 signature from a slot configured for clear reads.*

  - ATCA\_STATUS [atcab\\_read\\_config\\_zone](#) (uint8\_t \*config\_data)
- Executes Read command to read the complete device configuration zone.*

  - ATCA\_STATUS [atcab\\_read\\_config\\_zone\\_ext](#) (ATCADevice device, uint8\_t \*config\_data)
- Executes Read command to read the complete device configuration zone.*

  - ATCA\_STATUS [atcab\\_cmp\\_config\\_zone](#) (uint8\_t \*config\_data, bool \*same\_config)
- Compares a specified configuration zone with the configuration zone currently on the device.*

  - ATCA\_STATUS [atcab\\_read\\_enc](#) (uint16\_t key\_id, uint8\_t block, uint8\_t \*data, const uint8\_t \*enc\_key, const uint16\_t enc\_key\_id, const uint8\_t num\_in[(20)])
- Executes Read command on a slot configured for encrypted reads and decrypts the data to return it as plaintext.*

  - ATCA\_STATUS [atcab\\_secureboot](#) (uint8\_t mode, uint16\_t param2, const uint8\_t \*digest, const uint8\_t \*signature, uint8\_t \*mac)
- Executes Secure Boot command, which provides support for secure boot of an external MCU or MPU.*

  - ATCA\_STATUS [atcab\\_secureboot\\_mac](#) (uint8\_t mode, const uint8\_t \*digest, const uint8\_t \*signature, const uint8\_t \*num\_in, const uint8\_t \*io\_key, bool \*is\_verified)
- Executes Secure Boot command with encrypted digest and validated MAC response using the IO protection key.*

  - ATCA\_STATUS [atcab\\_selftest](#) (uint8\_t mode, uint16\_t param2, uint8\_t \*result)
- Executes the SelfTest command, which performs a test of one or more of the cryptographic engines within the ATECC608 chip.*

  - ATCA\_STATUS [atcab\\_sha\\_base](#) (uint8\_t mode, uint16\_t length, const uint8\_t \*data\_in, uint8\_t \*data\_out, uint16\_t \*data\_out\_size)
- Executes SHA command, which computes a SHA-256 or HMAC/SHA-256 digest for general purpose use by the host system.*

  - ATCA\_STATUS [atcab\\_sha\\_start](#) (void)
- Executes SHA command to initialize SHA-256 calculation engine.*

  - ATCA\_STATUS [atcab\\_sha\\_update](#) (const uint8\_t \*message)
- Executes SHA command to add 64 bytes of message data to the current context.*

  - ATCA\_STATUS [atcab\\_sha\\_end](#) (uint8\_t \*digest, uint16\_t length, const uint8\_t \*message)
- Executes SHA command to complete SHA-256 or HMAC/SHA-256 operation.*

  - ATCA\_STATUS [atcab\\_sha\\_read\\_context](#) (uint8\_t \*context, uint16\_t \*context\_size)
- Executes SHA command to read the SHA-256 context back. Only for ATECC608 with SHA-256 contexts. HMAC not supported.*

  - ATCA\_STATUS [atcab\\_sha\\_write\\_context](#) (const uint8\_t \*context, uint16\_t context\_size)
- Executes SHA command to write (restore) a SHA-256 context into the the device. Only supported for ATECC608 with SHA-256 contexts.*

  - ATCA\_STATUS [atcab\\_sha](#) (uint16\_t length, const uint8\_t \*message, uint8\_t \*digest)
- Use the SHA command to compute a SHA-256 digest.*

  - ATCA\_STATUS [atcab\\_hw\\_sha2\\_256](#) (const uint8\_t \*data, size\_t data\_size, uint8\_t \*digest)
- Use the SHA command to compute a SHA-256 digest.*

  - ATCA\_STATUS [atcab\\_hw\\_sha2\\_256\\_init](#) (atca\_sha256\_ctx\_t \*ctx)
- Initialize a SHA context for performing a hardware SHA-256 operation on a device. Note that only one SHA operation can be run at a time.*

  - ATCA\_STATUS [atcab\\_hw\\_sha2\\_256\\_update](#) (atca\_sha256\_ctx\_t \*ctx, const uint8\_t \*data, size\_t data\_size)
- Add message data to a SHA context for performing a hardware SHA-256 operation on a device.*

  - ATCA\_STATUS [atcab\\_hw\\_sha2\\_256\\_finish](#) (atca\_sha256\_ctx\_t \*ctx, uint8\_t \*digest)
- Finish SHA-256 digest for a SHA context for performing a hardware SHA-256 operation on a device.*

  - ATCA\_STATUS [atcab\\_sha\\_hmac\\_init](#) (atca\_hmac\_sha256\_ctx\_t \*ctx, uint16\_t key\_slot)
- Executes SHA command to start an HMAC/SHA-256 operation.*

- ATCA\_STATUS [atcab\\_sha\\_hmac\\_update](#) ([atca\\_hmac\\_sha256\\_ctx\\_t](#) \*ctx, const uint8\_t \*data, size\_t data\_size)
 

*Executes SHA command to add an arbitrary amount of message data to a HMAC/SHA-256 operation.*
- ATCA\_STATUS [atcab\\_sha\\_hmac\\_finish](#) ([atca\\_hmac\\_sha256\\_ctx\\_t](#) \*ctx, uint8\_t \*digest, uint8\_t target)
 

*Executes SHA command to complete a HMAC/SHA-256 operation.*
- ATCA\_STATUS [atcab\\_sha\\_hmac](#) (const uint8\_t \*data, size\_t data\_size, uint16\_t key\_slot, uint8\_t \*digest, uint8\_t target)
 

*Use the SHA command to compute an HMAC/SHA-256 operation.*
- ATCA\_STATUS [atcab\\_sha\\_hmac\\_ext](#) ([ATCADevice](#) device, const uint8\_t \*data, size\_t data\_size, uint16\_t key\_slot, uint8\_t \*digest, uint8\_t target)
 

*Use the SHA command to compute an HMAC/SHA-256 operation.*
- ATCA\_STATUS [atcab\\_sign\\_base](#) (uint8\_t mode, uint16\_t key\_id, uint8\_t \*signature)
 

*Executes the Sign command, which generates a signature using the ECDSA algorithm.*
- ATCA\_STATUS [atcab\\_sign](#) (uint16\_t key\_id, const uint8\_t \*msg, uint8\_t \*signature)
 

*Executes Sign command, to sign a 32-byte external message using the private key in the specified slot. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
- ATCA\_STATUS [atcab\\_sign\\_ext](#) ([ATCADevice](#) device, uint16\_t key\_id, const uint8\_t \*msg, uint8\_t \*signature)
 

*Executes Sign command, to sign a 32-byte external message using the private key in the specified slot. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
- ATCA\_STATUS [atcab\\_sign\\_internal](#) (uint16\_t key\_id, bool is\_invalidate, bool is\_full\_sn, uint8\_t \*signature)
 

*Executes Sign command to sign an internally generated message.*
- ATCA\_STATUS [atcab\\_updateextra](#) (uint8\_t mode, uint16\_t new\_value)
 

*Executes UpdateExtra command to update the values of the two extra bytes within the Configuration zone (bytes 84 and 85).*
- ATCA\_STATUS [atcab\\_verify](#) (uint8\_t mode, uint16\_t key\_id, const uint8\_t \*signature, const uint8\_t \*public\_key, const uint8\_t \*other\_data, uint8\_t \*mac)
 

*Executes the Verify command, which takes an ECDSA [R,S] signature and verifies that it is correctly generated from a given message and public key. In all cases, the signature is an input to the command.*
- ATCA\_STATUS [atcab\\_verify\\_extern](#) (const uint8\_t \*message, const uint8\_t \*signature, const uint8\_t \*public\_key, bool \*is\_verified)
 

*Executes the Verify command, which verifies a signature (ECDSA verify operation) with all components (message, signature, and public key) supplied. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
- ATCA\_STATUS [atcab\\_verify\\_extern\\_ext](#) ([ATCADevice](#) device, const uint8\_t \*message, const uint8\_t \*signature, const uint8\_t \*public\_key, bool \*is\_verified)
 

*Executes the Verify command, which verifies a signature (ECDSA verify operation) with all components (message, signature, and public key) supplied. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
- ATCA\_STATUS [atcab\\_verify\\_extern\\_mac](#) (const uint8\_t \*message, const uint8\_t \*signature, const uint8\_t \*public\_key, const uint8\_t \*num\_in, const uint8\_t \*io\_key, bool \*is\_verified)
 

*Executes the Verify command with verification MAC, which verifies a signature (ECDSA verify operation) with all components (message, signature, and public key) supplied. This function is only available on the ATECC608.*
- ATCA\_STATUS [atcab\\_verify\\_stored](#) (const uint8\_t \*message, const uint8\_t \*signature, uint16\_t key\_id, bool \*is\_verified)
 

*Executes the Verify command, which verifies a signature (ECDSA verify operation) with a public key stored in the device. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
- ATCA\_STATUS [atcab\\_verify\\_stored\\_ext](#) ([ATCADevice](#) device, const uint8\_t \*message, const uint8\_t \*signature, uint16\_t key\_id, bool \*is\_verified)
 

*Executes the Verify command, which verifies a signature (ECDSA verify operation) with a public key stored in the device. The message to be signed will be loaded into the Message Digest Buffer to the ATECC608 device or TempKey for other devices.*
- ATCA\_STATUS [atcab\\_verify\\_stored\\_with\\_tempkey](#) (const uint8\_t \*signature, uint16\_t key\_id, bool \*is\_verified)

Executes the Verify command, which verifies a signature (ECDSA verify operation) with a public key stored in the device. `keyConfig.reqrandom` bit should be set and the message to be signed should be already loaded into TempKey for all devices.

- ATCA\_STATUS `atcab_verify_stored_mac` (const uint8\_t \*message, const uint8\_t \*signature, uint16\_t key\_id, const uint8\_t \*num\_in, const uint8\_t \*io\_key, bool \*is\_verified)

Executes the Verify command with verification MAC, which verifies a signature (ECDSA verify operation) with a public key stored in the device. This function is only available on the ATECC608.

- ATCA\_STATUS `atcab_verify_validate` (uint16\_t key\_id, const uint8\_t \*signature, const uint8\_t \*other\_data, bool \*is\_verified)

Executes the Verify command in Validate mode to validate a public key stored in a slot.

- ATCA\_STATUS `atcab_verify_invalidate` (uint16\_t key\_id, const uint8\_t \*signature, const uint8\_t \*other\_data, bool \*is\_verified)

Executes the Verify command in Invalidate mode which invalidates a previously validated public key stored in a slot.

- ATCA\_STATUS `atcab_write` (uint8\_t zone, uint16\_t address, const uint8\_t \*value, const uint8\_t \*mac)

Executes the Write command, which writes either one four byte word or a 32-byte block to one of the EEPROM zones on the device. Depending upon the value of the WriteConfig byte for this slot, the data may be required to be encrypted by the system prior to being sent to the device. This command cannot be used to write slots configured as ECC private keys.

- ATCA\_STATUS `atcab_write_zone` (uint8\_t zone, uint16\_t slot, uint8\_t block, uint8\_t offset, const uint8\_t \*data, uint8\_t len)

Executes the Write command, which writes either 4 or 32 bytes of data into a device zone.

- ATCA\_STATUS `atcab_write_zone_ext` (ATCADevice device, uint8\_t zone, uint16\_t slot, uint8\_t block, uint8\_t offset, const uint8\_t \*data, uint8\_t len)

Executes the Write command, which writes either 4 or 32 bytes of data into a device zone.

- ATCA\_STATUS `atcab_write_bytes_zone_ext` (ATCADevice device, uint8\_t zone, uint16\_t slot, size\_t offset\_bytes, const uint8\_t \*data, size\_t length)

- ATCA\_STATUS `atcab_write_bytes_zone` (uint8\_t zone, uint16\_t slot, size\_t offset\_bytes, const uint8\_t \*data, size\_t length)

Executes the Write command, which writes data into the configuration, otp, or data zones with a given byte offset and length. Offset and length must be multiples of a word (4 bytes).

- ATCA\_STATUS `atcab_write_pubkey` (uint16\_t slot, const uint8\_t \*public\_key)

Uses the write command to write a public key to a slot in the proper format.

- ATCA\_STATUS `atcab_write_pubkey_ext` (ATCADevice device, uint16\_t slot, const uint8\_t \*public\_key)

Uses the write command to write a public key to a slot in the proper format.

- ATCA\_STATUS `atcab_write_config_zone` (const uint8\_t \*config\_data)

Executes the Write command, which writes the configuration zone.

- ATCA\_STATUS `atcab_write_config_zone_ext` (ATCADevice device, const uint8\_t \*config\_data)

Executes the Write command, which writes the configuration zone.

- ATCA\_STATUS `atcab_write_enc` (uint16\_t key\_id, uint8\_t block, const uint8\_t \*data, const uint8\_t \*enc\_key, const uint16\_t enc\_key\_id, const uint8\_t num\_in[(20)])

Executes the Write command, which performs an encrypted write of a 32 byte block into given slot.

- ATCA\_STATUS `atcab_write_config_counter` (uint16\_t counter\_id, uint32\_t counter\_value)

Initialize one of the monotonic counters in device with a specific value.

## Variables

- ATCADevice `g_atcab_device_ptr`

### 22.37.1 Detailed Description

CryptoAuthLib Basic API methods - a simple crypto authentication API. These methods manage a global ATCADevice object behind the scenes. They also manage the wake/idle state transitions so callers don't need to.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.38 atca\_cfgs.c File Reference

a set of default configurations for various ATCA devices and interfaces

```
#include <stddef.h>
#include "cryptoauthlib.h"
#include "atca_cfgs.h"
#include "atca_iface.h"
#include "atca_device.h"
```

### 22.38.1 Detailed Description

a set of default configurations for various ATCA devices and interfaces

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.39 atca\_cfgs.h File Reference

a set of default configurations for various ATCA devices and interfaces

```
#include "atca_iface.h"
```

### 22.39.1 Detailed Description

a set of default configurations for various ATCA devices and interfaces

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.40 atca\_compiler.h File Reference

CryptoAuthLib is meant to be portable across architectures, even non-Microchip architectures and compiler environments. This file is for isolating compiler specific macros.

```
#include <stdbool.h>
```

### Macros

- `#define SHARED_LIB_EXPORT`
- `#define ATCA_DLL extern`
- `#define ATCA_PACKED`
- `#define UNUSED_VAR(x)`



## 22.40.1 Detailed Description

CryptoAuthLib is meant to be portable across architectures, even non-Microchip architectures and compiler environments. This file is for isolating compiler specific macros.

### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.40.2 Macro Definition Documentation

### 22.40.2.1 UNUSED\_VAR

```
#define UNUSED_VAR(  
    x )
```

Enables removal of compiler warning due to unused variables

## 22.41 atca\_config\_check.h File Reference

Consistency checks for configuration options.

```
#include "atca_config.h"
```

### Macros

- #define **FEATURE\_ENABLED** (1)
- #define **FEATURE\_DISABLED** (0)
- #define **DEFAULT\_ENABLED** FEATURE\_ENABLED
- #define **DEFAULT\_DISABLED** FEATURE\_DISABLED
- #define **ATCA\_SHA\_SUPPORT** 1
- #define **ATCA\_ECC\_SUPPORT** DEFAULT\_ENABLED
- #define **ATCA\_CA2\_SUPPORT** DEFAULT\_ENABLED
- #define **ATCA\_CA2\_CERT\_SUPPORT** DEFAULT\_ENABLED
- #define **ATCA\_CA\_SUPPORT** DEFAULT\_ENABLED
- #define **ATCA\_HOSTLIB\_EN** DEFAULT\_ENABLED
- #define **ATCA\_USE\_ATCAB\_FUNCTIONS**
- #define **ATCA\_CHECK\_PARAMS\_EN** DEFAULT\_ENABLED
- #define **ATCA\_CHECK\_INVALID\_MSG**(c, s, m) if (c) { return ATCA\_TRACE(s, m); }
- #define **ATCA\_CHECK\_VALID\_MSG**(c, m) if (!ATCA\_TRACE(!c), m))
- #define **ATCA\_CHECK\_INVALID**(c, s) **ATCA\_CHECK\_INVALID\_MSG**(c, s, "")
- #define **ATCA\_CHECK\_VALID**(c) **ATCA\_CHECK\_VALID\_MSG**(c, "")
- #define **MULTIPART\_BUF\_EN** (DEFAULT\_DISABLED)
- #define **ATCACERT\_EN** (DEFAULT\_ENABLED)
- #define **ATCA\_HEAP**
- #define **ATCA\_UNUSED\_VAR\_CHECK** (DEFAULT\_ENABLED)

- #define **ATCAB\_AES\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_AES\_GFM\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_AES\_GCM\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_CHECKMAC\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_COUNTER\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_DERIVEKEY\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_ECDH\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_ECDH\_ENC\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_GENDIG\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_GENKEY\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_GENKEY\_MAC\_EN** ATCAB\_GENKEY\_EN
- #define **ATCAB\_HMAC\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_INFO\_LATCH\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_KDF\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_LOCK\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_MAC\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_NONCE\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_PRIVWRITE\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_RANDOM\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_READ\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_READ\_ENC\_EN** ATCAB\_READ\_EN
- #define **ATCAB\_SECUREBOOT\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_SECUREBOOT\_MAC\_EN** ATCAB\_SECUREBOOT\_EN
- #define **ATCAB\_SELFTEST\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_SHA\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_SHA\_HMAC\_EN** ATCAB\_SHA\_EN
- #define **ATCAB\_SHA\_CONTEXT\_EN** ATCAB\_SHA\_EN
- #define **ATCAB\_SIGN\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_SIGN\_INTERNAL\_EN** ATCAB\_SIGN\_EN
- #define **ATCAB\_UPDATEEXTRA\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_VERIFY\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_VERIFY\_EXTERN\_EN** ATCAB\_VERIFY\_EN
- #define **ATCAB\_VERIFY\_MAC\_EN** ATCAB\_VERIFY\_EN
- #define **ATCAB\_VERIFY\_STORED\_EN** ATCAB\_VERIFY\_EN
- #define **ATCAB\_VERIFY\_VALIDATE\_EN** ATCAB\_VERIFY\_EN
- #define **ATCAB\_WRITE\_EN** (DEFAULT\_ENABLED)
- #define **ATCAB\_WRITE\_ENC\_EN** ATCAB\_WRITE\_EN
- #define **ATCAC\_SHA1\_EN** (DEFAULT\_ENABLED)
- #define **ATCAC\_SHA256\_EN** (DEFAULT\_ENABLED)
- #define **ATCAC\_SHA256\_HMAC\_EN** ATCAC\_SHA256\_EN
- #define **ATCAC\_SHA256\_HMAC\_CTR\_EN** ATCAC\_SHA256\_HMAC\_EN
- #define **ATCAC\_RANDOM\_EN** ATCA\_HOSTLIB\_EN
- #define **ATCAC\_VERIFY\_EN** ATCA\_HOSTLIB\_EN
- #define **ATCAC\_SIGN\_EN** ATCA\_HOSTLIB\_EN

### 22.41.1 Detailed Description

Consistency checks for configuration options.

#### Copyright

(c) 2015-2021 Microchip Technology Inc. and its subsidiaries.



## 22.41.2 Macro Definition Documentation

### 22.41.2.1 ATCA\_CHECK\_INVALID\_MSG

```
#define ATCA_CHECK_INVALID_MSG(  
    c,  
    s,  
    m ) if (c) { return ATCA_TRACE(s, m); }
```

Emits message and returns the status code when the condition is true

### 22.41.2.2 ATCA\_SHA\_SUPPORT

```
#define ATCA_SHA_SUPPORT 1
```

Library Configuration File - All build attributes should be included in atca\_config.h

### 22.41.2.3 ATCA\_UNUSED\_VAR\_CHECK

```
#define ATCA_UNUSED_VAR_CHECK (DEFAULT_ENABLED)
```

Enables removal of compiler warning due to unused variables

### 22.41.2.4 ATCA\_USE\_ATCAB\_FUNCTIONS

```
#define ATCA_USE_ATCAB_FUNCTIONS
```

Does the atcab\_ API layer need to be instantiated (adds a layer of abstraction)

### 22.41.2.5 ATCAB\_AES\_GFM\_EN

```
#define ATCAB_AES_GFM_EN (DEFAULT_ENABLED)
```

Enable ATCAB\_AES\_GFM\_EN to enabled Galois Field Multiply

Supported API's: atcab\_aes

### 22.41.2.6 ATCAB\_GENKEY\_MAC\_EN

```
#define ATCAB_GENKEY_MAC_EN ATCAB_GENKEY_EN
```

Requires: ATCAB\_GENKEY\_EN

Enable ATCAB\_GENKEY\_MAC\_EN which provides for a mac with the genkey command

Supported API's: atcab\_genkey\_base

### 22.41.2.7 ATCAB\_INFO\_LATCH\_EN

```
#define ATCAB_INFO_LATCH_EN (DEFAULT_ENABLED)
```

Enable ATCAB\_INFO\_LATCH\_EN which enables control of GPIOs and the persistent latch

Supported API's: atcab\_info\_base

### 22.41.2.8 ATCAB\_VERIFY\_MAC\_EN

```
#define ATCAB_VERIFY_MAC_EN ATCAB_VERIFY_EN
```

Requires: ATCAB\_VERIFY

Executes verification command with verification MAC for the External or Stored Verify modes

Supported API's: atcab\_verify\_extern\_mac, atcab\_verify\_stored\_mac

### 22.41.2.9 ATCAC\_RANDOM\_EN

```
#define ATCAC_RANDOM_EN ATCA_HOSTLIB_EN
```

Requires: ATCA\_HOSTLIB\_EN

Enable ATCAC\_RANDOM\_EN get random numbers from the host's implementation - generally assumed to come from the host's cryptographic library or peripheral driver

### 22.41.2.10 ATCAC\_SHA1\_EN

```
#define ATCAC_SHA1_EN (DEFAULT_ENABLED)
```

Enable ATCAC\_SHA1\_EN to enable sha1 host side api

Supported API's: atcab\_write

### 22.41.2.11 ATCAC\_SHA256\_EN

```
#define ATCAC_SHA256_EN (DEFAULT_ENABLED)
```

Enable ATCAC\_SHA256\_EN to enable sha256 host side api

Supported API's: atcab\_write

### 22.41.2.12 ATCAC\_SIGN\_EN

```
#define ATCAC_SIGN_EN ATCA_HOSTLIB_EN
```

Requires: ATCA\_HOSTLIB\_EN

Enable ATCAC\_SIGN\_EN to use the host's sign functions. Generally assumed to come from the host's cryptographic library or peripheral driver.

### 22.41.2.13 ATCAC\_VERIFY\_EN

```
#define ATCAC_VERIFY_EN ATCA_HOSTLIB_EN
```

Requires: ATCA\_HOSTLIB\_EN

Enable ATCAC\_VERIFY\_EN to use the host's verify functions. Generally assumed to come from the host's cryptographic library or peripheral driver.

### 22.41.2.14 ATCACERT\_EN

```
#define ATCACERT_EN (DEFAULT_ENABLED)
```

Enables the ATCACERT x509 handling module

### 22.41.2.15 MULTIPART\_BUF\_EN

```
#define MULTIPART_BUF_EN (DEFAULT_DISABLED)
```

Enables multipart buffer handling (generally for small memory model platforms)

## 22.42 atca\_debug.c File Reference

Debug/Trace for CryptoAuthLib calls.

```
#include "cryptoauthlib.h"
```

### Functions

- ATCA\_STATUS **atca\_trace** (ATCA\_STATUS status)

### 22.42.1 Detailed Description

Debug/Trace for CryptoAuthLib calls.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.43 atca\_device.c File Reference

Microchip CryptoAuth device object.

```
#include "cryptoauthlib.h"
```

### Functions

- [ATCADevice newATCADevice](#) ([ATCAIfaceCfg](#) \*cfg)  
*constructor for a Microchip CryptoAuth device*
- void [deleteATCADevice](#) ([ATCADevice](#) \*ca\_dev)  
*destructor for a device NULLs reference after object is freed*
- [ATCA\\_STATUS initATCADevice](#) ([ATCAIfaceCfg](#) \*cfg, [ATCADevice](#) ca\_dev)  
*Initializer for an Microchip CryptoAuth device.*
- [ATCAIface atGetIFace](#) ([ATCADevice](#) dev)  
*returns a reference to the ATCAIface interface object for the device*
- [ATCA\\_STATUS releaseATCADevice](#) ([ATCADevice](#) ca\_dev)  
*Release any resources associated with the device.*

### 22.43.1 Detailed Description

Microchip CryptoAuth device object.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.44 atca\_device.h File Reference

Microchip Crypto Auth device object.

```
#include "atca_iface.h"
```

### Data Structures

- struct [atca\\_device](#)  
*[atca\\_device](#) is the C object backing ATCADevice. See the [atca\\_device.h](#) file for details on the ATCADevice methods*

### Typedefs

- typedef void(\* [ctx\\_cb](#)) (void \*ctx)  
*Callback function to clean up the session context.*
- typedef struct [atca\\_device](#) \* [ATCADevice](#)

### Enumerations

- enum [ATCADeviceState](#) { [ATCA\\_DEVICE\\_STATE\\_UNKNOWN](#) = 0 , [ATCA\\_DEVICE\\_STATE\\_SLEEP](#) , [ATCA\\_DEVICE\\_STATE\\_IDLE](#) , [ATCA\\_DEVICE\\_STATE\\_ACTIVE](#) }  
*ATCADeviceState says about device state.*

## Functions

- ATCA\_STATUS `initATCADevice` (`ATCAIfaceCfg` \*cfg, `ATCADevice` ca\_dev)  
*Initializer for an Microchip CryptoAuth device.*
- `ATCADevice` `newATCADevice` (`ATCAIfaceCfg` \*cfg)  
*constructor for a Microchip CryptoAuth device*
- ATCA\_STATUS `releaseATCADevice` (`ATCADevice` ca\_dev)  
*Release any resources associated with the device.*
- void `deleteATCADevice` (`ATCADevice` \*ca\_dev)  
*destructor for a device NULLs reference after object is freed*
- `ATCAIface` `atGetIFace` (`ATCADevice` dev)  
*returns a reference to the ATCAIface interface object for the device*

### 22.44.1 Detailed Description

Microchip Crypto Auth device object.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.45 atca\_devtypes.h File Reference

Microchip Crypto Auth.

```
#include <stdint.h>
```

## Macros

- #define **ATSHA204A** (0U)  
*The supported Device type in Cryptoauthlib library.*
- #define **ATECC108A** (1U)
- #define **ATECC508A** (2U)
- #define **ATECC608A** (3U)
- #define **ATECC608B** (3U)
- #define **ATECC608** (3U)
- #define **ATSHA206A** (4U)
- #define **TA100** (0x10U)
- #define **TA101** (0x11U)
- #define **ECC204** (0x20U)
- #define **TA010** (0x21U)
- #define **ECC206** (0x22U)
- #define **RNG90** (0x23U)
- #define **SHA104** (0x24U)
- #define **SHA105** (0x25U)
- #define **SHA106** (0x26U)
- #define **ATCA\_DEV\_UNKNOWN** (0x7EU)
- #define **ATCA\_DEV\_INVALID** (0x7FU)

## Typedefs

- typedef uint8\_t **ATCADeviceType**

### 22.45.1 Detailed Description

Microchip Crypto Auth.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.46 atca\_helpers.c File Reference

Helpers to support the CryptoAuthLib Basic API methods.

```
#include <stdlib.h>
#include <stdio.h>
#include <ctype.h>
#include <string.h>
#include "cryptoauthlib.h"
#include "atca_helpers.h"
```

## Macros

- #define **B64\_IS\_EQUAL** (64u)
- #define **B64\_IS\_INVALID** (-1)

## Functions

- const uint8\_t \* **atcab\_b64rules\_default** (void)
- const uint8\_t \* **atcab\_b64rules\_mime** (void)
- const uint8\_t \* **atcab\_b64rules\_urlsafe** (void)
- ATCA\_STATUS **atcab\_bin2hex** (const uint8\_t \*bin, size\_t bin\_size, char \*hex, size\_t \*hex\_size)  
*Convert a binary buffer to a hex string for easy reading.*
- ATCA\_STATUS **atcab\_reversal** (const uint8\_t \*bin, size\_t bin\_size, uint8\_t \*dest, size\_t \*dest\_size)  
*To reverse the input data.*
- ATCA\_STATUS **atcab\_bin2hex\_** (const uint8\_t \*bin, size\_t bin\_size, char \*hex, size\_t \*hex\_size, bool is\_↵  
pretty, bool is\_space, bool is\_upper)  
*Function that converts a binary buffer to a hex string suitable for easy reading.*
- ATCA\_STATUS **atcab\_hex2bin\_** (const char \*hex, size\_t hex\_size, uint8\_t \*bin, size\_t \*bin\_size, bool is\_↵  
\_space)
- ATCA\_STATUS **atcab\_hex2bin** (const char \*ascii\_hex, size\_t ascii\_hex\_len, uint8\_t \*binary, size\_t \*bin\_len)  
*Function that converts a hex string to binary buffer.*
- bool **isDigit** (char c)  
*Checks to see if a character is an ASCII representation of a digit ((c ge '0') and (c le '9'))*
- bool **isBlankSpace** (char c)  
*Checks to see if a character is blank space.*

- bool **isAlpha** (char c)  
*Checks to see if a character is an ASCII representation of hex ((c >= 'A') and (c <= 'F')) || ((c >= 'a') and (c <= 'f'))*
- bool **isHexAlpha** (char c)  
*Checks to see if a character is an ASCII representation of hex ((c >= 'A') and (c <= 'F')) || ((c >= 'a') and (c <= 'f'))*
- bool **isHex** (char c)  
*Returns true if this character is a valid hex character or if this is blankspace (The character can be included in a valid hexstring).*
- bool **isHexDigit** (char c)  
*Returns true if this character is a valid hex character.*
- ATCA\_STATUS **packHex** (const char \*ascii\_hex, size\_t ascii\_hex\_len, char \*packed\_hex, size\_t \*packed\_hex\_len)  
*Remove spaces from a ASCII hex string.*
- bool **isBase64** (char c, const uint8\_t \*rules)  
*Returns true if this character is a valid base 64 character or if this is space (A character can be included in a valid base 64 string).*
- bool **isBase64Digit** (char c, const uint8\_t \*rules)  
*Returns true if this character is a valid base 64 character.*
- ATCA\_STATUS **atcab\_base64decode** (const char \*encoded, size\_t encoded\_size, uint8\_t \*data, size\_t \*data\_size, const uint8\_t \*rules)  
*Decode base64 string to data with ruleset option.*
- ATCA\_STATUS **atcab\_base64encode** (const uint8\_t \*data, size\_t data\_size, char \*encoded, size\_t \*encoded\_size, const uint8\_t \*rules)  
*Encode data as base64 string with ruleset option.*
- ATCA\_STATUS **atcab\_base64encode** (const uint8\_t \*byte\_array, size\_t array\_len, char \*encoded, size\_t \*encoded\_len)  
*Encode data as base64 string.*
- ATCA\_STATUS **atcab\_base64decode** (const char \*encoded, size\_t encoded\_len, uint8\_t \*byte\_array, size\_t \*array\_len)  
*Decode base64 string to data.*
- size\_t **atcab\_pointer\_delta** (const void \*start, const void \*end)  
*Helper function to calculate the number of bytes between two pointers.*
- int **atcab\_memset\_s** (void \*dest, size\_t destsz, int ch, size\_t count)  
*Guaranteed to perform memory writes regardless of optimization level. Matches memset\_s signature.*
- char **lib\_toupper** (char c)  
*Converts a character to uppercase.*
- char **lib\_tolower** (char c)  
*Converts a character to lowercase.*
- const char \* **lib\_strcasestr** (const char \*haystack, const char \*needle)  
*Search for a substring in a case insensitive format.*

## 22.46.1 Detailed Description

Helpers to support the CryptoAuthLib Basic API methods.

### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.46.2 Function Documentation

### 22.46.2.1 atcab\_base64decode()

```
ATCA_STATUS atcab_base64decode (
    const char * encoded,
    size_t encoded_len,
    uint8_t * byte_array,
    size_t * array_len )
```

Decode base64 string to data.

#### Parameters

in	<i>encoded</i>	Base64 string to be decoded.
in	<i>encoded_len</i>	Size of the base64 string in bytes.
out	<i>byte_array</i>	Decoded data will be returned here.
in, out	<i>array_len</i>	As input, the size of the byte_array buffer. As output, the length of the decoded data.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 22.46.2.2 atcab\_base64decode\_()

```
ATCA_STATUS atcab_base64decode_ (
    const char * encoded,
    size_t encoded_size,
    uint8_t * data,
    size_t * data_size,
    const uint8_t * rules )
```

Decode base64 string to data with ruleset option.

#### Parameters

in	<i>encoded</i>	Base64 string to be decoded.
in	<i>encoded_size</i>	Size of the base64 string in bytes.
out	<i>data</i>	Decoded data will be returned here.
in, out	<i>data_size</i>	As input, the size of the byte_array buffer. As output, the length of the decoded data.
in	<i>rules</i>	base64 ruleset to use

### 22.46.2.3 atcab\_base64encode()

```
ATCA_STATUS atcab_base64encode (
    const uint8_t * byte_array,
    size_t array_len,
```



```
char * encoded,
size_t * encoded_len )
```

Encode data as base64 string.

#### Parameters

in	<i>byte_array</i>	Data to be encode in base64.
in	<i>array_len</i>	Size of <i>byte_array</i> in bytes.
in	<i>encoded</i>	Base64 output is returned here.
in, out	<i>encoded_len</i>	As input, the size of the encoded buffer. As output, the length of the encoded base64 character string.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 22.46.2.4 atcab\_base64encode\_()

```
ATCA_STATUS atcab_base64encode_ (
    const uint8_t * data,
    size_t data_size,
    char * encoded,
    size_t * encoded_size,
    const uint8_t * rules )
```

Encode data as base64 string with ruleset option.

#### Parameters

in	<i>data</i>	The input byte array that will be converted to base 64 encoded characters
in	<i>data_size</i>	The length of the byte array
in	<i>encoded</i>	The output converted to base 64 encoded characters.
in, out	<i>encoded_size</i>	Input: The size of the encoded buffer, Output: The length of the encoded base 64 character string
in	<i>rules</i>	ruleset to use during encoding

#### 22.46.2.5 atcab\_bin2hex\_()

```
ATCA_STATUS atcab_bin2hex_ (
    const uint8_t * bin,
    size_t bin_size,
    char * hex,
    size_t * hex_size,
    bool is_pretty,
```

```
bool is_space,  
bool is_upper )
```

Function that converts a binary buffer to a hex string suitable for easy reading.

Parameters

in	<i>bin</i>	Input data to convert.
in	<i>bin_size</i>	Size of data to convert.
out	<i>hex</i>	Buffer that receives hex string.
in, out	<i>hex_size</i>	As input, the size of the hex buffer. As output, the size of the output hex.
in	<i>is_pretty</i>	Indicates whether new lines should be added for pretty printing.
in	<i>is_space</i>	Convert the output hex with space between it.
in	<i>is_upper</i>	Convert the output hex to upper case.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.46.2.6 atcab\_hex2bin()

```
ATCA_STATUS atcab_hex2bin (  
    const char * ascii_hex,  
    size_t ascii_hex_len,  
    uint8_t * binary,  
    size_t * bin_len )
```

Function that converts a hex string to binary buffer.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>ascii_hex</i>	Input buffer to convert
in	<i>ascii_hex_len</i>	Length of buffer to convert
out	<i>binary</i>	Buffer that receives binary
in, out	<i>bin_len</i>	As input, the size of the bin buffer. As output, the size of the bin data.

22.46.2.7 atcab\_reversal()

```
ATCA_STATUS atcab_reversal (  
    const uint8_t * bin,
```

```
size_t bin_size,
uint8_t * dest,
size_t * dest_size )
```

To reverse the input data.

Parameters

in	<i>bin</i>	Input data to reverse.
in	<i>bin_size</i>	Size of data to reverse.
out	<i>dest</i>	Buffer to store reversed binary data.
in	<i>dest_size</i>	The size of the dest buffer.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.46.2.8 isAlpha()

```
bool isAlpha (
    char c )
```

Checks to see if a character is an ASCII representation of hex ((c >= 'A') and (c <= 'F')) || ((c >= 'a') and (c <= 'f'))

Parameters

in	<i>c</i>	character to check
----	----------	--------------------

Returns

True if the character is a hex

22.46.2.9 isBase64()

```
bool isBase64 (
    char c,
    const uint8_t * rules )
```

Returns true if this character is a valid base 64 character or if this is space (A character can be included in a valid base 64 string).

Parameters

in	<i>c</i>	character to check
in	<i>rules</i>	base64 ruleset to use

Returns

True if the character can be included in a valid base 64 string

22.46.2.10 isBase64Digit()

```
bool isBase64Digit (
    char c,
    const uint8_t * rules )
```

Returns true if this character is a valid base 64 character.

Parameters

in	<i>c</i>	character to check
in	<i>rules</i>	base64 ruleset to use

Returns

True if the character can be included in a valid base 64 string

22.46.2.11 isBlankSpace()

```
bool isBlankSpace (
    char c )
```

Checks to see if a character is blank space.

Parameters

in	<i>c</i>	character to check
----	----------	--------------------

Returns

True if the character is blankspace

22.46.2.12 isDigit()

```
bool isDigit (
    char c )
```

Checks to see if a character is an ASCII representation of a digit ((c ge '0') and (c le '9'))

**Parameters**

in	c	character to check
----	---	--------------------

**Returns**

True if the character is a digit

**22.46.2.13 isHex()**

```
bool isHex (
    char c )
```

Returns true if this character is a valid hex character or if this is blankspace (The character can be included in a valid hexstring).

**Parameters**

in	c	character to check
----	---	--------------------

**Returns**

True if the character can be included in a valid hexstring

**22.46.2.14 isHexAlpha()**

```
bool isHexAlpha (
    char c )
```

Checks to see if a character is an ASCII representation of hex ((c >= 'A') and (c <= 'F')) || ((c >= 'a') and (c <= 'f'))

**Parameters**

in	c	character to check
----	---	--------------------

**Returns**

True if the character is a hex

**22.46.2.15 isHexDigit()**

```
bool isHexDigit (
    char c )
```

Returns true if this character is a valid hex character.

Parameters

in	c	character to check
----	---	--------------------

Returns

True if the character can be included in a valid hexstring

22.46.2.16 packHex()

```
ATCA_STATUS packHex (
    const char * ascii_hex,
    size_t ascii_hex_len,
    char * packed_hex,
    size_t * packed_len )
```

Remove spaces from a ASCII hex string.

Parameters

in	ascii_hex	Initial hex string to remove blankspace from
in	ascii_hex_len	Length of the initial hex string
in	packed_hex	Resulting hex string without blankspace
in, out	packed_len	In: Size to packed_hex buffer Out: Number of bytes in the packed hex string

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.47 atca\_helpers.h File Reference

Helpers to support the CryptoAuthLib Basic API methods.

```
#include "cryptoauthlib.h"
```

Functions

- ATCA\_STATUS [atcab\\_bin2hex](#) (const uint8\_t \*bin, size\_t bin\_size, char \*hex, size\_t \*hex\_size)  
Convert a binary buffer to a hex string for easy reading.
- ATCA\_STATUS [atcab\\_bin2hex\\_](#) (const uint8\_t \*bin, size\_t bin\_size, char \*hex, size\_t \*hex\_size, bool is\_↵ pretty, bool is\_space, bool is\_upper)

*Function that converts a binary buffer to a hex string suitable for easy reading.*

- ATCA\_STATUS [atcab\\_hex2bin](#) (const char \*ascii\_hex, size\_t ascii\_hex\_len, uint8\_t \*binary, size\_t \*bin\_len)

*Function that converts a hex string to binary buffer.*

- ATCA\_STATUS [atcab\\_hex2bin\\_](#) (const char \*hex, size\_t hex\_size, uint8\_t \*bin, size\_t \*bin\_size, bool is\_↵ space)
- ATCA\_STATUS [packHex](#) (const char \*ascii\_hex, size\_t ascii\_hex\_len, char \*packed\_hex, size\_t \*packed\_↵ \_len)

*Remove spaces from a ASCII hex string.*

- bool [isDigit](#) (char c)

*Checks to see if a character is an ASCII representation of a digit ((c ge '0') and (c le '9'))*

- bool [isBlankSpace](#) (char c)

*Checks to see if a character is blank space.*

- bool [isAlpha](#) (char c)

*Checks to see if a character is an ASCII representation of hex ((c >= 'A') and (c <= 'F')) || ((c >= 'a') and (c <= 'f'))*

- bool [isHexAlpha](#) (char c)

*Checks to see if a character is an ASCII representation of hex ((c >= 'A') and (c <= 'F')) || ((c >= 'a') and (c <= 'f'))*

- bool [isHex](#) (char c)

*Returns true if this character is a valid hex character or if this is blankspace (The character can be included in a valid hexstring).*

- bool [isHexDigit](#) (char c)

*Returns true if this character is a valid hex character.*

- bool [isBase64](#) (char c, const uint8\_t \*rules)

*Returns true if this character is a valid base 64 character or if this is space (A character can be included in a valid base 64 string).*

- bool [isBase64Digit](#) (char c, const uint8\_t \*rules)

*Returns true if this character is a valid base 64 character.*

- const uint8\_t \* [atcab\\_b64rules\\_default](#) (void)
- const uint8\_t \* [atcab\\_b64rules\\_mime](#) (void)
- const uint8\_t \* [atcab\\_b64rules\\_urlsafe](#) (void)

- ATCA\_STATUS [atcab\\_base64decode\\_](#) (const char \*encoded, size\_t encoded\_size, uint8\_t \*data, size\_t\_↵ \*data\_size, const uint8\_t \*rules)

*Decode base64 string to data with ruleset option.*

- ATCA\_STATUS [atcab\\_base64encode](#) (const uint8\_t \*byte\_array, size\_t array\_len, char \*encoded, size\_t\_↵ \*encoded\_len)

*Encode data as base64 string.*

- ATCA\_STATUS [atcab\\_base64encode\\_](#) (const uint8\_t \*data, size\_t data\_size, char \*encoded, size\_t\_↵ \*encoded\_size, const uint8\_t \*rules)

*Encode data as base64 string with ruleset option.*

- ATCA\_STATUS [atcab\\_base64decode](#) (const char \*encoded, size\_t encoded\_len, uint8\_t \*byte\_array, size\_t\_↵ \*array\_len)

*Decode base64 string to data.*

- ATCA\_STATUS [atcab\\_reversal](#) (const uint8\_t \*bin, size\_t bin\_size, uint8\_t \*dest, size\_t \*dest\_size)

*To reverse the input data.*

- int [atcab\\_memset\\_s](#) (void \*dest, size\_t destsz, int ch, size\_t count)

*Guaranteed to perform memory writes regardless of optimization level. Matches memset\_s signature.*

- size\_t [atcab\\_pointer\\_delta](#) (const void \*start, const void \*end)

*Helper function to calculate the number of bytes between two pointers.*

- char [lib\\_toupper](#) (char c)

*Converts a character to uppercase.*

- char [lib\\_tolower](#) (char c)

*Converts a character to lowercase.*

### 22.47.1 Detailed Description

Helpers to support the CryptoAuthLib Basic API methods.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.48 atca\_iface.c File Reference

Microchip CryptoAuthLib hardware interface object.

```
#include "cryptoauthlib.h"
#include <ctype.h>
```

### Data Structures

- struct [devtype\\_names\\_t](#)

### Functions

- ATCA\_STATUS [initATCAiface](#) ([ATCAifaceCfg](#) \*cfg, [ATCAiface](#) ca\_iface)  
*Initializer for ATCAiface objects.*
- ATCA\_STATUS [atinit](#) ([ATCAiface](#) ca\_iface)  
*Performs the HAL initialization by calling intermediate HAL wrapper function. If using the basic API, the [atcab\\_init\(\)](#) function should be called instead.*
- ATCA\_STATUS [atsend](#) ([ATCAiface](#) ca\_iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*Sends the data to the device by calling intermediate HAL wrapper function.*
- ATCA\_STATUS [atreceive](#) ([ATCAiface](#) ca\_iface, uint8\_t word\_address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*Receives data from the device by calling intermediate HAL wrapper function.*
- ATCA\_STATUS [atcontrol](#) ([ATCAiface](#) ca\_iface, uint8\_t option, void \*param, size\_t paramlen)  
*Perform control operations with the underlying hal driver.*
- ATCA\_STATUS [atwake](#) ([ATCAiface](#) ca\_iface)  
*Wakes up the device by calling intermediate HAL wrapper function. The [atcab\\_wakeup\(\)](#) function should be used instead.*
- ATCA\_STATUS [atidle](#) ([ATCAiface](#) ca\_iface)  
*Puts the device into idle state by calling intermediate HAL wrapper function. The [atcab\\_idle\(\)](#) function should be used instead.*
- ATCA\_STATUS [atsleep](#) ([ATCAiface](#) ca\_iface)  
*Puts the device into sleep state by calling intermediate HAL wrapper function. The [atcab\\_sleep\(\)](#) function should be used instead.*
- [ATCAifaceCfg](#) \* [atgetifacecfg](#) ([ATCAiface](#) ca\_iface)  
*Returns the logical interface configuration for the device.*
- void \* [atgetifacehaldat](#) ([ATCAiface](#) ca\_iface)  
*Returns the HAL data pointer for the device.*
- bool [ifacetype\\_is\\_kit](#) ([ATCAifaceType](#) iface\_type)  
*Check if the given interface is a "kit protocol" one.*
- bool [atca\\_iface\\_is\\_kit](#) ([ATCAiface](#) ca\_iface)



Check if the given interface is configured as a "kit protocol" one where transactions are atomic.

- bool [atca\\_iface\\_is\\_swi](#) ([ATCAIface](#) ca\_iface)

Check if the given interface is configured as a SWI.

- int [atca\\_iface\\_get\\_retries](#) ([ATCAIface](#) ca\_iface)

Retrieve the number of retries for a configured interface.

- uint16\_t [atca\\_iface\\_get\\_wake\\_delay](#) ([ATCAIface](#) ca\_iface)

Retrieve the wake/retry delay for a configured interface/device.

- uint8\_t [ifacecfg\\_get\\_address](#) ([ATCAIfaceCfg](#) \*cfg)

Retrieves the device address given an interface configuration.

- ATCA\_STATUS [ifacecfg\\_set\\_address](#) ([ATCAIfaceCfg](#) \*cfg, uint8\_t [address](#), ATCAKitType kitiface)

Change the address of the selected device.

- ATCA\_STATUS [releaseATCAIface](#) ([ATCAIface](#) ca\_iface)

Instruct the HAL driver to release any resources associated with this interface.

- void [deleteATCAIface](#) ([ATCAIface](#) \*ca\_iface)

Instruct the HAL driver to release any resources associated with this interface, then delete the object.

- ATCADeviceType [iface\\_get\\_device\\_type\\_by\\_name](#) (const char \*name)

Get the ATCADeviceType for a string that looks like a part number.

## 22.48.1 Detailed Description

Microchip CryptoAuthLib hardware interface object.

### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.49 atca\_iface.h File Reference

Microchip Crypto Auth hardware interface object.

```
#include <stdint.h>
#include <stddef.h>
#include "atca_config.h"
#include "atca_devtypes.h"
#include "atca_status.h"
```

## Data Structures

- struct [ATCAIfaceCfg](#)
- struct [ATCAHAL\\_t](#)

*HAL Driver Structure.*

- struct [atca\\_iface](#)

*atca\_iface is the context structure for a configured interface*

## Macros

- #define **ATCA\_IFACECFG\_NAME**(x) (x)
- #define **ATCA\_IFACECFG\_I2C\_ADDRESS**(c) (c)->cfg.atcai2c.address
- #define **ATCA\_IFACECFG\_I2C\_BAUD**(c) (c)->cfg.atcai2c.baud
- #define **ATCA\_IFACECFG\_VALUE**(c, v) (c)->cfg.v

## Typedefs

- typedef struct [atca\\_iface](#) \* **ATCAIface**
- typedef struct [atca\\_iface](#) **atca\_iface\_t**  
*[atca\\_iface](#) is the context structure for a configured interface*

## Enumerations

- enum [ATCAIfaceType](#) {  
  [ATCA\\_I2C\\_IFACE](#) = 0 , [ATCA\\_SWI\\_IFACE](#) = 1 , [ATCA\\_UART\\_IFACE](#) = 2 , [ATCA\\_SPI\\_IFACE](#) = 3 ,  
  [ATCA\\_HID\\_IFACE](#) = 4 , [ATCA\\_KIT\\_IFACE](#) = 5 , [ATCA\\_CUSTOM\\_IFACE](#) = 6 , [ATCA\\_I2C\\_GPIO\\_IFACE](#) = 7 ,  
  [ATCA\\_SWI\\_GPIO\\_IFACE](#) = 8 , [ATCA\\_SPI\\_GPIO\\_IFACE](#) = 9 , [ATCA\\_UNKNOWN\\_IFACE](#) = 0xFE }
- enum [ATCAKitType](#) {  
  [ATCA\\_KIT\\_AUTO\\_IFACE](#) , [ATCA\\_KIT\\_I2C\\_IFACE](#) , [ATCA\\_KIT\\_SWI\\_IFACE](#) , [ATCA\\_KIT\\_SPI\\_IFACE](#) ,  
  [ATCA\\_KIT\\_UNKNOWN\\_IFACE](#) }

## Functions

- ATCA\_STATUS [initATCAIface](#) ([ATCAIfaceCfg](#) \*cfg, [ATCAIface](#) ca\_iface)  
*Initializer for ATCAIface objects.*
- ATCA\_STATUS [releaseATCAIface](#) ([ATCAIface](#) ca\_iface)  
*Instruct the HAL driver to release any resources associated with this interface.*
- void [deleteATCAIface](#) ([ATCAIface](#) \*ca\_iface)  
*Instruct the HAL driver to release any resources associated with this interface, then delete the object.*
- ATCA\_STATUS [atinit](#) ([ATCAIface](#) ca\_iface)  
*Performs the HAL initialization by calling intermediate HAL wrapper function. If using the basic API, the [atcab\\_init\(\)](#) function should be called instead.*
- ATCA\_STATUS [atsend](#) ([ATCAIface](#) ca\_iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*Sends the data to the device by calling intermediate HAL wrapper function.*
- ATCA\_STATUS [atreceive](#) ([ATCAIface](#) ca\_iface, uint8\_t word\_address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*Receives data from the device by calling intermediate HAL wrapper function.*
- ATCA\_STATUS [atcontrol](#) ([ATCAIface](#) ca\_iface, uint8\_t option, void \*param, size\_t paramlen)  
*Perform control operations with the underlying hal driver.*
- ATCA\_STATUS [atwake](#) ([ATCAIface](#) ca\_iface)  
*Wakes up the device by calling intermediate HAL wrapper function. The [atcab\\_wakeup\(\)](#) function should be used instead.*
- ATCA\_STATUS [atidle](#) ([ATCAIface](#) ca\_iface)  
*Puts the device into idle state by calling intermediate HAL wrapper function. The [atcab\\_idle\(\)](#) function should be used instead.*
- ATCA\_STATUS [atsleep](#) ([ATCAIface](#) ca\_iface)  
*Puts the device into sleep state by calling intermediate HAL wrapper function. The [atcab\\_sleep\(\)](#) function should be used instead.*
- [ATCAIfaceCfg](#) \* [atgetifacecfg](#) ([ATCAIface](#) ca\_iface)  
*Returns the logical interface configuration for the device.*

- void \* **atgetifacehaldat** (**ATCAIface** ca\_iface)  
*Returns the HAL data pointer for the device.*
- **ATCA\_STATUS ifacecfg\_set\_address** (**ATCAIfaceCfg** \*cfg, uint8\_t address, **ATCAKitType** kitiface)  
*Change the address of the selected device.*
- uint8\_t **ifacecfg\_get\_address** (**ATCAIfaceCfg** \*cfg)  
*Retrieves the device address given an interface configuration.*
- bool **ifacetype\_is\_kit** (**ATCAIfaceType** iface\_type)  
*Check if the given interface is a "kit protocol" one.*
- bool **atca\_iface\_is\_kit** (**ATCAIface** ca\_iface)  
*Check if the given interface is configured as a "kit protocol" one where transactions are atomic.*
- bool **atca\_iface\_is\_swi** (**ATCAIface** ca\_iface)  
*Check if the given interface is configured as a SWI.*
- int **atca\_iface\_get\_retries** (**ATCAIface** ca\_iface)  
*Retrive the number of retries for a configured interface.*
- uint16\_t **atca\_iface\_get\_wake\_delay** (**ATCAIface** ca\_iface)  
*Retrive the wake/retry delay for a configured interface/device.*
- **ATCADeviceType iface\_get\_device\_type\_by\_name** (const char \*name)  
*Get the ATCADeviceType for a string that looks like a part number.*

## Variables

- ```

struct {
    uint8_t address
    uint8_t bus
    uint32_t baud
} atcai2c

```
- ```

struct {
    uint8_t address
    uint8_t bus
} atcaswi

```
- ```

struct {
    uint8_t bus
    uint8_t select_pin
    uint32_t baud
} atcaspi

```
- ```

struct {
    ATCAKitType dev_interface
    uint8_t dev_identity
    uint8_t port
    uint32_t baud
    uint8_t wordsize
    uint8_t parity
    uint8_t stopbits
} atcauart

```
-

```
struct {
    int idx
    ATCAKitType dev_interface
    uint8_t dev_identity
        uint32_t vid
        uint32_t pid
        uint32_t packetsize
    } atcahid
```

•

```
struct {
    ATCAKitType dev_interface
    uint8_t dev_identity
    uint32_t flags
} atcakit
```

•

```
struct {
    ATCA_STATUS(* halinit )(void *hal, void *cfg)
    ATCA_STATUS(* halpostinit )(void *iface)
    ATCA_STATUS(* halsend )(void *iface, uint8_t
        word_address, uint8_t *txdata,
        int txlength)
    ATCA_STATUS(* halreceive )(void *iface, uint8_t
        word_address, uint8_t *rxdata,
        uint16_t *rxlength)
    ATCA_STATUS(* halwake )(void *iface)
    ATCA_STATUS(* halidle )(void *iface)
    ATCA_STATUS(* halsleep )(void *iface)
    ATCA_STATUS(* halrelease )(void *hal_data)
} atcacustom
```

## 22.49.1 Detailed Description

Microchip Crypto Auth hardware interface object.

### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.49.2 Variable Documentation

### 22.49.2.1 address

```
uint8_t address
```

Device address - the upper 7 bits are the I2c address bits

## 22.50 atca\_platform.h File Reference

Configure the platform interfaces for cryptoauthlib.

```
#include <stddef.h>
#include <string.h>
```

### Macros

- #define **hal\_memset\_s** [atcab\\_memset\\_s](#)

### Functions

- void \* **hal\_malloc** (size\_t size)
- void **hal\_free** (void \*ptr)
- const char \* **lib\_strcasestr** (const char \*haystack, const char \*needle)

*Search for a substring in a case insensitive format.*

### 22.50.1 Detailed Description

Configure the platform interfaces for cryptoauthlib.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.51 atca\_status.h File Reference

Microchip Crypto Auth status codes.

```
#include <stdint.h>
#include "atca_config.h"
#include "atca_compiler.h"
```

## Macros

- #define `ATCA_SUCCESS` (0)
- #define `ATCA_CONFIG_ZONE_LOCKED` (0x01)
- #define `ATCA_DATA_ZONE_LOCKED` (0x02)
- #define `ATCA_WAKE_FAILED` (-48)
- #define `ATCA_CHECKMAC_VERIFY_FAILED` (-47)
- #define `ATCA_PARSE_ERROR` (-46)
- #define `ATCA_STATUS_CRC` (-44)
- #define `ATCA_STATUS_UNKNOWN` (-43)
- #define `ATCA_STATUS_ECC` (-42)
- #define `ATCA_STATUS_SELFTEST_ERROR` (-41)
- #define `ATCA_FUNC_FAIL` (-32)
- #define `ATCA_GEN_FAIL` (-31)
- #define `ATCA_BAD_PARAM` (-30)
- #define `ATCA_INVALID_ID` (-29)
- #define `ATCA_INVALID_SIZE` (-28)
- #define `ATCA_RX_CRC_ERROR` (-27)
- #define `ATCA_RX_FAIL` (-26)
- #define `ATCA_RX_NO_RESPONSE` (-25)
- #define `ATCA_RESYNC_WITH_WAKEUP` (-24)
- #define `ATCA_PARITY_ERROR` (-23)
- #define `ATCA_TX_TIMEOUT` (-22)
- #define `ATCA_RX_TIMEOUT` (-21)
- #define `ATCA_TOO_MANY_COMM_RETRIES` (-20)
- #define `ATCA_SMALL_BUFFER` (-19)
- #define `ATCA_COMM_FAIL` (-16)
- #define `ATCA_TIMEOUT` (-15)
- #define `ATCA_BAD_OPCODE` (-14)
- #define `ATCA_WAKE_SUCCESS` (-13)
- #define `ATCA_EXECUTION_ERROR` (-12)
- #define `ATCA_UNIMPLEMENTED` (-11)
- #define `ATCA_ASSERT_FAILURE` (-10)
- #define `ATCA_TX_FAIL` (-9)
- #define `ATCA_NOT_LOCKED` (-8)
- #define `ATCA_NO_DEVICES` (-7)
- #define `ATCA_HEALTH_TEST_ERROR` (-6)
- #define `ATCA_ALLOC_FAILURE` (-5)
- #define `ATCA_USE_FLAGS_CONSUMED` (-4)
- #define `ATCA_NOT_INITIALIZED` (-3)
- #define `ATCA_STATUS_AUTH_BIT` 0x40u
- #define `ATCA_STATUS_AUTH_BIT_COMPLEMENT` ~(ATCA\_STATUS\_AUTH\_BIT & 0xffu)

## Typedefs

- typedef int `ATCA_STATUS`

### 22.51.1 Detailed Description

Microchip Crypto Auth status codes.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.51.2 Macro Definition Documentation

### 22.51.2.1 ATCA\_ALLOC\_FAILURE

```
#define ATCA_ALLOC_FAILURE (-5)
```

STATUS (0xFB): Couldn't allocate required memory

### 22.51.2.2 ATCA\_ASSERT\_FAILURE

```
#define ATCA_ASSERT_FAILURE (-10)
```

STATUS (0xF6): Code failed run-time consistency check

### 22.51.2.3 ATCA\_BAD\_OPCODE

```
#define ATCA_BAD_OPCODE (-14)
```

STATUS (0xF2): opcode is not supported by the device

### 22.51.2.4 ATCA\_BAD\_PARAM

```
#define ATCA_BAD_PARAM (-30)
```

STATUS (0xE2): bad argument (out of range, null pointer, etc.)

### 22.51.2.5 ATCA\_CHECKMAC\_VERIFY\_FAILED

```
#define ATCA_CHECKMAC_VERIFY_FAILED (-47)
```

STATUS (0xD1): response status byte indicates CheckMac failure(status byte = 0x01)

### 22.51.2.6 ATCA\_COMM\_FAIL

```
#define ATCA_COMM_FAIL (-16)
```

STATUS (0xF0): Communication with device failed. Same as in hardware dependent modules.

### 22.51.2.7 ATCA\_EXECUTION\_ERROR

```
#define ATCA_EXECUTION_ERROR (-12)
```

STATUS (0xF4): chip was in a state where it could not execute the command, response status byte indicates command execution error (status byte = 0x0F)

### 22.51.2.8 ATCA\_FUNC\_FAIL

```
#define ATCA_FUNC_FAIL (-32)
```

STATUS (0xE0): Function could not execute due to incorrect condition / state.

### 22.51.2.9 ATCA\_GEN\_FAIL

```
#define ATCA_GEN_FAIL (-31)
```

STATUS (0xE1): unspecified error

### 22.51.2.10 ATCA\_HEALTH\_TEST\_ERROR

```
#define ATCA_HEALTH_TEST_ERROR (-6)
```

STATUS (0xFA): random number generator health test error

### 22.51.2.11 ATCA\_INVALID\_ID

```
#define ATCA_INVALID_ID (-29)
```

STATUS (0xE3): invalid device id, id not set

### 22.51.2.12 ATCA\_INVALID\_SIZE

```
#define ATCA_INVALID_SIZE (-28)
```

STATUS (0xE4): Count value is out of range or greater than buffer size.

### 22.51.2.13 ATCA\_NO\_DEVICES

```
#define ATCA_NO_DEVICES (-7)
```

STATUS (0xF9): For protocols that support device discovery (kit protocol), no devices were found

### 22.51.2.14 ATCA\_NOT\_INITIALIZED

```
#define ATCA_NOT_INITIALIZED (-3)
```

STATUS (0xFD): The library has not been initialized so the command could not be executed

### 22.51.2.15 ATCA\_NOT\_LOCKED

```
#define ATCA_NOT_LOCKED (-8)
```

STATUS (0xF8): required zone was not locked



**22.51.2.16 ATCA\_PARITY\_ERROR**

```
#define ATCA_PARITY_ERROR (-23)
```

STATUS (0xE9): for protocols needing parity

**22.51.2.17 ATCA\_PARSE\_ERROR**

```
#define ATCA_PARSE_ERROR (-46)
```

STATUS (0xD2): response status byte indicates parsing error(status byte = 0x03)

**22.51.2.18 ATCA\_RESYNC\_WITH\_WAKEUP**

```
#define ATCA_RESYNC_WITH_WAKEUP (-24)
```

STATUS (0xE8): Re-synchronization succeeded, but only after generating a Wake-up

**22.51.2.19 ATCA\_RX\_CRC\_ERROR**

```
#define ATCA_RX_CRC_ERROR (-27)
```

STATUS (0xE5): CRC error in data received from device

**22.51.2.20 ATCA\_RX\_FAIL**

```
#define ATCA_RX_FAIL (-26)
```

STATUS (0xE6): Timed out while waiting for response. Number of bytes received is > 0.

**22.51.2.21 ATCA\_RX\_NO\_RESPONSE**

```
#define ATCA_RX_NO_RESPONSE (-25)
```

STATUS (0xE7): Not an error while the Command layer is polling for a command response.

**22.51.2.22 ATCA\_RX\_TIMEOUT**

```
#define ATCA_RX_TIMEOUT (-21)
```

STATUS (0xEB): for Microchip PHY protocol, timeout on receipt waiting for master

**22.51.2.23 ATCA\_SMALL\_BUFFER**

```
#define ATCA_SMALL_BUFFER (-19)
```

STATUS (0xED): Supplied buffer is too small for data required

### 22.51.2.24 ATCA\_STATUS\_CRC

```
#define ATCA_STATUS_CRC (-44)
```

STATUS (0xD4): response status byte indicates DEVICE did not receive data properly(status byte = 0xFF)

### 22.51.2.25 ATCA\_STATUS\_ECC

```
#define ATCA_STATUS_ECC (-42)
```

STATUS (0xD6): response status byte is ECC fault(status byte = 0x05)

### 22.51.2.26 ATCA\_STATUS\_SELFTEST\_ERROR

```
#define ATCA_STATUS_SELFTEST_ERROR (-41)
```

STATUS (0xD7): response status byte is Self Test Error, chip in failure mode (status byte = 0x07)

### 22.51.2.27 ATCA\_STATUS\_UNKNOWN

```
#define ATCA_STATUS_UNKNOWN (-43)
```

STATUS (0xD5): response status byte is unknown

### 22.51.2.28 ATCA\_SUCCESS

```
#define ATCA_SUCCESS (0)
```

STATUS (0x00): Function Successful

### 22.51.2.29 ATCA\_TIMEOUT

```
#define ATCA_TIMEOUT (-15)
```

STATUS (0xF1): Timed out while waiting for response. Number of bytes received is 0.

### 22.51.2.30 ATCA\_TOO\_MANY\_COMM\_RETRIES

```
#define ATCA_TOO_MANY_COMM_RETRIES (-20)
```

STATUS (0xEC): Device did not respond too many times during a transmission. Could indicate no device present.

### 22.51.2.31 ATCA\_TX\_FAIL

```
#define ATCA_TX_FAIL (-9)
```

STATUS (0xF7): Failed to write

**22.51.2.32 ATCA\_TX\_TIMEOUT**

```
#define ATCA_TX_TIMEOUT (-22)
```

STATUS (0xEA): for Microchip PHY protocol, timeout on transmission waiting for master

**22.51.2.33 ATCA\_UNIMPLEMENTED**

```
#define ATCA_UNIMPLEMENTED (-11)
```

STATUS (0xF5): Function or some element of it hasn't been implemented yet

**22.51.2.34 ATCA\_USE\_FLAGS\_CONSUMED**

```
#define ATCA_USE_FLAGS_CONSUMED (-4)
```

STATUS (0xFC): Use flags on the device indicates its consumed fully

**22.51.2.35 ATCA\_WAKE\_FAILED**

```
#define ATCA_WAKE_FAILED (-48)
```

STATUS (0xD0): response status byte indicates CheckMac failure(status byte = 0x01)

**22.51.2.36 ATCA\_WAKE\_SUCCESS**

```
#define ATCA_WAKE_SUCCESS (-13)
```

STATUS (0xF3): received proper wake token

**22.52 atca\_utils\_sizes.c File Reference**

API to Return structure sizes of cryptoauthlib structures.

```
#include "cryptoauthlib.h"
#include "cal_internal.h"
#include "atcacert/atcacert_check_config.h"
#include "atcacert/atcacert_date.h"
#include "atcacert/atcacert_def.h"
#include "host/atca_host.h"
```

**Macros**

- **#define SIZE\_OF\_API\_T(x)** size\_t x ## \_size(void); size\_t x ## \_size(void) { return sizeof( x ); }
- **#define SIZE\_OF\_API\_S(x)** size\_t x ## \_size(void); size\_t x ## \_size(void) { return sizeof(struct x ); }

## Functions

- `size_t atcacert_tm_utc_t_size` (void)
- `size_t atcacert_date_format_t_size` (void)
- `size_t atcacert_cert_type_t_size` (void)
- `size_t atcacert_cert_sn_src_t_size` (void)
- `size_t atcacert_device_zone_t_size` (void)
- `size_t atcacert_std_cert_element_t_size` (void)
- `size_t atcacert_device_loc_t_size` (void)
- `size_t atcacert_cert_loc_t_size` (void)
- `size_t atcacert_cert_element_t_size` (void)
- `size_t atcacert_def_t_size` (void)
- `size_t atcacert_build_state_t_size` (void)
- `size_t atca_temp_key_t_size` (void)
- `size_t atca_include_data_in_out_size` (void)
- `size_t atca_nonce_in_out_t_size` (void)
- `size_t atca_io_decrypt_in_out_t_size` (void)
- `size_t atca_verify_mac_in_out_t_size` (void)
- `size_t atca_secureboot_enc_in_out_t_size` (void)
- `size_t atca_secureboot_mac_in_out_t_size` (void)
- `size_t atca_mac_in_out_t_size` (void)
- `size_t atca_hmac_in_out_size` (void)
- `size_t atca_gen_dig_in_out_t_size` (void)
- `size_t atca_write_mac_in_out_t_size` (void)
- `size_t atca_derive_key_in_out_size` (void)
- `size_t atca_derive_key_mac_in_out_size` (void)
- `size_t atca_decrypt_in_out_size` (void)
- `size_t atca_check_mac_in_out_t_size` (void)
- `size_t atca_verify_in_out_t_size` (void)
- `size_t atca_gen_key_in_out_t_size` (void)
- `size_t atca_sign_internal_in_out_t_size` (void)
- `size_t bool_size` (void)
- `size_t ATCAPacket_size` (void)
- `size_t atca_device_size` (void)
- `size_t ATCADeviceType_size` (void)
- `size_t ATCAIfaceType_size` (void)
- `size_t ATCAIfaceCfg_size` (void)
- `size_t atca_iface_size` (void)
- `size_t ATCA_STATUS_size` (void)
- `size_t atcac_sha1_ctx_size` (void)
- `size_t atcac_sha1_ctx_t_size` (void)
- `size_t atcac_sha2_256_ctx_size` (void)
- `size_t atcac_sha2_256_ctx_t_size` (void)
- `size_t atcac_hmac_ctx_size` (void)
- `size_t atcac_hmac_ctx_t_size` (void)

### 22.52.1 Detailed Description

API to Return structure sizes of cryptoauthlib structures.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.53 atca\_version.h File Reference

Microchip CryptoAuth Library Version.

### Macros

- `#define ATCA_LIBRARY_VERSION_DATE "20240626"`
- `#define ATCA_LIBRARY_VERSION_MAJOR 3`
- `#define ATCA_LIBRARY_VERSION_MINOR 7`
- `#define ATCA_LIBRARY_VERSION_BUILD 5`

### 22.53.1 Detailed Description

Microchip CryptoAuth Library Version.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.54 atcacert.h File Reference

Declarations common to all atcacert code.

```
#include <stddef.h>
#include <stdint.h>
#include "atcacert_check_config.h"
#include "atca_status.h"
```

### Macros

- `#define FALSE (0)`
- `#define TRUE (1)`
- `#define ATCACERT_E_SUCCESS ATCA_SUCCESS`
- `#define ATCACERT_E_ERROR ATCA_GEN_FAIL`
- `#define ATCACERT_E_BAD_PARAMS ATCA_BAD_PARAM`
- `#define ATCACERT_E_BUFFER_TOO_SMALL ATCA_SMALL_BUFFER`
- `#define ATCACERT_E_UNIMPLEMENTED ATCA_UNIMPLEMENTED`
- `#define ATCACERT_E_DECODING_ERROR 4`
- `#define ATCACERT_E_INVALID_DATE 5`
- `#define ATCACERT_E_UNEXPECTED_ELEM_SIZE 7`
- `#define ATCACERT_E_ELEM_MISSING 8`
- `#define ATCACERT_E_ELEM_OUT_OF_BOUNDS 9`
- `#define ATCACERT_E_BAD_CERT 10`
- `#define ATCACERT_E_WRONG_CERT_DEF 11`
- `#define ATCACERT_E_VERIFY_FAILED 12`
- `#define ATCACERT_E_INVALID_TRANSFORM 13`

### 22.54.1 Detailed Description

Declarations common to all atcacert code.

These are common definitions used by all the atcacert code.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.55 atcacert\_check\_config.h File Reference

Configuration check and defaults for the atcacert module.

```
#include "cryptoauthlib.h"
#include "crypto/atca_crypto_sw.h"
```

### Macros

- `#define HOSTLIB_CERT_EN DEFAULT_DISABLED`
- `#define ATCACERT_INTEGRATION_EN HOSTLIB_CERT_EN`
- `#define ATCACERT_COMPCERT_EN (CALIB_ECC_SUPPORT || CALIB_CA2_CERT_SUPPORT)`
- `#define ATCACERT_HW_CHALLENGE_EN (ATCAB_RANDOM_EN && (ATCA_ECC_SUPPORT || ATCA_TA_SUPPORT))`
- `#define ATCACERT_HW_VERIFY_EN (ATCAB_VERIFY_EXTERN_EN && (ATCA_ECC_SUPPORT || ATCA_TA_SUPPORT))`
- `#define ATCACERT_DATEFMT_ISO_EN DEFAULT_ENABLED`
- `#define ATCACERT_DATEFMT_UTC_EN DEFAULT_ENABLED`
- `#define ATCACERT_DATEFMT_POSIX_EN DEFAULT_ENABLED`
- `#define ATCACERT_DATEFMT_GEN_EN DEFAULT_ENABLED`

### 22.55.1 Detailed Description

Configuration check and defaults for the atcacert module.

#### Copyright

(c) 2015-2022 Microchip Technology Inc. and its subsidiaries.

## 22.56 atcacert\_client.c File Reference

Client side cert i/o methods. These declarations deal with the client-side, the node being authenticated, of the authentication process. It is assumed the client has an ECC CryptoAuthentication device (e.g. ATECC508A) and the certificates are stored on that device.

```
#include <limits.h>
#include <stdlib.h>
#include "atcacert_client.h"
#include "atcacert_der.h"
#include "atcacert_pem.h"
#include "cryptoauthlib.h"
#include "calib/calib_basic.h"
#include "talib/talib_basic.h"
#include "talib/talib_internal.h"
```

## Functions

- ATCA\_STATUS `atcacert_read_cert_ext` (ATCADevice device, const `atcacert_def_t` \*cert\_def, const uint8\_t ca\_public\_key[64], uint8\_t \*cert, size\_t \*cert\_size)  
*Reads the certificate specified by the certificate definition from the ATECC508A device.*
- ATCA\_STATUS `atcacert_read_cert` (const `atcacert_def_t` \*cert\_def, const uint8\_t ca\_public\_key[64], uint8\_t \*cert, size\_t \*cert\_size)  
*Reads the certificate specified by the certificate definition from the ATECC508A device.*
- ATCA\_STATUS `atcacert_read_cert_size_ext` (ATCADevice device, const `atcacert_def_t` \*cert\_def, size\_t \*cert\_size)  
*Return the actual certificate size in bytes for a given cert def. Certificate can be variable size, so this gives the absolute buffer size when reading the certificates.*
- ATCA\_STATUS `atcacert_read_cert_size` (const `atcacert_def_t` \*cert\_def, size\_t \*cert\_size)  
*Return the actual certificate size in bytes for a given cert def. Certificate can be variable size, so this gives the absolute buffer size when reading the certificates.*

### 22.56.1 Detailed Description

Client side cert i/o methods. These declarations deal with the client-side, the node being authenticated, of the authentication process. It is assumed the client has an ECC CryptoAuthentication device (e.g. ATECC508A) and the certificates are stored on that device.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.57 atcacert\_client.h File Reference

Client side cert i/o methods. These declarations deal with the client-side, the node being authenticated, of the authentication process. It is assumed the client has an ECC CryptoAuthentication device (e.g. ATECC508A) and the certificates are stored on that device.

```
#include <stddef.h>
#include <stdint.h>
#include "atcacert_def.h"
```

## Functions

- ATCA\_STATUS `atcacert_read_device_loc` (const `atcacert_device_loc_t` \*device\_loc, uint8\_t \*data)  
*Read the data from a device location.*
- ATCA\_STATUS `atcacert_read_device_loc_ext` (ATCADevice device, const `atcacert_device_loc_t` \*device\_loc, uint8\_t \*data)  
*Read the data from a device location.*
- ATCA\_STATUS `atcacert_read_cert` (const `atcacert_def_t` \*cert\_def, const uint8\_t ca\_public\_key[64], uint8\_t \*cert, size\_t \*cert\_size)  
*Reads the certificate specified by the certificate definition from the ATECC508A device.*
- ATCA\_STATUS `atcacert_read_cert_ext` (ATCADevice device, const `atcacert_def_t` \*cert\_def, const uint8\_t ca\_public\_key[64], uint8\_t \*cert, size\_t \*cert\_size)  
*Reads the certificate specified by the certificate definition from the ATECC508A device.*

- ATCA\_STATUS [atcacert\\_write\\_cert](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size)  
*Take a full certificate and write it to the ATECC508A device according to the certificate definition.*
- ATCA\_STATUS [atcacert\\_write\\_cert\\_ext](#) (ATCADevice device, const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size)  
*Take a full certificate and write it to the ATECC508A device according to the certificate definition.*
- ATCA\_STATUS [atcacert\\_create\\_csr](#) (const [atcacert\\_def\\_t](#) \*csr\_def, uint8\_t \*csr, size\_t \*csr\_size)  
*Creates a CSR specified by the CSR definition from the ATECC508A device. This process involves reading the dynamic CSR data from the device and combining it with the template found in the CSR definition, then signing it. Return the CSR in der format.*
- ATCA\_STATUS [atcacert\\_create\\_csr\\_pem](#) (const [atcacert\\_def\\_t](#) \*csr\_def, char \*csr, size\_t \*csr\_size)  
*Creates a CSR specified by the CSR definition from the ATECC508A device. This process involves reading the dynamic CSR data from the device and combining it with the template found in the CSR definition, then signing it. Return the CSR in der format.*
- ATCA\_STATUS [atcacert\\_get\\_response](#) (uint8\_t device\_private\_key\_slot, const uint8\_t challenge[32], uint8\_t \*response[64])  
*Calculates the response to a challenge sent from the host.*
- ATCA\_STATUS [atcacert\\_read\\_subj\\_key\\_id](#) (const [atcacert\\_def\\_t](#) \*cert\_def, uint8\_t subj\_key\_id[20])  
*Reads the subject key ID based on a certificate definition.*
- ATCA\_STATUS [atcacert\\_read\\_subj\\_key\\_id\\_ext](#) (ATCADevice device, const [atcacert\\_def\\_t](#) \*cert\_def, uint8\_t subj\_key\_id[20])  
*Reads the subject key ID based on a certificate definition.*
- ATCA\_STATUS [atcacert\\_read\\_cert\\_size](#) (const [atcacert\\_def\\_t](#) \*cert\_def, size\_t \*cert\_size)  
*Return the actual certificate size in bytes for a given cert def. Certificate can be variable size, so this gives the absolute buffer size when reading the certificates.*
- ATCA\_STATUS [atcacert\\_read\\_cert\\_size\\_ext](#) (ATCADevice device, const [atcacert\\_def\\_t](#) \*cert\_def, size\_t \*cert\_size)  
*Return the actual certificate size in bytes for a given cert def. Certificate can be variable size, so this gives the absolute buffer size when reading the certificates.*

## 22.57.1 Detailed Description

Client side cert i/o methods. These declarations deal with the client-side, the node being authenticated, of the authentication process. It is assumed the client has an ECC CryptoAuthentication device (e.g. ATECC508A) and the certificates are stored on that device.

### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.58 atcacert\_date.c File Reference

Date handling with regard to certificates.

```
#include <string.h>
#include <limits.h>
#include "atcacert_date.h"
#include "atca_compiler.h"
```



## Functions

- `atcacert_date_format_t atcacert_date_from_asn1_tag` (const `uint8_t` tag)  
*Convert the `asn1` tag for the supported time formats into the local time format.*
- `ATCA_STATUS atcacert_date_enc` (`atcacert_date_format_t` format, const `atcacert_tm_utc_t` \*timestamp, `uint8_t` \*formatted\_date, `size_t` \*formatted\_date\_size)  
*Format a timestamp according to the format type.*
- `ATCA_STATUS atcacert_date_dec` (`atcacert_date_format_t` format, const `uint8_t` \*formatted\_date, `size_t` formatted\_date\_size, `atcacert_tm_utc_t` \*timestamp)  
*Parse a formatted timestamp according to the specified format.*
- `ATCA_STATUS atcacert_date_get_max_date` (`atcacert_date_format_t` format, `atcacert_tm_utc_t` \*timestamp)  
*Return the maximum date available for the given format.*
- `ATCA_STATUS atcacert_date_enc_compcert` (const `atcacert_tm_utc_t` \*issue\_date, `uint8_t` expire\_years, `uint8_t` enc\_dates[3])  
*Encode the issue and expire dates in the format used by the compressed certificate.*
- `ATCA_STATUS atcacert_date_enc_compcert_ext` (const `atcacert_tm_utc_t` \*issue\_date, `uint8_t` expire\_years, `uint8_t` comp\_cert[72u])  
*Encode the issue and expire dates in the format used by the compressed certificate.*
- `ATCA_STATUS atcacert_date_dec_compcert` (const `uint8_t` enc\_dates[3], `atcacert_date_format_t` expire\_date\_format, `atcacert_tm_utc_t` \*issue\_date, `atcacert_tm_utc_t` \*expire\_date)  
*Decode the issue and expire dates from the format used by the compressed certificate.*
- `ATCA_STATUS atcacert_date_dec_compcert_ext` (const `uint8_t` comp\_cert[72u], `atcacert_date_format_t` expire\_date\_format, `atcacert_tm_utc_t` \*issue\_date, `atcacert_tm_utc_t` \*expire\_date)  
*Decode the issue and expire dates from the format used by the compressed certificate.*
- `int atcacert_date_cmp` (const `atcacert_tm_utc_t` \*timestamp1, const `atcacert_tm_utc_t` \*timestamp2)  
*Compare two dates.*

## Variables

- const `size_t ATCACERT_DATE_FORMAT_SIZES` [5]

### 22.58.1 Detailed Description

Date handling with regard to certificates.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.59 atcacert\_date.h File Reference

Declarations for date handling with regard to certificates.

```
#include <stddef.h>
#include "atcacert.h"
```

## Data Structures

- struct [atcacert\\_tm\\_utc\\_s](#)

## Macros

- #define [DATEFMT\\_ISO8601\\_SEP](#) (0U)  
*ISO8601 full date YYYY-MM-DDThh:mm:ssZ.*
- #define [DATEFMT\\_RFC5280.UTC](#) (1U)  
*RFC 5280 (X.509) 4.1.2.5.1 UTCTime format YYMMDDhhmmssZ.*
- #define [DATEFMT\\_POSIX\\_UINT32\\_BE](#) (2U)  
*POSIX (aka UNIX) date format. Seconds since Jan 1, 1970. 32 bit unsigned integer, big endian.*
- #define [DATEFMT\\_POSIX\\_UINT32\\_LE](#) (3U)  
*POSIX (aka UNIX) date format. Seconds since Jan 1, 1970. 32 bit unsigned integer, little endian.*
- #define [DATEFMT\\_RFC5280\\_GEN](#) (4U)  
*RFC 5280 (X.509) 4.1.2.5.2 GeneralizedTime format YYYYMMDDhhmmssZ.*
- #define [DATEFMT\\_INVALID](#) (0xFFU)
- #define [DATEFMT\\_ISO8601\\_SEP\\_SIZE](#) (20)
- #define [DATEFMT\\_RFC5280.UTC\\_SIZE](#) (13)
- #define [DATEFMT\\_POSIX\\_UINT32\\_BE\\_SIZE](#) (4)
- #define [DATEFMT\\_POSIX\\_UINT32\\_LE\\_SIZE](#) (4)
- #define [DATEFMT\\_RFC5280\\_GEN\\_SIZE](#) (15)
- #define [DATEFMT\\_MAX\\_SIZE](#) [DATEFMT\\_ISO8601\\_SEP\\_SIZE](#)
- #define [ATCACERT\\_DATE\\_FORMAT\\_SIZES\\_COUNT](#) 5
- #define [ATCACERT\\_COMP\\_CERT\\_MAX\\_SIZE](#) 72u
- #define [atcacert\\_date\\_enc\\_posix\\_uint32\\_be](#) [atcacert\\_date\\_enc\\_posix\\_be](#)
- #define [atcacert\\_date\\_dec\\_posix\\_uint32\\_be](#) [atcacert\\_date\\_dec\\_posix\\_be](#)
- #define [atcacert\\_date\\_enc\\_posix\\_uint32\\_le](#) [atcacert\\_date\\_enc\\_posix\\_le](#)
- #define [atcacert\\_date\\_dec\\_posix\\_uint32\\_le](#) [atcacert\\_date\\_dec\\_posix\\_le](#)

## Typedefs

- typedef struct [atcacert\\_tm\\_utc\\_s](#) [atcacert\\_tm\\_utc\\_t](#)
- typedef uint8\_t [atcacert\\_date\\_format\\_t](#)

## Functions

- ATCA\_STATUS [atcacert\\_date\\_enc](#) ([atcacert\\_date\\_format\\_t](#) format, const [atcacert\\_tm\\_utc\\_t](#) \*timestamp, uint8\_t \*formatted\_date, size\_t \*formatted\_date\_size)  
*Format a timestamp according to the format type.*
- ATCA\_STATUS [atcacert\\_date\\_dec](#) ([atcacert\\_date\\_format\\_t](#) format, const uint8\_t \*formatted\_date, size\_t formatted\_date\_size, [atcacert\\_tm\\_utc\\_t](#) \*timestamp)  
*Parse a formatted timestamp according to the specified format.*
- ATCA\_STATUS [atcacert\\_date\\_enc\\_compcert](#) (const [atcacert\\_tm\\_utc\\_t](#) \*issue\_date, uint8\_t expire\_years, uint8\_t enc\_dates[3])  
*Encode the issue and expire dates in the format used by the compressed certificate.*
- ATCA\_STATUS [atcacert\\_date\\_enc\\_compcert\\_ext](#) (const [atcacert\\_tm\\_utc\\_t](#) \*issue\_date, uint8\_t expire\_years, uint8\_t comp\_cert[72u])  
*Encode the issue and expire dates in the format used by the compressed certificate.*
- ATCA\_STATUS [atcacert\\_date\\_dec\\_compcert](#) (const uint8\_t enc\_dates[3], [atcacert\\_date\\_format\\_t](#) expire\_date\_format, [atcacert\\_tm\\_utc\\_t](#) \*issue\_date, [atcacert\\_tm\\_utc\\_t](#) \*expire\_date)

*Decode the issue and expire dates from the format used by the compressed certificate.*

- ATCA\_STATUS [atcacert\\_date\\_dec\\_compcert\\_ext](#) (const uint8\_t comp\_cert[72u], atcacert\_date\_format\_t expire\_date\_format, [atcacert\\_tm\\_utc\\_t](#) \*issue\_date, [atcacert\\_tm\\_utc\\_t](#) \*expire\_date)

*Decode the issue and expire dates from the format used by the compressed certificate.*

- atcacert\_date\_format\_t [atcacert\\_date\\_from\\_asn1\\_tag](#) (const uint8\_t tag)

*Convert the asn1 tag for the supported time formats into the local time format.*

- ATCA\_STATUS [atcacert\\_date\\_get\\_max\\_date](#) (atcacert\_date\_format\_t format, [atcacert\\_tm\\_utc\\_t](#) \*timestamp)

*Return the maximum date available for the given format.*

- ATCA\_STATUS [atcacert\\_date\\_enc\\_iso8601\\_sep](#) (const [atcacert\\_tm\\_utc\\_t](#) \*timestamp, uint8\_t formatted\_date[(20)])
- ATCA\_STATUS [atcacert\\_date\\_dec\\_iso8601\\_sep](#) (const uint8\_t formatted\_date[(20)], [atcacert\\_tm\\_utc\\_t](#) \*timestamp)
- ATCA\_STATUS [atcacert\\_date\\_enc\\_rfc5280\\_utc](#) (const [atcacert\\_tm\\_utc\\_t](#) \*timestamp, uint8\_t formatted\_date[(13)])
- ATCA\_STATUS [atcacert\\_date\\_dec\\_rfc5280\\_utc](#) (const uint8\_t formatted\_date[(13)], [atcacert\\_tm\\_utc\\_t](#) \*timestamp)
- ATCA\_STATUS [atcacert\\_date\\_enc\\_rfc5280\\_gen](#) (const [atcacert\\_tm\\_utc\\_t](#) \*timestamp, uint8\_t formatted\_date[(15)])
- ATCA\_STATUS [atcacert\\_date\\_dec\\_rfc5280\\_gen](#) (const uint8\_t formatted\_date[(15)], [atcacert\\_tm\\_utc\\_t](#) \*timestamp)
- ATCA\_STATUS [atcacert\\_date\\_enc\\_posix\\_be](#) (const [atcacert\\_tm\\_utc\\_t](#) \*timestamp, uint8\_t formatted\_date[(4)])
- ATCA\_STATUS [atcacert\\_date\\_dec\\_posix\\_be](#) (const uint8\_t formatted\_date[(4)], [atcacert\\_tm\\_utc\\_t](#) \*timestamp)
- ATCA\_STATUS [atcacert\\_date\\_enc\\_posix\\_le](#) (const [atcacert\\_tm\\_utc\\_t](#) \*timestamp, uint8\_t formatted\_date[(4)])
- ATCA\_STATUS [atcacert\\_date\\_dec\\_posix\\_le](#) (const uint8\_t formatted\_date[(4)], [atcacert\\_tm\\_utc\\_t](#) \*timestamp)
- int [atcacert\\_date\\_cmp](#) (const [atcacert\\_tm\\_utc\\_t](#) \*timestamp1, const [atcacert\\_tm\\_utc\\_t](#) \*timestamp2)

*Compare two dates.*

## Variables

- const size\_t [ATCACERT\\_DATE\\_FORMAT\\_SIZES](#) [5]

### 22.59.1 Detailed Description

Declarations for date handling with regard to certificates.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.60 atcacert\_def.c File Reference

Main certificate definition implementation.

```
#include "atcacert_def.h"
#include "crypto/atca_crypto_sw.h"
#include "crypto/atca_crypto_sw_sha1.h"
#include "crypto/atca_crypto_sw_sha2.h"
#include "atcacert_der.h"
#include "atcacert_date.h"
#include <string.h>
#include "atca_helpers.h"
#include "cal_buffer.h"
```

## Functions

- ATCA\_STATUS [atcacert\\_get\\_subject](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, [cal\\_buffer](#) \*cert\_subj\_buf)  
*Gets the subject name from a certificate.*
- ATCA\_STATUS [atcacert\\_get\\_subj\\_public\\_key](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, uint8\_t subj\_public\_key[64])  
*Gets the subject public key from a certificate.*
- ATCA\_STATUS [atcacert\\_get\\_subj\\_key\\_id](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, uint8\_t subj\_key\_id[20])  
*Gets the subject key ID from a certificate.*
- ATCA\_STATUS [atcacert\\_get\\_issuer](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, uint8\_t cert\_issuer[128])  
*Gets the issuer name of a certificate.*
- ATCA\_STATUS [atcacert\\_get\\_issue\\_date](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, [atcacert\\_tm\\_utc\\_t](#) \*timestamp)  
*Gets the issue date from a certificate. Will be parsed according to the date format specified in the certificate definition.*
- ATCA\_STATUS [atcacert\\_get\\_expire\\_date](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, [atcacert\\_tm\\_utc\\_t](#) \*timestamp)  
*Gets the expire date from a certificate. Will be parsed according to the date format specified in the certificate definition.*
- ATCA\_STATUS [atcacert\\_get\\_cert\\_sn](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, uint8\_t \*cert\_sn, size\_t \*cert\_sn\_size)  
*Gets the certificate serial number from a certificate.*
- ATCA\_STATUS [atcacert\\_get\\_auth\\_key\\_id](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, uint8\_t auth\_key\_id[20])  
*Gets the authority key ID from a certificate.*
- int [atcacert\\_calc\\_expire\\_years](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, int issue\_tm\_year, uint8\_t \*expire\_years)

### 22.60.1 Detailed Description

Main certificate definition implementation.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.61 atcacert\_def.h File Reference

Declarations for certificates related to ECC CryptoAuthentication devices. These are the definitions required to define a certificate and its various elements with regards to the CryptoAuthentication ECC devices.

```
#include <stddef.h>
#include <stdint.h>
#include "atca_compiler.h"
#include "atcacert.h"
#include "atcacert_date.h"
#include "atca_helpers.h"
#include "crypto/atca_crypto_sw.h"
#include "cal_buffer.h"
```

## Data Structures

- struct [atcacert\\_device\\_loc\\_s](#)
- struct [atcacert\\_cert\\_loc\\_s](#)
- struct [atcacert\\_cert\\_element\\_s](#)
- struct [atcacert\\_def\\_s](#)
- struct [atcacert\\_build\\_state\\_s](#)

## Macros

- #define **ATCA\_MAX\_TRANSFORMS** 2
- #define **CA\_DEV\_SN\_SIZE** 9u
- #define **CA2\_DEV\_SN\_SIZE\_PART\_1** 4u
- #define **CA2\_DEV\_SN\_SIZE\_PART\_2** 5u
- #define **CA\_DEV\_SN\_CONFIG\_ZONE\_OFFSET** 0u
- #define **CA2\_DEV\_SN\_CONFIG\_ZONE\_OFFSET\_PART\_1** 0u
- #define **CA2\_DEV\_SN\_CONFIG\_ZONE\_OFFSET\_PART\_2** 8u

## Typedefs

- typedef enum [atcacert\\_cert\\_type\\_e](#) [atcacert\\_cert\\_type\\_t](#)
- typedef enum [atcacert\\_cert\\_sn\\_src\\_e](#) [atcacert\\_cert\\_sn\\_src\\_t](#)
- typedef enum [atcacert\\_device\\_zone\\_e](#) [atcacert\\_device\\_zone\\_t](#)
- typedef enum [atcacert\\_transform\\_e](#) [atcacert\\_transform\\_t](#)  
*How to transform the data from the device to the certificate.*
- typedef enum [atcacert\\_std\\_cert\\_element\\_e](#) [atcacert\\_std\\_cert\\_element\\_t](#)
- typedef struct ATCA\_PACKED [atcacert\\_device\\_loc\\_s](#) [atcacert\\_device\\_loc\\_t](#)
- typedef struct ATCA\_PACKED [atcacert\\_cert\\_loc\\_s](#) [atcacert\\_cert\\_loc\\_t](#)
- typedef struct ATCA\_PACKED [atcacert\\_cert\\_element\\_s](#) [atcacert\\_cert\\_element\\_t](#)
- typedef struct [atcacert\\_def\\_s](#) [atcacert\\_def\\_t](#)
- typedef struct [atcacert\\_build\\_state\\_s](#) [atcacert\\_build\\_state\\_t](#)

## Enumerations

- enum [atcacert\\_cert\\_type\\_e](#) { CERTTYPE\_X509 , CERTTYPE\_CUSTOM , CERTTYPE\_X509\_FULL\_STORED }
- enum [atcacert\\_cert\\_sn\\_src\\_e](#) {  
**SNSRC\_STORED** = 0x0 , **SNSRC\_STORED\_DYNAMIC** = 0x7 , **SNSRC\_DEVICE\_SN** = 0x8 ,  
**SNSRC\_SIGNER\_ID** = 0x9 ,  
**SNSRC\_PUB\_KEY\_HASH** = 0xA , **SNSRC\_DEVICE\_SN\_HASH** = 0xB , **SNSRC\_PUB\_KEY\_HASH\_POS**  
= 0xC , **SNSRC\_DEVICE\_SN\_HASH\_POS** = 0xD ,  
**SNSRC\_PUB\_KEY\_HASH\_RAW** = 0xE , **SNSRC\_DEVICE\_SN\_HASH\_RAW** = 0xF }
- enum [atcacert\\_device\\_zone\\_e](#) {  
**DEVZONE\_CONFIG** = 0x00 , **DEVZONE\_OTP** = 0x01 , **DEVZONE\_DATA** = 0x02 , **DEVZONE\_GENKEY** =  
0x03 ,  
**DEVZONE\_NONE** = 0x07 }
- enum [atcacert\\_transform\\_e](#) {  
**TF\_NONE** , **TF\_REVERSE** , **TF\_BIN2HEX\_UC** , **TF\_BIN2HEX\_LC** ,  
**TF\_HEX2BIN\_UC** , **TF\_HEX2BIN\_LC** , **TF\_BIN2HEX\_SPACE\_UC** , **TF\_BIN2HEX\_SPACE\_LC** ,  
**TF\_HEX2BIN\_SPACE\_UC** , **TF\_HEX2BIN\_SPACE\_LC** }
- enum [atcacert\\_std\\_cert\\_element\\_e](#) {  
**STDCERT\_PUBLIC\_KEY** , **STDCERT\_SIGNATURE** , **STDCERT\_ISSUE\_DATE** , **STDCERT\_EXPIRE\_↵**  
**DATE** ,  
**STDCERT\_SIGNER\_ID** , **STDCERT\_CERT\_SN** , **STDCERT\_AUTH\_KEY\_ID** , **STDCERT\_SUBJ\_KEY\_ID** ,  
**STDCERT\_NUM\_ELEMENTS** }

## Functions

- ATCA\_STATUS [atcacert\\_get\\_subject](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, [cal\\_buffer](#) \*cert\_subj\_buf)  
*Gets the subject name from a certificate.*
- ATCA\_STATUS [atcacert\\_get\\_subj\\_public\\_key](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, uint8\_t subj\_public\_key[64])  
*Gets the subject public key from a certificate.*
- ATCA\_STATUS [atcacert\\_get\\_subj\\_key\\_id](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, uint8\_t subj\_key\_id[20])  
*Gets the subject key ID from a certificate.*
- ATCA\_STATUS [atcacert\\_get\\_issuer](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, uint8\_t cert\_issuer[128])  
*Gets the issuer name of a certificate.*
- ATCA\_STATUS [atcacert\\_get\\_issue\\_date](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, [atcacert\\_tm\\_utc\\_t](#) \*timestamp)  
*Gets the issue date from a certificate. Will be parsed according to the date format specified in the certificate definition.*
- ATCA\_STATUS [atcacert\\_get\\_expire\\_date](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, [atcacert\\_tm\\_utc\\_t](#) \*timestamp)  
*Gets the expire date from a certificate. Will be parsed according to the date format specified in the certificate definition.*
- ATCA\_STATUS [atcacert\\_get\\_cert\\_sn](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, uint8\_t \*cert\_sn, size\_t \*cert\_sn\_size)  
*Gets the certificate serial number from a certificate.*
- ATCA\_STATUS [atcacert\\_get\\_auth\\_key\\_id](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, uint8\_t auth\_key\_id[20])  
*Gets the authority key ID from a certificate.*
- int [atcacert\\_calc\\_expire\\_years](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, int issue\_tm\_year, uint8\_t \*expire\_years)

### 22.61.1 Detailed Description

Declarations for certificates related to ECC CryptoAuthentication devices. These are the definitions required to define a certificate and its various elements with regards to the CryptoAuthentication ECC devices.

Only the dynamic elements of a certificate (the parts of the certificate that change from device to device) are stored on the ATECC device. The definitions here describe the form of the certificate, and where the dynamic elements can be found both on the ATECC device itself and in the certificate template.

This also defines utility functions for working with the certificates and their definitions.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.62 atcacert\_der.c File Reference

functions required to work with DER encoded data related to X.509 certificates.

```
#include "cryptoauthlib.h"
#include "atcacert_der.h"
#include <string.h>
```

## 22.62.1 Detailed Description

functions required to work with DER encoded data related to X.509 certificates.

### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.63 atcacert\_der.h File Reference

function declarations required to work with DER encoded data related to X.509 certificates.

```
#include <stddef.h>
#include <stdint.h>
#include "atcacert.h"
```

### Functions

- ATCA\_STATUS [atcacert\\_der\\_enc\\_length](#) (size\_t length, uint8\_t \*der\_length, size\_t \*der\_length\_size)  
*Encode a length in DER format.*
- ATCA\_STATUS [atcacert\\_der\\_dec\\_length](#) (const uint8\_t \*der\_length, size\_t \*der\_length\_size, size\_t \*length)  
*Decode a DER format length.*
- ATCA\_STATUS [atcacert\\_der\\_adjust\\_length](#) (uint8\_t \*der\_length, size\_t \*der\_length\_size, int delta\_length, size\_t \*new\_length)
- ATCA\_STATUS [atcacert\\_der\\_enc\\_integer](#) (const uint8\_t \*int\_data, size\_t int\_data\_size, uint8\_t is\_unsigned, uint8\_t \*der\_int, size\_t \*der\_int\_size)  
*Encode an ASN.1 integer in DER format, including tag and length fields.*
- ATCA\_STATUS [atcacert\\_der\\_dec\\_integer](#) (const uint8\_t \*der\_int, size\_t \*der\_int\_size, uint8\_t \*int\_data, size\_t \*int\_data\_size)  
*Decode an ASN.1 DER encoded integer.*
- ATCA\_STATUS [atcacert\\_der\\_enc\\_ecdsa\\_sig\\_value](#) (const uint8\_t raw\_sig[64], uint8\_t \*der\_sig, size\_t \*der\_sig\_size)  
*Formats a raw ECDSA P256 signature in the DER encoding found in X.509 certificates.*
- ATCA\_STATUS [atcacert\\_der\\_dec\\_ecdsa\\_sig\\_value](#) (const uint8\_t \*der\_sig, size\_t \*der\_sig\_size, uint8\_t raw\_sig[64])  
*Parses an ECDSA P256 signature in the DER encoding as found in X.509 certificates.*

## 22.63.1 Detailed Description

function declarations required to work with DER encoded data related to X.509 certificates.

### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.64 atcacert\_host\_hw.c File Reference

host side methods using CryptoAuth hardware

```
#include "atcacert_host_hw.h"
#include "atca_basic.h"
#include "crypto/atca_crypto_sw_sha2.h"
```

### 22.64.1 Detailed Description

host side methods using CryptoAuth hardware

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.65 atcacert\_host\_hw.h File Reference

host side methods using CryptoAuth hardware

```
#include <stddef.h>
#include <stdint.h>
#include "atcacert_def.h"
```

### Functions

- ATCA\_STATUS [atcacert\\_verify\\_cert\\_hw](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, const uint8\_t ca\_public\_key[64])  
*Verify a certificate against its certificate authority's public key using the host's ATECC device for crypto functions.*
- ATCA\_STATUS [atcacert\\_gen\\_challenge\\_hw](#) (uint8\_t challenge[32])  
*Generate a random challenge to be sent to the client using the RNG on the host's ATECC device.*
- ATCA\_STATUS [atcacert\\_verify\\_response\\_hw](#) (const uint8\_t device\_public\_key[64], const uint8\_t challenge[32], const uint8\_t response[64])  
*Verify a client's response to a challenge using the host's ATECC device for crypto functions.*

### 22.65.1 Detailed Description

host side methods using CryptoAuth hardware

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.



## 22.66 atcacert\_host\_sw.c File Reference

host side methods using software implementations

```
#include "atcacert_host_sw.h"
#include "crypto/atca_crypto_sw.h"
#include "cal_internal.h"
```

### 22.66.1 Detailed Description

host side methods using software implementations

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.67 atcacert\_host\_sw.h File Reference

Host side methods using software implementations. host-side, the one authenticating a client, of the authentication process. Crypto functions are performed using a software library.

```
#include <stddef.h>
#include <stdint.h>
#include "atcacert_def.h"
```

### Functions

- ATCA\_STATUS [atcacert\\_verify\\_cert\\_sw](#) (const [atcacert\\_def\\_t](#) \*cert\_def, const uint8\_t \*cert, size\_t cert\_size, const uint8\_t ca\_public\_key[64])  
*Verify a certificate against its certificate authority's public key using software crypto functions. The function is currently not implemented.*
- ATCA\_STATUS [atcacert\\_gen\\_challenge\\_sw](#) (uint8\_t challenge[32])  
*Generate a random challenge to be sent to the client using a software PRNG. The function is currently not implemented.*
- ATCA\_STATUS [atcacert\\_verify\\_response\\_sw](#) (const uint8\_t device\_public\_key[64], const uint8\_t challenge[32], const uint8\_t response[64])  
*Verify a client's response to a challenge using software crypto functions. The function is currently not implemented.*

### 22.67.1 Detailed Description

Host side methods using software implementations. host-side, the one authenticating a client, of the authentication process. Crypto functions are performed using a software library.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.68 atcacert\_pem.c File Reference

Functions required to work with PEM encoded data related to X.509 certificates.

```
#include <string.h>
#include "atcacert.h"
#include "atcacert_pem.h"
#include "atca_helpers.h"
```

### 22.68.1 Detailed Description

Functions required to work with PEM encoded data related to X.509 certificates.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.69 atcacert\_pem.h File Reference

Functions for converting between DER and PEM formats.

```
#include <stdint.h>
```

### Macros

- `#define PEM_CERT_BEGIN "-----BEGIN CERTIFICATE-----"`
- `#define PEM_CERT_END "-----END CERTIFICATE-----"`
- `#define PEM_CSR_BEGIN "-----BEGIN CERTIFICATE REQUEST-----"`
- `#define PEM_CSR_END "-----END CERTIFICATE REQUEST-----"`

### Functions

- ATCA\_STATUS [atcacert\\_encode\\_pem](#) (const uint8\_t \*der, size\_t der\_size, char \*pem, size\_t \*pem\_size, const char \*header, const char \*footer)  
*Encode a DER data in PEM format.*
- ATCA\_STATUS [atcacert\\_decode\\_pem](#) (const char \*pem, size\_t pem\_size, uint8\_t \*der, size\_t \*der\_size, const char \*header, const char \*footer)  
*Decode PEM data into DER format.*
- ATCA\_STATUS [atcacert\\_encode\\_pem\\_cert](#) (const uint8\_t \*der\_cert, size\_t der\_cert\_size, char \*pem\_cert, size\_t \*pem\_cert\_size)  
*Encode a DER certificate in PEM format.*
- ATCA\_STATUS [atcacert\\_decode\\_pem\\_cert](#) (const char \*pem\_cert, size\_t pem\_cert\_size, uint8\_t \*der\_cert, size\_t \*der\_cert\_size)  
*Decode a PEM certificate into DER format.*
- ATCA\_STATUS [atcacert\\_encode\\_pem\\_csr](#) (const uint8\_t \*der\_csr, size\_t der\_csr\_size, char \*pem\_csr, size\_t \*pem\_csr\_size)  
*Encode a DER CSR in PEM format.*
- ATCA\_STATUS [atcacert\\_decode\\_pem\\_csr](#) (const char \*pem\_csr, size\_t pem\_csr\_size, uint8\_t \*der\_csr, size\_t \*der\_csr\_size)  
*Extract the CSR certificate bytes from a PEM encoded CSR certificate.*

### 22.69.1 Detailed Description

Functions for converting between DER and PEM formats.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.69.2 Function Documentation

#### 22.69.2.1 atcacert\_decode\_pem()

```
ATCA_STATUS atcacert_decode_pem (
    const char * pem,
    size_t pem_size,
    uint8_t * der,
    size_t * der_size,
    const char * header,
    const char * footer )
```

Decode PEM data into DER format.

#### Parameters

in	<i>pem</i>	PEM data to decode to DER.
in	<i>pem_size</i>	PEM data size in bytes.
out	<i>der</i>	DER data is returned here.
in, out	<i>der_size</i>	As input, the size of the der buffer. As output, the size of the DER data.
in	<i>header</i>	Header to find the beginning of the PEM data.
in	<i>footer</i>	Footer to find the end of the PEM data.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 22.69.2.2 atcacert\_decode\_pem\_cert()

```
ATCA_STATUS atcacert_decode_pem_cert (
    const char * pem_cert,
    size_t pem_cert_size,
    uint8_t * der_cert,
    size_t * der_cert_size )
```

Decode a PEM certificate into DER format.

### Parameters

in	<i>pem_cert</i>	PEM certificate to decode to DER.
in	<i>pem_cert_size</i>	PEM certificate size in bytes.
out	<i>der_cert</i>	DER certificate is returned here.
in, out	<i>der_cert_size</i>	As input, the size of the der_cert buffer. As output, the size of the DER certificate.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 22.69.2.3 atcacert\_decode\_pem\_csr()

```
ATCA_STATUS atcacert_decode_pem_csr (
    const char * pem_csr,
    size_t pem_csr_size,
    uint8_t * der_csr,
    size_t * der_csr_size )
```

Extract the CSR certificate bytes from a PEM encoded CSR certificate.

### Parameters

in	<i>pem_csr</i>	PEM CSR to decode to DER.
in	<i>pem_csr_size</i>	PEM CSR size in bytes.
out	<i>der_csr</i>	DER CSR is returned here.
in, out	<i>der_csr_size</i>	As input, the size of the der_csr buffer. As output, the size of the DER CSR.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 22.69.2.4 atcacert\_encode\_pem()

```
ATCA_STATUS atcacert_encode_pem (
    const uint8_t * der,
    size_t der_size,
    char * pem,
    size_t * pem_size,
    const char * header,
    const char * footer )
```

Encode a DER data in PEM format.

**Parameters**

in	<i>der</i>	DER data to be encoded as PEM.
out	<i>der_size</i>	DER data size in bytes.
out	<i>pem</i>	PEM encoded data is returned here.
in, out	<i>pem_size</i>	As input, the size of the pem buffer. As output, the size of the PEM data.
in	<i>header</i>	Header to place at the beginning of the PEM data.
in	<i>footer</i>	Footer to place at the end of the PEM data.

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

**22.69.2.5 atcacert\_encode\_pem\_cert()**

```
ATCA_STATUS atcacert_encode_pem_cert (
    const uint8_t * der_cert,
    size_t der_cert_size,
    char * pem_cert,
    size_t * pem_cert_size )
```

Encode a DER certificate in PEM format.

**Parameters**

in	<i>der_cert</i>	DER certificate to be encoded as PEM.
out	<i>der_cert_size</i>	DER certificate size in bytes.
out	<i>pem_cert</i>	PEM encoded certificate is returned here.
in, out	<i>pem_cert_size</i>	As input, the size of the pem_cert buffer. As output, the size of the PEM certificate.

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

**22.69.2.6 atcacert\_encode\_pem\_csr()**

```
ATCA_STATUS atcacert_encode_pem_csr (
    const uint8_t * der_csr,
    size_t der_csr_size,
    char * pem_csr,
    size_t * pem_csr_size )
```

Encode a DER CSR in PEM format.

## Parameters

in	der_csr	DER CSR to be encoded as PEM.
out	der_csr_size	DER CSR size in bytes.
out	pem_csr	PEM encoded CSR is returned here.
in, out	pem_csr_size	As input, the size of the pem_csr buffer. As output, the size of the PEM CSR.

## Returns

ATCA\_SUCCESS on success, otherwise an error code.

## 22.70 cal\_buffer.c File Reference

Cryptoauthlib buffer management system.

```
#include <string.h>
#include "cal_buffer.h"
```

### Functions

- ATCA\_STATUS [cal\\_buf\\_read\\_bytes](#) ([cal\\_buffer](#) \*cab, size\_t offset, void \*dest, size\_t length)  
*Read bytes from a cal\_buffer or cal\_buffer linked list.*
- ATCA\_STATUS [cal\\_buf\\_read\\_byte](#) ([cal\\_buffer](#) \*cab, size\_t offset, uint8\_t \*value)
- ATCA\_STATUS [cal\\_buf\\_write\\_byte](#) ([cal\\_buffer](#) \*cab, size\_t offset, uint8\_t value)
- ATCA\_STATUS [cal\\_buf\\_write\\_bytes](#) ([cal\\_buffer](#) \*cab, size\_t offset, const void \*source, size\_t length)  
*Write bytes into a single cal\_buffer structure or cal\_buffer linked list.*
- ATCA\_STATUS [cal\\_buf\\_read\\_number](#) ([cal\\_buffer](#) \*cab, size\_t offset, void \*dest, size\_t num\_size, bool buf↔\_big\_endian)  
*Read a number from a cal\_buffer or cal\_buffer linked list This function does not reinterpret the number and signedness is only preserved if the destination is the same size as the representation in the buffer.*
- ATCA\_STATUS [cal\\_buf\\_write\\_number](#) ([cal\\_buffer](#) \*cab, size\_t offset, const void \*source, size\_t num\_size, bool buf\_big\_endian)  
*Write a number into a cal\_buffer or cal\_buffer linked list This function does not reinterpret the number and signedness is only preserved if the destination is the same size as the source.*
- ATCA\_STATUS [cal\\_buf\\_set\\_used](#) ([cal\\_buffer](#) \*buf, size\_t used)
- size\_t [cal\\_buf\\_get\\_used](#) ([cal\\_buffer](#) \*buf)
- ATCA\_STATUS [cal\\_buf\\_copy](#) ([cal\\_buffer](#) \*dst, size\_t dst\_offset, [cal\\_buffer](#) \*src, size\_t src\_offset, size\_t length)
- ATCA\_STATUS [cal\\_buf\\_set](#) ([cal\\_buffer](#) \*dst, size\_t dst\_offset, uint8\_t value, size\_t length)
- [cal\\_buffer](#) [cal\\_buf\\_init\\_const\\_ptr](#) (size\_t len, const uint8\_t \*message)  
*Initialize a cal buffer with constant pointer Returns the initialized cal buffer.*

### 22.70.1 Detailed Description

Cryptoauthlib buffer management system.

#### Copyright

(c) 2023 Microchip Technology Inc. and its subsidiaries.

## 22.70.2 Function Documentation

### 22.70.2.1 cal\_buf\_read\_bytes()

```
ATCA_STATUS cal_buf_read_bytes (
    cal_buffer * cab,
    size_t offset,
    void * dest,
    size_t length )
```

Read bytes from a cal\_buffer or cal\_buffer linked list.

#### Parameters

in	<i>cab</i>	Pointer to a buffer structure or the head of a buffer structure linked list
in	<i>offset</i>	Offset to start the read from
in	<i>dest</i>	Pointer to a destination buffer
in	<i>length</i>	Length of the read - assumes dest has sufficient memory to accept the bytes being read

### 22.70.2.2 cal\_buf\_read\_number()

```
ATCA_STATUS cal_buf_read_number (
    cal_buffer * cab,
    size_t offset,
    void * dest,
    size_t num_size,
    bool buf_big_endian )
```

Read a number from a cal\_buffer or cal\_buffer linked list This function does not reinterpret the number and signedness is only preserved if the destination is the same size as the representation in the buffer.

#### Parameters

in	<i>cab</i>	Pointer to a buffer structure or the head of a buffer structure linked list
in	<i>offset</i>	Offset to start the read from
in	<i>dest</i>	Pointer to a destination number
in	<i>num_size</i>	Size of the number in bytes
in	<i>buf_big_endian</i>	Specifies the expected endianness representation within the buffer

### 22.70.2.3 cal\_buf\_write\_bytes()

```
ATCA_STATUS cal_buf_write_bytes (
    cal_buffer * cab,
```

```
size_t offset,
const void * source,
size_t length )
```

Write bytes into a single cal\_buffer structure or cal\_buffer linked list.

Parameters

in	<i>cab</i>	Pointer to a buffer structure or the head of a buffer structure linked list
in	<i>offset</i>	Target offset to start the write at
in	<i>source</i>	Pointer to a source buffer
in	<i>length</i>	Length of the write - assumes source is sufficiently large to support this operation

22.70.2.4 cal\_buf\_write\_number()

```
ATCA_STATUS cal_buf_write_number (
    cal_buffer * cab,
    size_t offset,
    const void * source,
    size_t num_size,
    bool buf_big_endian )
```

Write a number into a cal\_buffer or cal\_buffer linked list This function does not reinterpret the number and signedness is only preserved if the destination is the same size as the source.

Parameters

in	<i>cab</i>	Pointer to a buffer structure or the head of a buffer structure linked list
in	<i>offset</i>	Offset to start the write at
in	<i>source</i>	Pointer to a number to be written
in	<i>num_size</i>	Size of the number in bytes
in	<i>buf_big_endian</i>	Specifies the expected endianness representation within the buffer

22.71 cal\_buffer.h File Reference

Cryptoauthlib buffer management system.

```
#include <stdint.h>
#include <stdlib.h>
#include <stdbool.h>
#include "atca_config_check.h"
#include "atca_status.h"
```

Data Structures

- struct [cal\\_buffer\\_s](#)



- `#define CAL_BUF_INIT(s, b) { (size_t)(s), (uint8_t*)(b) }`
- `typedef struct cal_buffer_s cal_buffer`
- `ATCA_STATUS cal_buf_read_byte (cal_buffer *cab, size_t offset, uint8_t *value)`
- `ATCA_STATUS cal_buf_write_byte (cal_buffer *cab, size_t offset, uint8_t value)`
- `ATCA_STATUS cal_buf_read_bytes (cal_buffer *cab, size_t offset, void *dest, size_t length)`  
*Read bytes from a cal\_buffer or cal\_buffer linked list.*
- `ATCA_STATUS cal_buf_write_bytes (cal_buffer *cab, size_t offset, const void *source, size_t length)`  
*Write bytes into a single cal\_buffer structure or cal\_buffer linked list.*
- `ATCA_STATUS cal_buf_read_number (cal_buffer *cab, size_t offset, void *dest, size_t num_size, bool buf↔_big_endian)`  
*Read a number from a cal\_buffer or cal\_buffer linked list This function does not reinterpret the number and signedness is only preserved if the destination is the same size as the representation in the buffer.*
- `ATCA_STATUS cal_buf_write_number (cal_buffer *cab, size_t offset, const void *source, size_t num_size, bool buf_big_endian)`  
*Write a number into a cal\_buffer or cal\_buffer linked list This function does not reinterpret the number and signedness is only preserved if the destination is the same size as the source.*
- `ATCA_STATUS cal_buf_copy (cal_buffer *dst, size_t dst_offset, cal_buffer *src, size_t src_offset, size_t length)`
- `ATCA_STATUS cal_buf_set (cal_buffer *dst, size_t dst_offset, uint8_t value, size_t length)`
- `ATCA_STATUS cal_buf_set_used (cal_buffer *buf, size_t used)`
- `size_t cal_buf_get_used (cal_buffer *buf)`
- `cal_buffer cal_buf_init_const_ptr (size_t len, const uint8_t *message)`  
*Initialize a cal buffer with constant pointer Returns the initialized cal buffer.*

## 22.71.1 Detailed Description

Cryptoauthlib buffer management system.

### Copyright

(c) 2023 Microchip Technology Inc. and its subsidiaries.

## 22.71.2 Function Documentation

### 22.71.2.1 cal\_buf\_read\_bytes()

```
ATCA_STATUS cal_buf_read_bytes (
    cal_buffer * cab,
    size_t offset,
    void * dest,
    size_t length )
```

Read bytes from a cal\_buffer or cal\_buffer linked list.

#### Parameters

in	<i>cab</i>	Pointer to a buffer structure or the head of a buffer structure linked list
in	<i>offset</i>	Offset to start the read from
in	<i>dest</i>	Pointer to a destination buffer
in	<i>length</i>	Length of the read - assumes dest has sufficient memory to accept the bytes being read

### 22.71.2.2 cal\_buf\_read\_number()

```
ATCA_STATUS cal_buf_read_number (
    cal_buffer * cab,
    size_t offset,
    void * dest,
    size_t num_size,
    bool buf_big_endian )
```

Read a number from a cal\_buffer or cal\_buffer linked list. This function does not reinterpret the number and signedness is only preserved if the destination is the same size as the representation in the buffer.

#### Parameters

in	<i>cab</i>	Pointer to a buffer structure or the head of a buffer structure linked list
in	<i>offset</i>	Offset to start the read from
in	<i>dest</i>	Pointer to a destination number
in	<i>num_size</i>	Size of the number in bytes
in	<i>buf_big_endian</i>	Specifies the expected endianness representation within the buffer

### 22.71.2.3 cal\_buf\_write\_bytes()

```
ATCA_STATUS cal_buf_write_bytes (
    cal_buffer * cab,
    size_t offset,
    const void * source,
    size_t length )
```

Write bytes into a single cal\_buffer structure or cal\_buffer linked list.

#### Parameters

in	<i>cab</i>	Pointer to a buffer structure or the head of a buffer structure linked list
in	<i>offset</i>	Target offset to start the write at
in	<i>source</i>	Pointer to a source buffer
in	<i>length</i>	Length of the write - assumes source is sufficiently large to support this operation

### 22.71.2.4 cal\_buf\_write\_number()

```
ATCA_STATUS cal_buf_write_number (
    cal_buffer * cab,
    size_t offset,
    const void * source,
```

```

size_t num_size,
bool buf_big_endian )

```

Write a number into a cal\_buffer or cal\_buffer linked list This function does not reinterpret the number and signedness is only preserved if the destination is the same size as the source.

Parameters

in	<i>cab</i>	Pointer to a buffer structure or the head of a buffer structure linked list
in	<i>offset</i>	Offset to start the write at
in	<i>source</i>	Pointer to a number to be written
in	<i>num_size</i>	Size of the number in bytes
in	<i>buf_big_endian</i>	Specifies the expected endianness representation within the buffer

### 22.72 cal\_internal.h File Reference

Internal CryptoAuthLib Interfaces.

```

#include "atca_config_check.h"
#include "crypto/atca_crypto_sw.h"
#include "mbedtls/atca_mbedtls_wrap.h"

```

#### 22.72.1 Detailed Description

Internal CryptoAuthLib Interfaces.

Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.73 calib\_aes.c File Reference

CryptoAuthLib Basic API methods for AES command.

```

#include "cryptoauthlib.h"

```

#### 22.73.1 Detailed Description

CryptoAuthLib Basic API methods for AES command.

The AES command supports 128-bit AES encryption or decryption of small messages or data packets in ECB mode. Also can perform GFM (Galois Field Multiply) calculation in support of AES-GCM.

Note

List of devices that support this command - ATECC608A/B. Refer to device edatasheet for full details.

Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.74 calib\_aes\_gcm.c File Reference

CryptoAuthLib Basic API methods for AES GCM mode.

```
#include "cryptoauthlib.h"
```

### 22.74.1 Detailed Description

CryptoAuthLib Basic API methods for AES GCM mode.

The AES command supports 128-bit AES encryption or decryption of small messages or data packets in ECB mode. Also can perform GFM (Galois Field Multiply) calculation in support of AES-GCM.

#### Note

List of devices that support this command - ATECC608A/B. Refer to device datasheet for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.75 calib\_aes\_gcm.h File Reference

Unity tests for the cryptoauthlib AES GCM functions.

```
#include "calib_config_check.h"
```

### 22.75.1 Detailed Description

Unity tests for the cryptoauthlib AES GCM functions.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.76 calib\_basic.c File Reference

CryptoAuthLib Basic API methods. These methods provide a simpler way to access the core crypto methods.

```
#include "cryptoauthlib.h"
```

## Functions

- ATCA\_STATUS [calib\\_wakeup\\_i2c](#) (ATCADevice device)  
*basic API methods are all prefixed with atcab\_ (CryptoAuthLib Basic) the fundamental premise of the basic API is it is based on a single interface instance and that instance is global, so all basic API commands assume that one global device is the one to operate on.*
- ATCA\_STATUS [calib\\_wakeup](#) (ATCADevice device)  
*wakeup the CryptoAuth device*
- ATCA\_STATUS [calib\\_idle](#) (ATCADevice device)  
*idle the CryptoAuth device*
- ATCA\_STATUS [calib\\_sleep](#) (ATCADevice device)  
*invoke sleep on the CryptoAuth device*
- ATCA\_STATUS [calib\\_exit](#) (ATCADevice device)  
*common cleanup code which idles the device after any operation*
- ATCA\_STATUS [calib\\_get\\_addr](#) (uint8\_t zone, uint16\_t slot, uint8\_t block, uint8\_t offset, uint16\_t \*addr)  
*Compute the address given the zone, slot, block, and offset.*
- ATCA\_STATUS [calib\\_ca2\\_get\\_addr](#) (uint8\_t zone, uint16\_t slot, uint8\_t block, uint8\_t offset, uint16\_t \*addr)  
*Compute the address given the zone, slot, block, and offset for the device.*
- ATCA\_STATUS [calib\\_get\\_zone\\_size](#) (ATCADevice device, uint8\_t zone, uint16\_t slot, size\_t \*size)  
*Gets the size of the specified zone in bytes.*

### 22.76.1 Detailed Description

CryptoAuthLib Basic API methods. These methods provide a simpler way to access the core crypto methods.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.77 calib\_checkmac.c File Reference

CryptoAuthLib Basic API methods for CheckMAC command.

```
#include "cryptoauthlib.h"
```

### 22.77.1 Detailed Description

CryptoAuthLib Basic API methods for CheckMAC command.

The CheckMac command calculates a MAC response that would have been generated on a different CryptoAuth Authentication device and then compares the result with input value.

#### Note

List of devices that support this command - ATSHA204A, ATECC108A, ATECC508A, and ATECC608A/B. There are differences in the modes that they support. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.78 calib\_command.c File Reference

Microchip CryptoAuthentication device command builder - this is the main object that builds the command byte strings for the given device. It does not execute the command. The basic flow is to call a command method to build the command you want given the parameters and then send that byte string through the device interface.

```
#include "cryptoauthlib.h"
```

### Functions

- ATCA\_STATUS [atInfo](#) (ATCADeviceType device\_type, [ATCAPacket](#) \*packet)  
*ATCACommand Info method.*
- ATCA\_STATUS [atPause](#) (ATCADeviceType device\_type, [ATCAPacket](#) \*packet)  
*ATCACommand Pause method.*
- void [atCRC](#) (size\_t length, const uint8\_t \*data, uint8\_t \*crc\_le)  
*Calculates CRC over the given raw data and returns the CRC in little-endian byte order.*
- void [atCalcCrc](#) ([ATCAPacket](#) \*packet)  
*This function calculates CRC and adds it to the correct offset in the packet data.*
- ATCA\_STATUS [atCheckCrc](#) (const uint8\_t \*response)  
*This function checks the consistency of a response.*
- bool [atIsSHAFamily](#) (ATCADeviceType device\_type)  
*determines if a given device type is a SHA device or a superset of a SHA device*
- bool [atIsECCFamily](#) (ATCADeviceType device\_type)  
*determines if a given device type is an ECC device or a superset of a ECC device*
- ATCA\_STATUS [isATCAError](#) (uint8\_t \*data)  
*checks for basic error frame in data*

### 22.78.1 Detailed Description

Microchip CryptoAuthentication device command builder - this is the main object that builds the command byte strings for the given device. It does not execute the command. The basic flow is to call a command method to build the command you want given the parameters and then send that byte string through the device interface.

The primary goal of the command builder is to wrap the given parameters with the correct packet size and CRC. The caller should first fill in the parameters required in the [ATCAPacket](#) parameter given to the command. The command builder will deal with the mechanics of creating a valid packet using the parameter information.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.78.2 Function Documentation

#### 22.78.2.1 atCalcCrc()

```
void atCalcCrc (  
    ATCAPacket * packet )
```

This function calculates CRC and adds it to the correct offset in the packet data.

Parameters

in	<i>packet</i>	Packet to calculate CRC data for
----	---------------	----------------------------------

22.78.2.2 atCheckCrc()

```
ATCA_STATUS atCheckCrc (
    const uint8_t * response )
```

This function checks the consistency of a response.

Parameters

in	<i>response</i>	pointer to response
----	-----------------	---------------------

Returns

ATCA\_SUCCESS on success, otherwise ATCA\_RX\_CRC\_ERROR

22.78.2.3 atCRC()

```
void atCRC (
    size_t length,
    const uint8_t * data,
    uint8_t * crc_le )
```

Calculates CRC over the given raw data and returns the CRC in little-endian byte order.

Parameters

in	<i>length</i>	Size of data not including the CRC byte positions
in	<i>data</i>	Pointer to the data over which to compute the CRC
out	<i>crc_le</i>	Pointer to the place where the two-bytes of CRC will be returned in little-endian byte order.

22.78.2.4 atInfo()

```
ATCA_STATUS atInfo (
    ATCADeviceType device_type,
    ATCAPacket * packet )
```

ATCACommand Info method.

### Parameters

in	<i>ca_cmd</i>	instance
in	<i>packet</i>	pointer to the packet containing the command being built

### Returns

ATCA\_SUCCESS

### 22.78.2.5 atIsECCFamily()

```
bool atIsECCFamily (  
    ATCADeviceType device_type )
```

determines if a given device type is an ECC device or a superset of a ECC device

#### Parameters

in	<i>device_type</i>	Type of device to check for family type
----	--------------------	---

### Returns

boolean indicating whether the given device is an ECC family device.

### 22.78.2.6 atIsSHAFamily()

```
bool atIsSHAFamily (  
    ATCADeviceType device_type )
```

determines if a given device type is a SHA device or a superset of a SHA device

#### Parameters

in	<i>device_type</i>	Type of device to check for family type
----	--------------------	---

### Returns

boolean indicating whether the given device is a SHA family device.



### 22.78.2.7 atPause()

```
ATCA_STATUS atPause (
    ATCADeviceType device_type,
    ATCAPacket * packet )
```

ATCACommand Pause method.

Parameters

in	<i>ca_cmd</i>	instance
in	<i>packet</i>	pointer to the packet containing the command being built

Returns

ATCA\_SUCCESS

### 22.78.2.8 isATCAError()

```
ATCA_STATUS isATCAError (
    uint8_t * data )
```

checks for basic error frame in data

Parameters

in	<i>data</i>	pointer to received data - expected to be in the form of a CA device response frame
----	-------------	---

Returns

ATCA\_SUCCESS on success, otherwise an error code.

## 22.79 calib\_command.h File Reference

Microchip Crypto Auth device command object - this is a command builder only, it does not send the command. The result of a command method is a fully formed packet, ready to send to the ATCAIFace object to dispatch.

```
#include <stddef.h>
#include "calib_config_check.h"
```

### Data Structures

- struct [ATCAPacket](#)

## Macros

- **#define ATCA\_CMD\_SIZE\_MIN** (7u)  
*minimum number of bytes in command (from count byte to second CRC byte)*
- **#define ATCA\_CMD\_SIZE\_MAX** ((uint8\_t)4 \* 36 + 7)  
*maximum size of command packet (Verify)*
- **#define CMD\_STATUS\_SUCCESS** ((uint8\_t)0x00)  
*status byte for success*
- **#define CMD\_STATUS\_WAKEUP** ((uint8\_t)0x11)  
*status byte after wake-up*
- **#define CMD\_STATUS\_BYTE\_PARSE** ((uint8\_t)0x03)  
*command parse error*
- **#define CMD\_STATUS\_BYTE\_ECC** ((uint8\_t)0x05)  
*command ECC error*
- **#define CMD\_STATUS\_BYTE\_EXEC** ((uint8\_t)0x0F)  
*command execution error*
- **#define CMD\_STATUS\_BYTE\_COMM** ((uint8\_t)0xFF)  
*communication error*

## Opcodes for Crypto Authentication device commands

- **#define ATCA\_CHECKMAC** ((uint8\_t)0x28)  
*CheckMac command op-code.*
- **#define ATCA\_DERIVE\_KEY** ((uint8\_t)0x1C)  
*DeriveKey command op-code.*
- **#define ATCA\_INFO** ((uint8\_t)0x30)  
*Info command op-code.*
- **#define ATCA\_GENDIG** ((uint8\_t)0x15)  
*GenDig command op-code.*
- **#define ATCA\_GENKEY** ((uint8\_t)0x40)  
*GenKey command op-code.*
- **#define ATCA\_HMAC** ((uint8\_t)0x11)  
*HMAC command op-code.*
- **#define ATCA\_LOCK** ((uint8\_t)0x17)  
*Lock command op-code.*
- **#define ATCA\_MAC** ((uint8\_t)0x08)  
*MAC command op-code.*
- **#define ATCA\_NONCE** ((uint8\_t)0x16)  
*Nonce command op-code.*
- **#define ATCA\_PAUSE** ((uint8\_t)0x01)  
*Pause command op-code.*
- **#define ATCA\_PRIVWRITE** ((uint8\_t)0x46)  
*PrivWrite command op-code.*
- **#define ATCA\_RANDOM** ((uint8\_t)0x1B)  
*Random command op-code.*
- **#define ATCA\_READ** ((uint8\_t)0x02)  
*Read command op-code.*
- **#define ATCA\_SIGN** ((uint8\_t)0x41)  
*Sign command op-code.*
- **#define ATCA\_UPDATE\_EXTRA** ((uint8\_t)0x20)  
*UpdateExtra command op-code.*
- **#define ATCA\_VERIFY** ((uint8\_t)0x45)  
*GenKey command op-code.*
- **#define ATCA\_WRITE** ((uint8\_t)0x12)  
*Write command op-code.*
- **#define ATCA\_ECDH** ((uint8\_t)0x43)

- *ECDH command op-code.*
- **#define ATCA\_COUNTER** ((uint8\_t)0x24)
- *Counter command op-code.*
- **#define ATCA\_DELETE** ((uint8\_t)0x13)
- *Delete command op-code.*
- **#define ATCA\_SHA** ((uint8\_t)0x47)
- *SHA command op-code.*
- **#define ATCA\_AES** ((uint8\_t)0x51)
- *AES command op-code.*
- **#define ATCA\_KDF** ((uint8\_t)0x56)
- *KDF command op-code.*
- **#define ATCA\_SECUREBOOT** ((uint8\_t)0x80)
- *Secure Boot command op-code.*
- **#define ATCA\_SELFTEST** ((uint8\_t)0x77)
- *Self test command op-code.*

### Definitions of Data and Packet Sizes

- **#define ATCA\_BLOCK\_SIZE** (32u)
- *size of a block*
- **#define ATCA\_WORD\_SIZE** (4u)
- *size of a word*
- **#define ATCA\_PUB\_KEY\_PAD** (4u)
- *size of the public key pad*
- **#define ATCA\_SERIAL\_NUM\_SIZE** (9u)
- *number of bytes in the device serial number*
- **#define ATCA\_RSP\_SIZE\_VAL** ((uint8\_t)7)
- *size of response packet containing four bytes of data*
- **#define ATCA\_KEY\_COUNT** (16u)
- *number of keys*
- **#define ATCA\_ECC\_CONFIG\_SIZE** (128u)
- *size of configuration zone*
- **#define ATCA\_SHA\_CONFIG\_SIZE** (88u)
- *size of configuration zone*
- **#define ATCA\_CA2\_CONFIG\_SIZE** (64u)
- *size of ECC204 configuration zone*
- **#define ATCA\_CA2\_CONFIG\_SLOT\_SIZE** (16u)
- *size of ECC204 configuration slot size*
- **#define ATCA\_OTP\_SIZE** (64u)
- *size of OTP zone*
- **#define ATCA\_DATA\_SIZE** (ATCA\_KEY\_COUNT \* ATCA\_KEY\_SIZE)
- *size of data zone*
- **#define ATCA\_AES\_GFM\_SIZE** ATCA\_BLOCK\_SIZE
- *size of GFM data*
- **#define ATCA\_CHIPMODE\_OFFSET** (19u)
- *ChipMode byte offset within the configuration zone.*
- **#define ATCA\_CHIPMODE\_I2C\_ADDRESS\_FLAG** ((uint8\_t)0x01)
- *ChipMode I2C Address in UserExtraAdd flag.*
- **#define ATCA\_CHIPMODE\_TTL\_ENABLE\_FLAG** ((uint8\_t)0x02)
- *ChipMode TTLEnable flag.*
- **#define ATCA\_CHIPMODE\_WATCHDOG\_MASK** ((uint8\_t)0x04)
- *ChipMode watchdog duration mask.*
- **#define ATCA\_CHIPMODE\_WATCHDOG\_SHORT** ((uint8\_t)0x00)
- *ChipMode short watchdog (~1.3s)*
- **#define ATCA\_CHIPMODE\_WATCHDOG\_LONG** ((uint8\_t)0x04)
- *ChipMode long watchdog (~13s)*
- **#define ATCA\_CHIPMODE\_CLOCK\_DIV\_MASK** ((uint8\_t)0xF8)
- *ChipMode clock divider mask.*

- `#define ATCA_CHIPMODE_CLOCK_DIV_M0 ((uint8_t)0x00)`  
*ChipMode clock divider M0.*
- `#define ATCA_CHIPMODE_CLOCK_DIV_M1 ((uint8_t)0x28)`  
*ChipMode clock divider M1.*
- `#define ATCA_CHIPMODE_CLOCK_DIV_M2 ((uint8_t)0x68)`  
*ChipMode clock divider M2.*
- `#define ATCA_COUNT_SIZE (1u)`  
*Number of bytes in the command packet Count.*
- `#define ATCA_CRC_SIZE (2u)`  
*Number of bytes in the command packet CRC.*
- `#define ATCA_PACKET_OVERHEAD (ATCA_COUNT_SIZE + ATCA_CRC_SIZE)`  
*Number of bytes in the command packet.*
- `#define ATCA_PUB_KEY_SIZE (64u)`  
*size of a p256 public key*
- `#define ATCA_PRIV_KEY_SIZE (32u)`  
*size of a p256 private key*
- `#define ATCA_SIG_SIZE (64u)`  
*size of a p256 signature*
- `#define ATCA_KEY_SIZE (32u)`  
*size of a symmetric SHA key*
- `#define RSA2048_KEY_SIZE (256u)`  
*size of a RSA private key*
- `#define ATCA_RSP_SIZE_MIN ((uint8_t)4)`  
*minimum number of bytes in response*
- `#define ATCA_RSP_SIZE_4 ((uint8_t)7)`  
*size of response packet containing 4 bytes data*
- `#define ATCA_RSP_SIZE_72 ((uint8_t)75)`  
*size of response packet containing 64 bytes data*
- `#define ATCA_RSP_SIZE_64 ((uint8_t)67)`  
*size of response packet containing 64 bytes data*
- `#define ATCA_RSP_SIZE_32 (35u)`  
*size of response packet containing 32 bytes data*
- `#define ATCA_RSP_SIZE_16 ((uint8_t)19)`  
*size of response packet containing 16 bytes data*
- `#define ATCA_RSP_SIZE_MAX ((uint8_t)75)`  
*maximum size of response packet (GenKey and Verify command)*
- `#define OUTNONCE_SIZE (32u)`  
*Size of the OutNonce response expected from several commands.*

#### Definitions for Command Parameter Ranges

- `#define ATCA_KEY_ID_MAX ((uint8_t)15)`  
*maximum value for key id*
- `#define ATCA_OTP_BLOCK_MAX ((uint8_t)1)`  
*maximum value for OTP block*

#### Definitions for Indexes Common to All Commands

- `#define ATCA_COUNT_IDX (0)`  
*command packet index for count*
- `#define ATCA_OPCODE_IDX (1)`  
*command packet index for op-code*
- `#define ATCA_PARAM1_IDX (2)`  
*command packet index for first parameter*
- `#define ATCA_PARAM2_IDX (3)`  
*command packet index for second parameter*
- `#define ATCA_DATA_IDX (5)`  
*command packet index for data load*

- #define **ATCA\_RSP\_DATA\_IDX** (1u)  
*buffer index of data in response*

### Definitions for Zone and Address Parameters

- #define **ATCA\_ZONE\_MASK** ((uint8\_t)0x03)  
*Zone mask.*
- #define **ATCA\_ZONE\_ENCRYPTED** ((uint8\_t)0x40)  
*Zone bit 6 set: Write is encrypted with an unlocked data zone.*
- #define **ATCA\_ZONE\_READWRITE\_32** ((uint8\_t)0x80)  
*Zone bit 7 set: Access 32 bytes, otherwise 4 bytes.*
- #define **ATCA\_ADDRESS\_MASK\_CONFIG** ((uint16\_t)0x001F)  
*Address bits 5 to 7 are 0 for Configuration zone.*
- #define **ATCA\_ADDRESS\_MASK\_OTP** ((uint16\_t)0x000F)  
*Address bits 4 to 7 are 0 for OTP zone.*
- #define **ATCA\_ADDRESS\_MASK** ((uint16\_t)0x007F)  
*Address bit 7 to 15 are always 0.*
- #define **ATCA\_TEMPKEY\_KEYID** ((uint16\_t)0xFFFF)  
*KeyID when referencing TempKey.*

### Definitions for Key types

- #define **ATCA\_B283\_KEY\_TYPE** 0  
*B283 NIST ECC key.*
- #define **ATCA\_K283\_KEY\_TYPE** 1  
*K283 NIST ECC key.*
- #define **ATCA\_P256\_KEY\_TYPE** 4  
*P256 NIST ECC key.*
- #define **ATCA\_AES\_KEY\_TYPE** 6  
*AES-128 Key.*
- #define **ATCA\_SHA\_KEY\_TYPE** 7  
*SHA key or other data.*

### Definitions for the AES Command

- #define **AES\_MODE\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*AES command index for mode.*
- #define **AES\_KEYID\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
*AES command index for key id.*
- #define **AES\_INPUT\_IDX** [ATCA\\_DATA\\_IDX](#)  
*AES command index for input data.*
- #define **AES\_COUNT** (23u)  
*AES command packet size.*
- #define **AES\_MODE\_MASK** ((uint8\_t)0xC7)  
*AES mode bits 3 to 5 are 0.*
- #define **AES\_MODE\_KEY\_BLOCK\_MASK** ((uint8\_t)0xC0)  
*AES mode mask for key block field.*
- #define **AES\_MODE\_OP\_MASK** ((uint8\_t)0x07)  
*AES mode operation mask.*
- #define **AES\_MODE\_ENCRYPT** ((uint8\_t)0x00)  
*AES mode: Encrypt.*
- #define **AES\_MODE\_DECRYPT** ((uint8\_t)0x01)  
*AES mode: Decrypt.*
- #define **AES\_MODE\_GFM** ((uint8\_t)0x03)  
*AES mode: GFM calculation.*
- #define **AES\_MODE\_KEY\_BLOCK\_POS** (6u)  
*Bit shift for key block in mode.*

- #define **AES\_DATA\_SIZE** (16u)  
*size of AES encrypt/decrypt data*
- #define **AES\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_16](#)  
*AES command response packet size.*

#### Definitions for the CheckMac Command

- #define **CHECKMAC\_MODE\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*CheckMAC command index for mode.*
- #define **CHECKMAC\_KEYID\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
*CheckMAC command index for key identifier.*
- #define **CHECKMAC\_CLIENT\_CHALLENGE\_IDX** [ATCA\\_DATA\\_IDX](#)  
*CheckMAC command index for client challenge.*
- #define **CHECKMAC\_CLIENT\_RESPONSE\_IDX** (37u)  
*CheckMAC command index for client response.*
- #define **CHECKMAC\_DATA\_IDX** (69u)  
*CheckMAC command index for other data.*
- #define **CHECKMAC\_COUNT** (84u)  
*CheckMAC command packet size.*
- #define **CHECKMAC\_MODE\_CHALLENGE** ((uint8\_t)0x00)  
*CheckMAC mode 0: first SHA block from key id.*
- #define **CHECKMAC\_MODE\_BLOCK2\_TEMPKEY** ((uint8\_t)0x01)  
*CheckMAC mode bit 0: second SHA block from TempKey.*
- #define **CHECKMAC\_MODE\_BLOCK1\_TEMPKEY** ((uint8\_t)0x02)  
*CheckMAC mode bit 1: first SHA block from TempKey.*
- #define **CHECKMAC\_MODE\_SOURCE\_FLAG\_MATCH** ((uint8\_t)0x04)  
*CheckMAC mode bit 2: match TempKey.SourceFlag.*
- #define **CHECKMAC\_MODE\_INCLUDE\_OTP\_64** ((uint8\_t)0x20)  
*CheckMAC mode bit 5: include first 64 OTP bits.*
- #define **CHECKMAC\_MODE\_MASK** ((uint8\_t)0x27)  
*CheckMAC mode bits 3, 4, 6, and 7 are 0.*
- #define **CHECKMAC\_MODE\_OUTPUT\_MAC\_RESPONSE** ((uint8\_t)0x08)  
*CheckMAC mode bit 3: Single byte boolean response + 32 bytes mac in SHA105 device.*
- #define **CHECKMAC\_CLIENT\_CHALLENGE\_SIZE** (32u)  
*CheckMAC size of client challenge.*
- #define **CHECKMAC\_CLIENT\_RESPONSE\_SIZE** (32u)  
*CheckMAC size of client response.*
- #define **CHECKMAC\_OTHER\_DATA\_SIZE** (13u)  
*CheckMAC size of "other data".*
- #define **CHECKMAC\_CLIENT\_COMMAND\_SIZE** (4u)  
*CheckMAC size of client command header size inside "other data".*
- #define **CHECKMAC\_CMD\_MATCH** (0u)  
*CheckMAC return value when there is a match.*
- #define **CHECKMAC\_CMD\_MISMATCH** (1u)  
*CheckMAC return value when there is a mismatch.*
- #define **CHECKMAC\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_MIN](#)  
*CheckMAC response packet size.*
- #define **CHECKMAC\_SINGLE\_BYTE\_BOOL\_RESP** (1u)
- #define **CHECKMAC\_SHA105\_DEFAULT\_KEYID** ((uint16\_t)0x0003)

#### Definitions for the Counter command

- #define **COUNTER\_COUNT** [ATCA\\_CMD\\_SIZE\\_MIN](#)
- #define **COUNTER\_MODE\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*Counter command index for mode.*
- #define **COUNTER\_KEYID\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
*Counter command index for key id.*
- #define **COUNTER\_MODE\_MASK** ((uint8\_t)0x01)

- Counter mode bits 1 to 7 are 0.
- #define **COUNTER\_MAX\_VALUE** ((uint32\_t)2097151)  
Counter maximum value of the counter.
- #define **COUNTER\_MODE\_READ** ((uint8\_t)0x00)  
Counter command mode for reading.
- #define **COUNTER\_MODE\_INCREMENT** ((uint8\_t)0x01)  
Counter command mode for incrementing.
- #define **COUNTER\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_4](#)  
Counter command response packet size.
- #define **COUNTER\_SIZE** [ATCA\\_RSP\\_SIZE\\_MIN](#)  
Counter size in binary.
- #define **COUNTER\_MAX\_VALUE\_CA2** ((uint16\_t)10000)  
Counter maximum value of the counter for ECC204.

#### Definitions for the Delete command

- #define **DELETE\_COUNT** (39u)
- #define **DELETE\_MODE** ((uint8\_t)0x00)
- #define **DELETE\_MAC\_SIZE** (32u)
- #define **DELETE\_NONCE\_KEY\_ID** ((uint16\_t)0x8000)

#### Definitions for the DeriveKey Command

- #define **DERIVE\_KEY\_RANDOM\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
DeriveKey command index for random bit.
- #define **DERIVE\_KEY\_TARGETKEY\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
DeriveKey command index for target slot.
- #define **DERIVE\_KEY\_MAC\_IDX** [ATCA\\_DATA\\_IDX](#)  
DeriveKey command index for optional MAC.
- #define **DERIVE\_KEY\_COUNT\_SMALL** [ATCA\\_CMD\\_SIZE\\_MIN](#)  
DeriveKey command packet size without MAC.
- #define **DERIVE\_KEY\_MODE** ((uint8\_t)0x04)  
DeriveKey command mode set to 4 as in datasheet.
- #define **DERIVE\_KEY\_COUNT\_LARGE** (39u)  
DeriveKey command packet size with MAC.
- #define **DERIVE\_KEY\_RANDOM\_FLAG** ((uint8\_t)4)  
DeriveKey 1. parameter; has to match TempKey.SourceFlag.
- #define **DERIVE\_KEY\_MAC\_SIZE** (32u)  
DeriveKey MAC size.
- #define **DERIVE\_KEY\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_MIN](#)  
DeriveKey response packet size.

#### Definitions for the ECDH Command

- #define **ECDH\_PREFIX\_MODE** ((uint8\_t)0x00)
- #define **ECDH\_COUNT** ([ATCA\\_CMD\\_SIZE\\_MIN](#) + [ATCA\\_PUB\\_KEY\\_SIZE](#))
- #define **ECDH\_MODE\_SOURCE\_MASK** ((uint8\_t)0x01)
- #define **ECDH\_MODE\_SOURCE\_EEPROM\_SLOT** ((uint8\_t)0x00)
- #define **ECDH\_MODE\_SOURCE\_TEMPKEY** ((uint8\_t)0x01)
- #define **ECDH\_MODE\_OUTPUT\_MASK** ((uint8\_t)0x02)
- #define **ECDH\_MODE\_OUTPUT\_CLEAR** ((uint8\_t)0x00)
- #define **ECDH\_MODE\_OUTPUT\_ENC** ((uint8\_t)0x02)
- #define **ECDH\_MODE\_COPY\_MASK** ((uint8\_t)0x0C)
- #define **ECDH\_MODE\_COPY\_COMPATIBLE** ((uint8\_t)0x00)
- #define **ECDH\_MODE\_COPY\_EEPROM\_SLOT** ((uint8\_t)0x04)
- #define **ECDH\_MODE\_COPY\_TEMP\_KEY** ((uint8\_t)0x08)
- #define **ECDH\_MODE\_COPY\_OUTPUT\_BUFFER** ((uint8\_t)0x0C)
- #define **ECDH\_KEY\_SIZE** [ATCA\\_BLOCK\\_SIZE](#)  
ECDH output data size.

- #define **ECDH\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_64](#)  
*ECDH command packet size.*

#### Definitions for the GenDig Command

- #define **GENDIG\_ZONE\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*GenDig command index for zone.*
- #define **GENDIG\_KEYID\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
*GenDig command index for key id.*
- #define **GENDIG\_DATA\_IDX** [ATCA\\_DATA\\_IDX](#)  
*GenDig command index for optional data.*
- #define **GENDIG\_COUNT** [ATCA\\_CMD\\_SIZE\\_MIN](#)  
*GenDig command packet size without "other data".*
- #define **GENDIG\_ZONE\_CONFIG** ((uint8\_t)0)  
*GenDig zone id config. Use KeyID to specify any of the four 256-bit blocks of the Configuration zone.*
- #define **GENDIG\_ZONE\_OTP** ((uint8\_t)1)  
*GenDig zone id OTP. Use KeyID to specify either the first or second 256-bit block of the OTP zone.*
- #define **GENDIG\_ZONE\_DATA** ((uint8\_t)2)  
*GenDig zone id data. Use KeyID to specify a slot in the Data zone or a transport key in the hardware array.*
- #define **GENDIG\_ZONE\_SHARED\_NONCE** ((uint8\_t)3)  
*GenDig zone id shared nonce. KeyID specifies the location of the input value in the message generation.*
- #define **GENDIG\_ZONE\_COUNTER** ((uint8\_t)4)  
*GenDig zone id counter. KeyID specifies the monotonic counter ID to be included in the message generation.*
- #define **GENDIG\_ZONE\_KEY\_CONFIG** ((uint8\_t)5)  
*GenDig zone id key config. KeyID specifies the slot for which the configuration information is to be included in the message generation.*
- #define **GENDIG\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_MIN](#)  
*GenDig command response packet size.*
- #define **GENDIG\_USE\_TEMPKEY\_BIT** ((uint16\_t)0x8000)  
*Use temp key for GenDig command if bit 15 is 1.*

#### Definitions for the GenDivKey Command

- #define **GENDIVKEY\_MODE** ((uint8\_t)2)
- #define **GENDIVKEY\_OTHER\_DATA\_SIZE** ((uint8\_t)4)
- #define **GENDIVKEY\_DEFAULT\_KEYID** ((uint16\_t)0x0003)

#### Definitions for the GenKey Command

- #define **GENKEY\_MODE\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*GenKey command index for mode.*
- #define **GENKEY\_KEYID\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
*GenKey command index for key id.*
- #define **GENKEY\_DATA\_IDX** (5u)  
*GenKey command index for other data.*
- #define **GENKEY\_COUNT** [ATCA\\_CMD\\_SIZE\\_MIN](#)  
*GenKey command packet size without "other data".*
- #define **GENKEY\_COUNT\_DATA** (10u)  
*GenKey command packet size with "other data".*
- #define **GENKEY\_OTHER\_DATA\_SIZE** (3u)  
*GenKey size of "other data".*
- #define **GENKEY\_MODE\_MASK** ((uint8\_t)0x1C)  
*GenKey mode bits 0 to 1 and 5 to 7 are 0.*
- #define **GENKEY\_MODE\_PRIVATE** ((uint8\_t)0x04)  
*GenKey mode: private key generation.*
- #define **GENKEY\_MODE\_PUBLIC** ((uint8\_t)0x00)  
*GenKey mode: public key calculation.*



- #define **GENKEY\_MODE\_DIGEST** ((uint8\_t)0x08)  
*GenKey mode: PubKey digest will be created after the public key is calculated.*
- #define **GENKEY\_MODE\_PUBKEY\_DIGEST** ((uint8\_t)0x10)  
*GenKey mode: Calculate PubKey digest on the public key in KeyId.*
- #define **GENKEY\_MODE\_MAC** ((uint8\_t)0x20)  
*Genkey mode: Calculate MAC of public key + session key.*
- #define **GENKEY\_PRIVATE\_TO\_TEMPKEY** ((uint16\_t)0xFFFF)  
*GenKey Create private key and store to tempkey (608 only)*
- #define **GENKEY\_RSP\_SIZE\_SHORT** [ATCA\\_RSP\\_SIZE\\_MIN](#)  
*GenKey response packet size in Digest mode.*
- #define **GENKEY\_RSP\_SIZE\_LONG** [ATCA\\_RSP\\_SIZE\\_64](#)  
*GenKey response packet size when returning a public key.*

### Definitions for the HMAC Command

- #define **HMAC\_MODE\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*HMAC command index for mode.*
- #define **HMAC\_KEYID\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
*HMAC command index for key id.*
- #define **HMAC\_COUNT** [ATCA\\_CMD\\_SIZE\\_MIN](#)  
*HMAC command packet size.*
- #define **HMAC\_MODE\_FLAG\_TK\_RAND** ((uint8\_t)0x00)  
*HMAC mode bit 2: The value of this bit must match the value in TempKey.SourceFlag or the command will return an error.*
- #define **HMAC\_MODE\_FLAG\_TK\_NORAND** ((uint8\_t)0x04)  
*HMAC mode bit 2: The value of this bit must match the value in TempKey.SourceFlag or the command will return an error.*
- #define **HMAC\_MODE\_FLAG\_OTP88** ((uint8\_t)0x10)  
*HMAC mode bit 4: Include the first 88 OTP bits (OTP[0] through OTP[10]) in the message.; otherwise, the corresponding message bits are set to zero. Not applicable for ATECC508A.*
- #define **HMAC\_MODE\_FLAG\_OTP64** ((uint8\_t)0x20)  
*HMAC mode bit 5: Include the first 64 OTP bits (OTP[0] through OTP[7]) in the message.; otherwise, the corresponding message bits are set to zero. If Mode[4] is set, the value of this mode bit is ignored. Not applicable for ATECC508A.*
- #define **HMAC\_MODE\_FLAG\_FULLSN** ((uint8\_t)0x40)  
*HMAC mode bit 6: If set, include the 48 bits SN[2:3] and SN[4:7] in the message.; otherwise, the corresponding message bits are set to zero.*
- #define **HMAC\_MODE\_MASK** ((uint8\_t)0x74)  
*HMAC mode bits 0, 1, 3, and 7 are 0.*
- #define **HMAC\_DIGEST\_SIZE** (32u)  
*HMAC size of digest response.*
- #define **HMAC\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_32](#)  
*HMAC command response packet size.*

### Definitions for the Info Command

- #define **INFO\_PARAM1\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*Info command index for 1. parameter.*
- #define **INFO\_PARAM2\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
*Info command index for 2. parameter.*
- #define **INFO\_COUNT** [ATCA\\_CMD\\_SIZE\\_MIN](#)  
*Info command packet size.*
- #define **INFO\_MODE\_REVISION** ((uint8\_t)0x00)  
*Info mode Revision.*
- #define **INFO\_MODE\_KEY\_VALID** ((uint8\_t)0x01)  
*Info mode KeyValid.*
- #define **INFO\_MODE\_STATE** ((uint8\_t)0x02)  
*Info mode State.*

- **#define INFO\_MODE\_LOCK\_STATUS** ((uint8\_t)0x02)  
*Info mode Lock status for ECC204,TA010,SHA10x devices.*
- **#define INFO\_MODE\_CHIP\_STATUS** ((uint8\_t)0xC5)  
*Info mode Chip status for ECC204,TA010,SHA10x devices.*
- **#define INFO\_MODE\_GPIO** ((uint8\_t)0x03)  
*Info mode GPIO.*
- **#define INFO\_MODE\_VOL\_KEY\_PERMIT** ((uint8\_t)0x04)  
*Info mode GPIO.*
- **#define INFO\_MODE\_MAX** ((uint8\_t)0x03)  
*Info mode maximum value.*
- **#define INFO\_NO\_STATE** ((uint8\_t)0x00)  
*Info mode is not the state mode.*
- **#define INFO\_OUTPUT\_STATE\_MASK** ((uint8\_t)0x01)  
*Info output state mask.*
- **#define INFO\_DRIVER\_STATE\_MASK** ((uint8\_t)0x02)  
*Info driver state mask.*
- **#define INFO\_PARAM2\_SET\_LATCH\_STATE** ((uint16\_t)0x0002)  
*Info param2 to set the persistent latch state.*
- **#define INFO\_PARAM2\_LATCH\_SET** ((uint16\_t)0x0001)  
*Info param2 to set the persistent latch.*
- **#define INFO\_PARAM2\_LATCH\_CLEAR** ((uint16\_t)0x0000)  
*Info param2 to clear the persistent latch.*
- **#define INFO\_SIZE** ((uint8\_t)0x04)  
*Info return size.*
- **#define INFO\_RSP\_SIZE ATCA\_RSP\_SIZE\_VAL**  
*Info command response packet size.*

#### Definitions for the KDF Command

- **#define KDF\_MODE\_IDX ATCA\_PARAM1\_IDX**  
*KDF command index for mode.*
- **#define KDF\_KEYID\_IDX ATCA\_PARAM2\_IDX**  
*KDF command index for key id.*
- **#define KDF\_DETAILS\_IDX ATCA\_DATA\_IDX**  
*KDF command index for details.*
- **#define KDF\_DETAILS\_SIZE** (4u)  
*KDF details (param3) size.*
- **#define KDF\_MESSAGE\_IDX (ATCA\_DATA\_IDX + KDF\_DETAILS\_SIZE)**
- **#define KDF\_MODE\_SOURCE\_MASK** ((uint8\_t)0x03)  
*KDF mode source key mask.*
- **#define KDF\_MODE\_SOURCE\_TEMPKEY** ((uint8\_t)0x00)  
*KDF mode source key in TempKey.*
- **#define KDF\_MODE\_SOURCE\_TEMPKEY\_UP** ((uint8\_t)0x01)  
*KDF mode source key in upper TempKey.*
- **#define KDF\_MODE\_SOURCE\_SLOT** ((uint8\_t)0x02)  
*KDF mode source key in a slot.*
- **#define KDF\_MODE\_SOURCE\_ALTKEYBUF** ((uint8\_t)0x03)  
*KDF mode source key in alternate key buffer.*
- **#define KDF\_MODE\_TARGET\_MASK** ((uint8\_t)0x1C)  
*KDF mode target key mask.*
- **#define KDF\_MODE\_TARGET\_TEMPKEY** ((uint8\_t)0x00)  
*KDF mode target key in TempKey.*
- **#define KDF\_MODE\_TARGET\_TEMPKEY\_UP** ((uint8\_t)0x04)  
*KDF mode target key in upper TempKey.*
- **#define KDF\_MODE\_TARGET\_SLOT** ((uint8\_t)0x08)  
*KDF mode target key in slot.*
- **#define KDF\_MODE\_TARGET\_ALTKEYBUF** ((uint8\_t)0x0C)  
*KDF mode target key in alternate key buffer.*

- **#define KDF\_MODE\_TARGET\_OUTPUT** ((uint8\_t)0x10)  
*KDF mode target key in output buffer.*
- **#define KDF\_MODE\_TARGET\_OUTPUT\_ENC** ((uint8\_t)0x14)  
*KDF mode target key encrypted in output buffer.*
- **#define KDF\_MODE\_ALG\_MASK** ((uint8\_t)0x60)  
*KDF mode algorithm mask.*
- **#define KDF\_MODE\_ALG\_PRF** ((uint8\_t)0x00)  
*KDF mode PRF algorithm.*
- **#define KDF\_MODE\_ALG\_AES** ((uint8\_t)0x20)  
*KDF mode AES algorithm.*
- **#define KDF\_MODE\_ALG\_HKDF** ((uint8\_t)0x40)  
*KDF mode HKDF algorithm.*
- **#define KDF\_DETAILS\_PRF\_KEY\_LEN\_MASK** ((uint32\_t)0x00000003)  
*KDF details for PRF, source key length mask.*
- **#define KDF\_DETAILS\_PRF\_KEY\_LEN\_16** ((uint32\_t)0x00000000)  
*KDF details for PRF, source key length is 16 bytes.*
- **#define KDF\_DETAILS\_PRF\_KEY\_LEN\_32** ((uint32\_t)0x00000001)  
*KDF details for PRF, source key length is 32 bytes.*
- **#define KDF\_DETAILS\_PRF\_KEY\_LEN\_48** ((uint32\_t)0x00000002)  
*KDF details for PRF, source key length is 48 bytes.*
- **#define KDF\_DETAILS\_PRF\_KEY\_LEN\_64** ((uint32\_t)0x00000003)  
*KDF details for PRF, source key length is 64 bytes.*
- **#define KDF\_DETAILS\_PRF\_TARGET\_LEN\_MASK** ((uint32\_t)0x00000100)  
*KDF details for PRF, target length mask.*
- **#define KDF\_DETAILS\_PRF\_TARGET\_LEN\_32** ((uint32\_t)0x00000000)  
*KDF details for PRF, target length is 32 bytes.*
- **#define KDF\_DETAILS\_PRF\_TARGET\_LEN\_64** ((uint32\_t)0x00000100)  
*KDF details for PRF, target length is 64 bytes.*
- **#define KDF\_DETAILS\_PRF\_AEAD\_MASK** ((uint32\_t)0x00000600)  
*KDF details for PRF, AEAD processing mask.*
- **#define KDF\_DETAILS\_PRF\_AEAD\_MODE0** ((uint32\_t)0x00000000)  
*KDF details for PRF, AEAD no processing.*
- **#define KDF\_DETAILS\_PRF\_AEAD\_MODE1** ((uint32\_t)0x00000200)  
*KDF details for PRF, AEAD First 32 go to target, second 32 go to output buffer.*
- **#define KDF\_DETAILS\_AES\_KEY\_LOC\_MASK** ((uint32\_t)0x00000003)  
*KDF details for AES, key location mask.*
- **#define KDF\_DETAILS\_HKDF\_MSG\_LOC\_MASK** ((uint32\_t)0x00000003)  
*KDF details for HKDF, message location mask.*
- **#define KDF\_DETAILS\_HKDF\_MSG\_LOC\_SLOT** ((uint32\_t)0x00000000)  
*KDF details for HKDF, message location in slot.*
- **#define KDF\_DETAILS\_HKDF\_MSG\_LOC\_TEMPKEY** ((uint32\_t)0x00000001)  
*KDF details for HKDF, message location in TempKey.*
- **#define KDF\_DETAILS\_HKDF\_MSG\_LOC\_INPUT** ((uint32\_t)0x00000002)  
*KDF details for HKDF, message location in input parameter.*
- **#define KDF\_DETAILS\_HKDF\_MSG\_LOC\_IV** ((uint32\_t)0x00000003)  
*KDF details for HKDF, message location is a special IV function.*
- **#define KDF\_DETAILS\_HKDF\_ZERO\_KEY** ((uint32\_t)0x00000004)  
*KDF details for HKDF, key is 32 bytes of zero.*

### Definitions for the Lock Command

- **#define LOCK\_ZONE\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*Lock command index for zone.*
- **#define LOCK\_SUMMARY\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
*Lock command index for summary.*
- **#define LOCK\_COUNT** [ATCA\\_CMD\\_SIZE\\_MIN](#)  
*Lock command packet size.*
- **#define LOCK\_ZONE\_CONFIG** ((uint8\_t)0x00)

- Lock zone is Config.*
- #define **LOCK\_ZONE\_DATA** ((uint8\_t)0x01)
- Lock zone is OTP or Data.*
- #define **LOCK\_ZONE\_DATA\_SLOT** ((uint8\_t)0x02)
- Lock slot of Data.*
- #define **LOCK\_ZONE\_CA2\_DATA** ((uint8\_t)0x00)
- Lock second gen Data zone by slot.*
- #define **LOCK\_ZONE\_CA2\_CONFIG** ((uint8\_t)0x01)
- Lock second gen configuration zone by slot.*
- #define **LOCK\_ZONE\_NO\_CRC** ((uint8\_t)0x80)
- Lock command: Ignore summary.*
- #define **LOCK\_ZONE\_MASK** ((uint8\_t)0xBF)
- Lock parameter 1 bits 6 are 0.*
- #define **ATCA\_UNLOCKED** ((uint8\_t)0x55)
- Value indicating an unlocked zone.*
- #define **ATCA\_LOCKED** ((uint8\_t)0x00)
- Value indicating a locked zone.*
- #define **LOCK\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_MIN](#)
- Lock command response packet size.*

### Definitions for the MAC Command

- #define **MAC\_MODE\_IDX** [ATCA\\_PARAM1\\_IDX](#)
- MAC command index for mode.*
- #define **MAC\_KEYID\_IDX** [ATCA\\_PARAM2\\_IDX](#)
- MAC command index for key id.*
- #define **MAC\_CHALLENGE\_IDX** [ATCA\\_DATA\\_IDX](#)
- MAC command index for optional challenge.*
- #define **MAC\_COUNT\_SHORT** [ATCA\\_CMD\\_SIZE\\_MIN](#)
- MAC command packet size without challenge.*
- #define **MAC\_COUNT\_LONG** (39u)
- MAC command packet size with challenge.*
- #define **MAC\_MODE\_CHALLENGE** ((uint8\_t)0x00)
- MAC mode 0: first SHA block from data slot.*
- #define **MAC\_MODE\_BLOCK2\_TEMPKEY** ((uint8\_t)0x01)
- MAC mode bit 0: second SHA block from TempKey.*
- #define **MAC\_MODE\_BLOCK1\_TEMPKEY** ((uint8\_t)0x02)
- MAC mode bit 1: first SHA block from TempKey.*
- #define **MAC\_MODE\_SOURCE\_FLAG\_MATCH** ((uint8\_t)0x04)
- MAC mode bit 2: match TempKey.SourceFlag.*
- #define **MAC\_MODE\_PTNONCE\_TEMPKEY** ((uint8\_t)0x06)
- MAC mode bit 0: second SHA block from TempKey.*
- #define **MAC\_MODE\_PASSTHROUGH** ((uint8\_t)0x07)
- MAC mode bit 0-2: pass-through mode.*
- #define **MAC\_MODE\_INCLUDE\_OTP\_88** ((uint8\_t)0x10)
- MAC mode bit 4: include first 88 OTP bits.*
- #define **MAC\_MODE\_INCLUDE\_OTP\_64** ((uint8\_t)0x20)
- MAC mode bit 5: include first 64 OTP bits.*
- #define **MAC\_MODE\_INCLUDE\_SN** ((uint8\_t)0x40)
- MAC mode bit 6: include serial number.*
- #define **MAC\_CHALLENGE\_SIZE** (32u)
- MAC size of challenge.*
- #define **MAC\_SIZE** (32u)
- MAC size of response.*
- #define **MAC\_MODE\_MASK** ((uint8\_t)0x77)
- MAC mode bits 3 and 7 are 0.*
- #define **MAC\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_32](#)
- MAC command response packet size.*

- #define **MAC\_SHA104\_DEFAULT\_KEYID** ((uint16\_t)0x0003)

### Definitions for the Nonce Command

- #define **NONCE\_MODE\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*Nonce command index for mode.*
- #define **NONCE\_PARAM2\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
*Nonce command index for 2. parameter.*
- #define **NONCE\_INPUT\_IDX** [ATCA\\_DATA\\_IDX](#)  
*Nonce command index for input data.*
- #define **NONCE\_COUNT\_SHORT** ([ATCA\\_CMD\\_SIZE\\_MIN](#) + 20u)  
*Nonce command packet size for 20 bytes of NumIn.*
- #define **NONCE\_COUNT\_LONG** ([ATCA\\_CMD\\_SIZE\\_MIN](#) + 32u)  
*Nonce command packet size for 32 bytes of NumIn.*
- #define **NONCE\_COUNT\_LONG\_64** ([ATCA\\_CMD\\_SIZE\\_MIN](#) + 64u)  
*Nonce command packet size for 64 bytes of NumIn.*
- #define **NONCE\_MODE\_MASK** ((uint8\_t)0x03)  
*Nonce mode bits 2 to 7 are 0.*
- #define **NONCE\_MODE\_SEED\_UPDATE** ((uint8\_t)0x00)  
*Nonce mode: update seed.*
- #define **NONCE\_MODE\_NO\_SEED\_UPDATE** ((uint8\_t)0x01)  
*Nonce mode: do not update seed.*
- #define **NONCE\_MODE\_INVALID** ((uint8\_t)0x02)  
*Nonce mode 2 is invalid.*
- #define **NONCE\_MODE\_PASSTHROUGH** ((uint8\_t)0x03)  
*Nonce mode: pass-through.*
- #define **NONCE\_MODE\_GEN\_SESSION\_KEY** ((uint8\_t)0x02)  
*Nonce mode: Generate session key in ECC204 device.*
- #define **NONCE\_MODE\_INPUT\_LEN\_MASK** ((uint8\_t)0x20)  
*Nonce mode: input size mask.*
- #define **NONCE\_MODE\_INPUT\_LEN\_32** ((uint8\_t)0x00)  
*Nonce mode: input size is 32 bytes.*
- #define **NONCE\_MODE\_INPUT\_LEN\_64** ((uint8\_t)0x20)  
*Nonce mode: input size is 64 bytes.*
- #define **NONCE\_MODE\_TARGET\_MASK** ((uint8\_t)0xC0)  
*Nonce mode: target mask.*
- #define **NONCE\_MODE\_TARGET\_TEMPKEY** ((uint8\_t)0x00)  
*Nonce mode: target is TempKey.*
- #define **NONCE\_MODE\_TARGET\_MSGDIGBUF** ((uint8\_t)0x40)  
*Nonce mode: target is Message Digest Buffer.*
- #define **NONCE\_MODE\_TARGET\_ALTKEYBUF** ((uint8\_t)0x80)  
*Nonce mode: target is Alternate Key Buffer.*
- #define **NONCE\_ZERO\_CALC\_MASK** ((uint16\_t)0x8000)  
*Nonce zero (param2): calculation mode mask.*
- #define **NONCE\_ZERO\_CALC\_RANDOM** ((uint16\_t)0x0000)  
*Nonce zero (param2): calculation mode random, use RNG in calculation and return RNG output.*
- #define **NONCE\_ZERO\_CALC\_TEMPKEY** ((uint16\_t)0x8000)  
*Nonce zero (param2): calculation mode TempKey, use TempKey in calculation and return new TempKey value.*
- #define **NONCE\_NUMIN\_SIZE** (20)  
*Nonce NumIn size for random modes.*
- #define **NONCE\_NUMIN\_SIZE\_PASSTHROUGH** (32)  
*Nonce NumIn size for 32-byte pass-through mode.*
- #define **NONCE\_RSP\_SIZE\_SHORT** [ATCA\\_RSP\\_SIZE\\_MIN](#)  
*Nonce command response packet size with no output.*
- #define **NONCE\_RSP\_SIZE\_LONG** [ATCA\\_RSP\\_SIZE\\_32](#)  
*Nonce command response packet size with output.*

### Definitions for the Pause Command

- #define **PAUSE\_SELECT\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*Pause command index for Selector.*
- #define **PAUSE\_PARAM2\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
*Pause command index for 2. parameter.*
- #define **PAUSE\_COUNT** [ATCA\\_CMD\\_SIZE\\_MIN](#)  
*Pause command packet size.*
- #define **PAUSE\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_MIN](#)  
*Pause command response packet size.*

#### Definitions for the PrivWrite Command

- #define **PRIVWRITE\_ZONE\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*PrivWrite command index for zone.*
- #define **PRIVWRITE\_KEYID\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
*PrivWrite command index for KeyID.*
- #define **PRIVWRITE\_VALUE\_IDX** ( 5)  
*PrivWrite command index for value.*
- #define **PRIVWRITE\_MAC\_IDX** (41)  
*PrivWrite command index for MAC.*
- #define **PRIVWRITE\_COUNT** (75)  
*PrivWrite command packet size.*
- #define **PRIVWRITE\_ZONE\_MASK** ((uint8\_t)0x40)  
*PrivWrite zone bits 0 to 5 and 7 are 0.*
- #define **PRIVWRITE\_MODE\_ENCRYPT** ((uint8\_t)0x40)  
*PrivWrite mode: encrypted.*
- #define **PRIVWRITE\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_MIN](#)  
*PrivWrite command response packet size.*

#### Definitions for the Random Command

- #define **RANDOM\_MODE\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*Random command index for mode.*
- #define **RANDOM\_PARAM2\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
*Random command index for 2. parameter.*
- #define **RANDOM\_COUNT** [ATCA\\_CMD\\_SIZE\\_MIN](#)  
*Random command packet size.*
- #define **RANDOM\_SEED\_UPDATE** ((uint8\_t)0x00)  
*Random mode for automatic seed update.*
- #define **RANDOM\_NO\_SEED\_UPDATE** ((uint8\_t)0x01)  
*Random mode for no seed update.*
- #define **RANDOM\_NUM\_SIZE** ((uint8\_t)32)  
*Number of bytes in the data packet of a random command.*
- #define **RANDOM\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_32](#)  
*Random command response packet size.*

#### Definitions for the Read Command

- #define **READ\_ZONE\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*Read command index for zone.*
- #define **READ\_ADDR\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
*Read command index for address.*
- #define **READ\_COUNT** [ATCA\\_CMD\\_SIZE\\_MIN](#)  
*Read command packet size.*
- #define **READ\_ZONE\_MASK** ((uint8\_t)0x83)  
*Read zone bits 2 to 6 are 0.*
- #define **READ\_4\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_VAL](#)  
*Read command response packet size when reading 4 bytes.*



- #define **READ\_32\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_32](#)  
*Read command response packet size when reading 32 bytes.*

### Definitions for the SecureBoot Command

- #define **SECUREBOOT\_MODE\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*SecureBoot command index for mode.*
- #define **SECUREBOOT\_DIGEST\_SIZE** (32u)  
*SecureBoot digest input size.*
- #define **SECUREBOOT\_SIGNATURE\_SIZE** (64u)  
*SecureBoot signature input size.*
- #define **SECUREBOOT\_COUNT\_DIG** ([ATCA\\_CMD\\_SIZE\\_MIN](#) + [SECUREBOOT\\_DIGEST\\_SIZE](#))  
*SecureBoot command packet size for just a digest.*
- #define **SECUREBOOT\_COUNT\_DIG\_SIG** ([ATCA\\_CMD\\_SIZE\\_MIN](#) + [SECUREBOOT\\_DIGEST\\_SIZE](#) + [SECUREBOOT\\_SIGNATURE\\_SIZE](#))  
*SecureBoot command packet size for a digest and signature.*
- #define **SECUREBOOT\_MAC\_SIZE** (32u)  
*SecureBoot MAC output size.*
- #define **SECUREBOOT\_RSP\_SIZE\_NO\_MAC** [ATCA\\_RSP\\_SIZE\\_MIN](#)  
*SecureBoot response packet size for no MAC.*
- #define **SECUREBOOT\_RSP\_SIZE\_MAC** ([ATCA\\_PACKET\\_OVERHEAD](#) + [SECUREBOOT\\_MAC\\_SIZE](#))  
*SecureBoot response packet size with MAC.*
- #define **SECUREBOOT\_MODE\_MASK** ((uint8\_t)0x07)  
*SecureBoot mode mask.*
- #define **SECUREBOOT\_MODE\_FULL** ((uint8\_t)0x05)  
*SecureBoot mode Full.*
- #define **SECUREBOOT\_MODE\_FULL\_STORE** ((uint8\_t)0x06)  
*SecureBoot mode FullStore.*
- #define **SECUREBOOT\_MODE\_FULL\_COPY** ((uint8\_t)0x07)  
*SecureBoot mode FullCopy.*
- #define **SECUREBOOT\_MODE\_PROHIBIT\_FLAG** ((uint8\_t)0x40)  
*SecureBoot mode flag to prohibit SecureBoot until next power cycle.*
- #define **SECUREBOOT\_MODE\_ENC\_MAC\_FLAG** ((uint8\_t)0x80)  
*SecureBoot mode flag for encrypted digest and returning validating MAC.*
- #define **SECUREBOOTCONFIG\_OFFSET** (70)  
*SecureBootConfig byte offset into the configuration zone.*
- #define **SECUREBOOTCONFIG\_MODE\_MASK** ((uint16\_t)0x0003)  
*Mask for SecureBootMode field in SecureBootConfig value.*
- #define **SECUREBOOTCONFIG\_MODE\_DISABLED** ((uint16\_t)0x0000)  
*Disabled SecureBootMode in SecureBootConfig value.*
- #define **SECUREBOOTCONFIG\_MODE\_FULL\_BOTH** ((uint16\_t)0x0001)  
*Both digest and signature always required SecureBootMode in SecureBootConfig value.*
- #define **SECUREBOOTCONFIG\_MODE\_FULL\_SIG** ((uint16\_t)0x0002)  
*Signature stored SecureBootMode in SecureBootConfig value.*
- #define **SECUREBOOTCONFIG\_MODE\_FULL\_DIG** ((uint16\_t)0x0003)  
*Digest stored SecureBootMode in SecureBootConfig value.*

### Definitions for the SelfTest Command

- #define **SELFTEST\_MODE\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*SelfTest command index for mode.*
- #define **SELFTEST\_COUNT** [ATCA\\_CMD\\_SIZE\\_MIN](#)  
*SelfTest command packet size.*
- #define **SELFTEST\_MODE\_RNG** ((uint8\_t)0x01)  
*SelfTest mode RNG DRBG function.*
- #define **SELFTEST\_MODE\_ECDSA\_SIGN\_VERIFY** ((uint8\_t)0x04)  
*SelfTest mode ECDSA verify function.*
- #define **SELFTEST\_MODE\_ECDH** ((uint8\_t)0x08)

- SelfTest mode ECDH function.*
- #define **SELFTEST\_MODE\_AES** ((uint8\_t)0x10)  
*SelfTest mode AES encrypt function.*
- #define **SELFTEST\_MODE\_SHA** ((uint8\_t)0x20)  
*SelfTest mode SHA function.*
- #define **SELFTEST\_MODE\_ALL** ((uint8\_t)0x3B)  
*SelfTest mode all algorithms.*
- #define **SELFTEST\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_MIN](#)  
*SelfTest command response packet size.*

### Definitions for the SHA Command

- #define **SHA\_COUNT\_SHORT** [ATCA\\_CMD\\_SIZE\\_MIN](#)
- #define **SHA\_COUNT\_LONG** [ATCA\\_CMD\\_SIZE\\_MIN](#)  
*Just a starting size.*
- #define **ATCA\_SHA\_DIGEST\_SIZE** (32u)
- #define **SHA\_DATA\_MAX** (64)
- #define **SHA\_MODE\_MASK** ((uint8\_t)0x07)  
*Mask the bit 0-2.*
- #define **SHA\_MODE\_SHA256\_START** ((uint8\_t)0x00)  
*Initialization, does not accept a message.*
- #define **SHA\_MODE\_SHA256\_UPDATE** ((uint8\_t)0x01)  
*Add 64 bytes in the message to the SHA context.*
- #define **SHA\_MODE\_SHA256\_END** ((uint8\_t)0x02)  
*Complete the calculation and return the digest.*
- #define **SHA\_MODE\_SHA256\_PUBLIC** ((uint8\_t)0x03)  
*Add 64 byte ECC public key in the slot to the SHA context.*
- #define **SHA\_MODE\_HMAC\_START** ((uint8\_t)0x04)  
*Initialization, HMAC calculation.*
- #define **SHA\_MODE\_ECC204\_HMAC\_START** ((uint8\_t)0x03)  
*Initialization, HMAC calculation for ECC204.*
- #define **SHA\_MODE\_HMAC\_UPDATE** ((uint8\_t)0x01)  
*Add 64 bytes in the message to the SHA context.*
- #define **SHA\_MODE\_HMAC\_END** ((uint8\_t)0x05)  
*Complete the HMAC computation and return digest.*
- #define **SHA\_MODE\_608\_HMAC\_END** ((uint8\_t)0x02)  
*Complete the HMAC computation and return digest... Different command on 608.*
- #define **SHA\_MODE\_ECC204\_HMAC\_END** ((uint8\_t)0x02)  
*Complete the HMAC computation and return digest... Different mode on ECC204.*
- #define **SHA\_MODE\_READ\_CONTEXT** ((uint8\_t)0x06)  
*Read current SHA-256 context out of the device.*
- #define **SHA\_MODE\_WRITE\_CONTEXT** ((uint8\_t)0x07)  
*Restore a SHA-256 context into the device.*
- #define **SHA\_MODE\_TARGET\_MASK** ((uint8\_t)0xC0)  
*Resulting digest target location mask.*
- #define **SHA\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_32](#)  
*SHA command response packet size.*
- #define **SHA\_RSP\_SIZE\_SHORT** [ATCA\\_RSP\\_SIZE\\_MIN](#)  
*SHA command response packet size only status code.*
- #define **SHA\_RSP\_SIZE\_LONG** [ATCA\\_RSP\\_SIZE\\_32](#)  
*SHA command response packet size.*

### Definitions for the Sign Command

- #define **SIGN\_MODE\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*Sign command index for mode.*
- #define **SIGN\_KEYID\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
*Sign command index for key id.*



- **#define SIGN\_COUNT** [ATCA\\_CMD\\_SIZE\\_MIN](#)  
*Sign command packet size.*
- **#define SIGN\_MODE\_MASK** ((uint8\_t)0xE1)  
*Sign mode bits 1 to 4 are 0.*
- **#define SIGN\_MODE\_INTERNAL** ((uint8\_t)0x00)  
*Sign mode 0: internal.*
- **#define SIGN\_MODE\_INVALIDATE** ((uint8\_t)0x01)  
*Sign mode bit 1: Signature will be used for Verify(Invalidate)*
- **#define SIGN\_MODE\_INCLUDE\_SN** ((uint8\_t)0x40)  
*Sign mode bit 6: include serial number.*
- **#define SIGN\_MODE\_EXTERNAL** ((uint8\_t)0x80)  
*Sign mode bit 7: external.*
- **#define SIGN\_MODE\_SOURCE\_MASK** ((uint8\_t)0x20)  
*Sign mode message source mask.*
- **#define SIGN\_MODE\_SOURCE\_TEMPKEY** ((uint8\_t)0x00)  
*Sign mode message source is TempKey.*
- **#define SIGN\_MODE\_SOURCE\_MSGDIGBUF** ((uint8\_t)0x20)  
*Sign mode message source is the Message Digest Buffer.*
- **#define SIGN\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_MAX](#)  
*Sign command response packet size.*

#### Definitions for the UpdateExtra Command

- **#define UPDATE\_MODE\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*UpdateExtra command index for mode.*
- **#define UPDATE\_VALUE\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
*UpdateExtra command index for new value.*
- **#define UPDATE\_COUNT** [ATCA\\_CMD\\_SIZE\\_MIN](#)  
*UpdateExtra command packet size.*
- **#define UPDATE\_MODE\_USER\_EXTRA** ((uint8\_t)0x00)  
*UpdateExtra mode update UserExtra (config byte 84)*
- **#define UPDATE\_MODE\_SELECTOR** ((uint8\_t)0x01)  
*UpdateExtra mode update Selector (config byte 85)*
- **#define UPDATE\_MODE\_USER\_EXTRA\_ADD** [UPDATE\\_MODE\\_SELECTOR](#)  
*UpdateExtra mode update UserExtraAdd (config byte 85)*
- **#define UPDATE\_MODE\_DEC\_COUNTER** ((uint8\_t)0x02)  
*UpdateExtra mode: decrement counter.*
- **#define UPDATE\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_MIN](#)  
*UpdateExtra command response packet size.*

#### Definitions for the Verify Command

- **#define VERIFY\_MODE\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*Verify command index for mode.*
- **#define VERIFY\_KEYID\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
*Verify command index for key id.*
- **#define VERIFY\_DATA\_IDX** ( 5)  
*Verify command index for data.*
- **#define VERIFY\_256\_STORED\_COUNT** ( 71)  
*Verify command packet size for 256-bit key in stored mode.*
- **#define VERIFY\_283\_STORED\_COUNT** ( 79)  
*Verify command packet size for 283-bit key in stored mode.*
- **#define VERIFY\_256\_VALIDATE\_COUNT** ( 90)  
*Verify command packet size for 256-bit key in validate mode.*
- **#define VERIFY\_283\_VALIDATE\_COUNT** ( 98)  
*Verify command packet size for 283-bit key in validate mode.*
- **#define VERIFY\_256\_EXTERNAL\_COUNT** (135)  
*Verify command packet size for 256-bit key in external mode.*

- **#define VERIFY\_283\_EXTERNAL\_COUNT** (151)  
*Verify command packet size for 283-bit key in external mode.*
- **#define VERIFY\_256\_KEY\_SIZE** ( 64)  
*Verify key size for 256-bit key.*
- **#define VERIFY\_283\_KEY\_SIZE** ( 72)  
*Verify key size for 283-bit key.*
- **#define VERIFY\_256\_SIGNATURE\_SIZE** ( 64)  
*Verify signature size for 256-bit key.*
- **#define VERIFY\_283\_SIGNATURE\_SIZE** ( 72)  
*Verify signature size for 283-bit key.*
- **#define VERIFY\_OTHER\_DATA\_SIZE** ( 19u)  
*Verify size of "other data".*
- **#define VERIFY\_MODE\_MASK** ((uint8\_t)0x07)  
*Verify mode bits 3 to 7 are 0.*
- **#define VERIFY\_MODE\_STORED** ((uint8\_t)0x00)  
*Verify mode: stored.*
- **#define VERIFY\_MODE\_VALIDATE\_EXTERNAL** ((uint8\_t)0x01)  
*Verify mode: validate external.*
- **#define VERIFY\_MODE\_EXTERNAL** ((uint8\_t)0x02)  
*Verify mode: external.*
- **#define VERIFY\_MODE\_VALIDATE** ((uint8\_t)0x03)  
*Verify mode: validate.*
- **#define VERIFY\_MODE\_INVALIDATE** ((uint8\_t)0x07)  
*Verify mode: invalidate.*
- **#define VERIFY\_MODE\_SOURCE\_MASK** ((uint8\_t)0x20)  
*Verify mode message source mask.*
- **#define VERIFY\_MODE\_SOURCE\_TEMPKEY** ((uint8\_t)0x00)  
*Verify mode message source is TempKey.*
- **#define VERIFY\_MODE\_SOURCE\_MSGDIGBUF** ((uint8\_t)0x20)  
*Verify mode message source is the Message Digest Buffer.*
- **#define VERIFY\_MODE\_MAC\_FLAG** ((uint8\_t)0x80)  
*Verify mode: MAC.*
- **#define VERIFY\_KEY\_B283** ((uint16\_t)0x0000)  
*Verify key type: B283.*
- **#define VERIFY\_KEY\_K283** ((uint16\_t)0x0001)  
*Verify key type: K283.*
- **#define VERIFY\_KEY\_P256** ((uint16\_t)0x0004)  
*Verify key type: P256.*
- **#define VERIFY\_RSP\_SIZE** [ATCA\\_RSP\\_SIZE\\_MIN](#)  
*Verify command response packet size.*
- **#define VERIFY\_RSP\_SIZE\_MAC** [ATCA\\_RSP\\_SIZE\\_32](#)  
*Verify command response packet size with validating MAC.*

#### Definitions for the Write Command

- **#define WRITE\_ZONE\_IDX** [ATCA\\_PARAM1\\_IDX](#)  
*Write command index for zone.*
- **#define WRITE\_ADDR\_IDX** [ATCA\\_PARAM2\\_IDX](#)  
*Write command index for address.*
- **#define WRITE\_VALUE\_IDX** [ATCA\\_DATA\\_IDX](#)  
*Write command index for data.*
- **#define WRITE\_MAC\_VS\_IDX** ( 9)  
*Write command index for MAC following short data.*
- **#define WRITE\_MAC\_VL\_IDX** (37)  
*Write command index for MAC following long data.*
- **#define WRITE\_MAC\_SIZE** (32u)  
*Write MAC size.*
- **#define WRITE\_ZONE\_MASK** ((uint8\_t)0xC3)

- *Write zone bits 2 to 5 are 0.*  
• #define **WRITE\_ZONE\_WITH\_MAC** ((uint8\_t)0x40)  
*Write zone bit 6: write encrypted with MAC.*
- #define **WRITE\_ZONE\_OTP** ((uint8\_t)1)  
*Write zone id OTP.*
- #define **WRITE\_ZONE\_DATA** ((uint8\_t)2)  
*Write zone id data.*
- #define **WRITE\_RSP\_SIZE** **ATCA\_RSP\_SIZE\_MIN**  
*Write command response packet size.*

## Functions

- ATCA\_STATUS **atInfo** (ATCADeviceType device\_type, **ATCAPacket** \*packet)  
*ATCACommand Info method.*
- ATCA\_STATUS **atPause** (ATCADeviceType device\_type, **ATCAPacket** \*packet)  
*ATCACommand Pause method.*
- bool **atIsSHAFamily** (ATCADeviceType device\_type)  
*determines if a given device type is a SHA device or a superset of a SHA device*
- bool **atIsECCFamily** (ATCADeviceType device\_type)  
*determines if a given device type is an ECC device or a superset of a ECC device*
- ATCA\_STATUS **isATCAError** (uint8\_t \*data)  
*checks for basic error frame in data*
- void **atCRC** (size\_t length, const uint8\_t \*data, uint8\_t \*crc\_le)  
*Calculates CRC over the given raw data and returns the CRC in little-endian byte order.*
- void **atCalcCRC** (**ATCAPacket** \*packet)  
*This function calculates CRC and adds it to the correct offset in the packet data.*
- ATCA\_STATUS **atCheckCRC** (const uint8\_t \*response)  
*This function checks the consistency of a response.*

### 22.79.1 Detailed Description

Microchip Crypto Auth device command object - this is a command builder only, it does not send the command. The result of a command method is a fully formed packet, ready to send to the ATCAIFace object to dispatch.

This command object supports the ATSHA and ATECC device family. The command list is a superset of all device commands for this family. The command object differentiates the packet contents based on specific device type within the family.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.79.2 Function Documentation

#### 22.79.2.1 atCalcCRC()

```
void atCalcCRC (
    ATCAPacket * packet )
```

This function calculates CRC and adds it to the correct offset in the packet data.

Parameters

in	<i>packet</i>	Packet to calculate CRC data for
----	---------------	----------------------------------

22.79.2.2 atCheckCrc()

```
ATCA_STATUS atCheckCrc (
    const uint8_t * response )
```

This function checks the consistency of a response.

Parameters

in	<i>response</i>	pointer to response
----	-----------------	---------------------

Returns

ATCA\_SUCCESS on success, otherwise ATCA\_RX\_CRC\_ERROR

22.79.2.3 atCRC()

```
void atCRC (
    size_t length,
    const uint8_t * data,
    uint8_t * crc_le )
```

Calculates CRC over the given raw data and returns the CRC in little-endian byte order.

Parameters

in	<i>length</i>	Size of data not including the CRC byte positions
in	<i>data</i>	Pointer to the data over which to compute the CRC
out	<i>crc↔ _le</i>	Pointer to the place where the two-bytes of CRC will be returned in little-endian byte order.

22.79.2.4 atInfo()

```
ATCA_STATUS atInfo (
    ATCADeviceType device_type,
    ATCAPacket * packet )
```

ATCACommand Info method.

**Parameters**

in	<i>ca_cmd</i>	instance
in	<i>packet</i>	pointer to the packet containing the command being built

**Returns**

ATCA\_SUCCESS

**22.79.2.5 atIsECCFamily()**

```
bool atIsECCFamily (
    ATCADeviceType device_type )
```

determines if a given device type is an ECC device or a superset of a ECC device

**Parameters**

in	<i>device_type</i>	Type of device to check for family type
----	--------------------	---

**Returns**

boolean indicating whether the given device is an ECC family device.

**22.79.2.6 atIsSHAFamily()**

```
bool atIsSHAFamily (
    ATCADeviceType device_type )
```

determines if a given device type is a SHA device or a superset of a SHA device

**Parameters**

in	<i>device_type</i>	Type of device to check for family type
----	--------------------	---

**Returns**

boolean indicating whether the given device is a SHA family device.

22.79.2.7 atPause()

```
ATCA_STATUS atPause (
    ATCADeviceType device_type,
    ATCAPacket * packet )
```

ATCACommand Pause method.

Parameters

in	<i>ca_cmd</i>	instance
in	<i>packet</i>	pointer to the packet containing the command being built

Returns

ATCA\_SUCCESS

22.79.2.8 isATCAError()

```
ATCA_STATUS isATCAError (
    uint8_t * data )
```

checks for basic error frame in data

Parameters

in	<i>data</i>	pointer to received data - expected to be in the form of a CA device response frame
----	-------------	---

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.80 calib\_config\_check.h File Reference

Consistency checks for configuration options.

```
#include "atca_config_check.h"
#include "crypto/crypto_sw_config_check.h"
```

Macros

- #define **CALIB\_SHA204\_EN** DEFAULT\_ENABLED
- #define **CALIB\_SHA206\_EN** DEFAULT\_ENABLED
- #define **CALIB\_ECC108\_EN** DEFAULT\_DISABLED
- #define **CALIB\_ECC508\_EN** DEFAULT\_ENABLED

- #define **CALIB\_ECC608\_EN** DEFAULT\_ENABLED
- #define **CALIB\_ECC204\_EN** DEFAULT\_ENABLED
- #define **CALIB\_TA010\_EN** DEFAULT\_ENABLED
- #define **CALIB\_SHA104\_EN** DEFAULT\_ENABLED
- #define **CALIB\_SHA105\_EN** DEFAULT\_ENABLED
- #define **CALIB\_FULL\_FEATURE** (CALIB\_SHA204\_EN || CALIB\_ECC108\_EN || CALIB\_ECC508\_EN || CALIB\_ECC608\_EN)
- #define **CALIB\_ECC\_SUPPORT** (CALIB\_ECC108\_EN || CALIB\_ECC508\_EN || CALIB\_ECC608\_EN || CALIB\_ECC204\_EN || CALIB\_TA010\_EN)
- #define **CALIB\_CA2\_SUPPORT** (CALIB\_ECC204\_EN || CALIB\_TA010\_EN || CALIB\_SHA104\_EN || CALIB\_SHA105\_EN)
- #define **CALIB\_CA2\_CERT\_SUPPORT** (CALIB\_ECC204\_EN || CALIB\_TA010\_EN)
- #define **CALIB\_SHA206\_ONLY** (CALIB\_SHA206\_EN && !(CALIB\_FULL\_FEATURE || ATCA\_CA2\_SUPPORT))
- #define **DEFAULT\_CA\_MAX\_PACKET\_SIZE** (198u)
- #define **CA\_MAX\_PACKET\_SIZE** (DEFAULT\_CA\_MAX\_PACKET\_SIZE)
- #define **CALIB\_AES\_EN** (ATCAB\_AES\_EN && CALIB\_ECC608\_EN)
- #define **CALIB\_AES\_GCM\_EN** (ATCAB\_AES\_GCM\_EN && CALIB\_AES\_EN && CALIB\_ECC608\_EN)
- #define **CALIB\_CHECKMAC\_EN** (ATCAB\_CHECKMAC\_EN && (CALIB\_FULL\_FEATURE || CALIB\_SHA105\_EN))
- #define **CALIB\_COUNTER\_EN** (ATCAB\_COUNTER\_EN && (CALIB\_ECC\_SUPPORT || CALIB\_SHA104\_EN || CALIB\_SHA105\_EN))
- #define **CALIB\_DELETE\_EN** (DEFAULT\_DISABLED)
- #define **CALIB\_DERIVEKEY\_EN** (ATCAB\_DERIVEKEY\_EN && (CALIB\_FULL\_FEATURE || CALIB\_SHA206\_EN))
- #define **CALIB\_ECDH\_EN** (ATCAB\_ECDH\_EN && (CALIB\_ECC508\_EN || CALIB\_ECC608\_EN))
- #define **CALIB\_ECDH\_ENC\_EN** (ATCAB\_ECDH\_ENC\_EN && (CALIB\_ECC508\_EN || CALIB\_ECC608\_EN))
- #define **CALIB\_GENDIG\_EN** (ATCAB\_GENDIG\_EN && (CALIB\_FULL\_FEATURE || CALIB\_SHA105\_EN))
- #define **CALIB\_GENDIVKEY\_EN** (ATCAB\_GENDIG\_EN && CALIB\_SHA105\_EN)
- #define **CALIB\_GENKEY\_EN** (ATCAB\_GENKEY\_EN && CALIB\_ECC\_SUPPORT)
- #define **CALIB\_GENKEY\_MAC\_EN** (ATCAB\_GENKEY\_MAC\_EN && CALIB\_ECC\_SUPPORT)
- #define **CALIB\_HMAC\_EN** (ATCAB\_HMAC\_EN && (CALIB\_SHA204\_EN || CALIB\_ECC108\_EN || CALIB\_ECC508\_EN))
- #define **CALIB\_INFO\_LATCH\_EN** ATCAB\_INFO\_LATCH\_EN
- #define **CALIB\_KDF\_EN** (ATCAB\_KDF\_EN && CALIB\_ECC608\_EN)
- #define **CALIB\_LOCK\_EN** (ATCAB\_LOCK\_EN && CALIB\_FULL\_FEATURE)
- #define **CALIB\_LOCK\_CA2\_EN** (ATCAB\_LOCK\_EN && ATCA\_CA2\_SUPPORT)
- #define **CALIB\_MAC\_EN** (ATCAB\_MAC\_EN && (CALIB\_FULL\_FEATURE || CALIB\_SHA206\_EN || CALIB\_SHA104\_EN))
- #define **CALIB\_NONCE\_EN** (ATCAB\_NONCE\_EN && (CALIB\_FULL\_FEATURE || CALIB\_CA2\_SUPPORT))
- #define **CALIB\_PRIVWRITE\_EN** (ATCAB\_PRIVWRITE\_EN && (CALIB\_ECC108\_EN || CALIB\_ECC508\_EN || CALIB\_ECC608\_EN))
- #define **CALIB\_RANDOM\_EN** (ATCAB\_RANDOM\_EN && CALIB\_FULL\_FEATURE)
- #define **CALIB\_READ\_EN** (ATCAB\_READ\_EN && (CALIB\_FULL\_FEATURE || CALIB\_SHA206\_EN))
- #define **CALIB\_READ\_CA2\_EN** (ATCAB\_READ\_EN && CALIB\_CA2\_SUPPORT)
- #define **CALIB\_READ\_ENC\_EN** (ATCAB\_READ\_ENC\_EN && CALIB\_FULL\_FEATURE)
- #define **CALIB\_SECUREBOOT\_EN** (ATCAB\_SECUREBOOT\_EN && CALIB\_ECC608\_EN)
- #define **CALIB\_SECUREBOOT\_MAC\_EN** (ATCAB\_SECUREBOOT\_MAC\_EN && CALIB\_ECC608\_EN)
- #define **CALIB\_SELFTEST\_EN** (ATCAB\_SELFTEST\_EN && (CALIB\_ECC608\_EN || CALIB\_CA2\_SUPPORT))
- #define **CALIB\_SHA\_EN** (ATCAB\_SHA\_EN && (CALIB\_FULL\_FEATURE || CALIB\_CA2\_SUPPORT))
- #define **CALIB\_SHA\_HMAC\_EN** (ATCAB\_SHA\_HMAC\_EN && CALIB\_ECC\_SUPPORT)
- #define **CALIB\_SHA\_CONTEXT\_EN** (ATCAB\_SHA\_CONTEXT\_EN && CALIB\_ECC608\_EN)

- `#define CALIB_SIGN_EN (ATCAB_SIGN_EN && (CALIB_ECC108_EN || CALIB_ECC508_EN || CALIB_ECC608_EN))`
- `#define CALIB_SIGN_CA2_EN (ATCAB_SIGN_EN && (CALIB_ECC204_EN || CALIB_TA010_EN))`
- `#define CALIB_SIGN_INTERNAL_EN (ATCAB_SIGN_INTERNAL_EN && CALIB_SIGN_EN)`
- `#define CALIB_UPDATEEXTRA_EN (ATCAB_UPDATEEXTRA_EN && CALIB_FULL_FEATURE)`
- `#define CALIB_VERIFY_EN (ATCAB_VERIFY_EN && (CALIB_ECC108_EN || CALIB_ECC508_EN || CALIB_ECC608_EN))`
- `#define CALIB_VERIFY_MAC_EN (ATCAB_VERIFY_MAC_EN && CALIB_ECC608_EN)`
- `#define CALIB_VERIFY_EXTERN_EN (ATCAB_VERIFY_EXTERN_EN && CALIB_VERIFY_EN)`
- `#define CALIB_VERIFY_STORED_EN (ATCAB_VERIFY_STORED_EN && CALIB_VERIFY_EN)`
- `#define CALIB_VERIFY_VALIDATE_EN (ATCAB_VERIFY_VALIDATE_EN && CALIB_VERIFY_EN)`
- `#define CALIB_WRITE_EN (ATCAB_WRITE_EN && (CALIB_FULL_FEATURE || CALIB_SHA206_EN))`
- `#define CALIB_WRITE_ENC_EN (ATCAB_WRITE_ENC_EN && CALIB_FULL_FEATURE)`
- `#define CALIB_WRITE_CA2_EN (ATCAB_WRITE_EN && CALIB_CA2_SUPPORT)`

### 22.80.1 Detailed Description

Consistency checks for configuration options.

Copyright

(c) 2015-2021 Microchip Technology Inc. and its subsidiaries.

### 22.80.2 Macro Definition Documentation

#### 22.80.2.1 CALIB\_INFO\_LATCH\_EN

```
#define CALIB_INFO_LATCH_EN ATCAB_INFO_LATCH_EN
```

Supported API's: `calib_info_get_latch` `calib_info_set_latch`

ECC204 specific api: `calib_info_lock_status`

#### 22.80.2.2 CALIB\_LOCK\_CA2\_EN

```
#define CALIB_LOCK_CA2_EN (ATCAB_LOCK_EN && ATCA_CA2_SUPPORT)
```

Enable `CALIB_LOCK_CA2_EN` which enables the lock command for the ecc204 and ta010 devices

Supported API's: `calib_lock`

#### 22.80.2.3 CALIB\_LOCK\_EN

```
#define CALIB_LOCK_EN (ATCAB_LOCK_EN && CALIB_FULL_FEATURE)
```

Enable `CALIB_LOCK_EN` to enable the lock commands for the classic cryptoauth parts

Supported API's: `calib_lock`



#### 22.80.2.4 CALIB\_READ\_EN

```
#define CALIB_READ_EN (ATCAB_READ_EN && (CALIB_FULL_FEATURE || CALIB_SHA206_EN))
```

Enable CALIB\_READ\_EN which enables the read commands

Supported API's: calib\_read\_zone

#### 22.80.2.5 CALIB\_SHA\_CONTEXT\_EN

```
#define CALIB_SHA_CONTEXT_EN (ATCAB_SHA_CONTEXT_EN && CALIB_ECC608_EN)
```

Requires: CALIB\_SHA\_BASE

Use the SHA command to compute an HMAC/SHA-256 operation

Supported API's: calib\_sha\_read\_context

#### 22.80.2.6 CALIB\_SHA\_EN

```
#define CALIB_SHA_EN (ATCAB_SHA_EN && (CALIB_FULL_FEATURE || CALIB_CA2_SUPPORT))
```

Enable CALIB\_SHA\_EN to compute a SHA-256 or HMAC/SHA-256 digest for general purpose use by the host system

Supported API's: calib\_sha\_base

#### 22.80.2.7 CALIB\_SHA\_HMAC\_EN

```
#define CALIB_SHA_HMAC_EN (ATCAB_SHA_HMAC_EN && CALIB_ECC_SUPPORT)
```

Requires: CALIB\_SHA\_HMAC CALIB\_SHA\_BASE

Use the SHA command to compute an HMAC/SHA-256 operation

Supported API's: calib\_sha\_hmac, calib\_sha\_hmac\_init, calib\_sha\_hmac\_update, calib\_sha\_hmac\_finish

#### 22.80.2.8 CALIB\_SIGN\_CA2\_EN

```
#define CALIB_SIGN_CA2_EN (ATCAB_SIGN_EN && (CALIB_ECC204_EN || CALIB_TA010_EN))
```

Enable CALIB\_SIGN\_CA2\_EN to generate a signature using the ECDSA algorithm

Supported API's: calib\_sign\_base

#### 22.80.2.9 CALIB\_SIGN\_EN

```
#define CALIB_SIGN_EN (ATCAB_SIGN_EN && (CALIB_ECC108_EN || CALIB_ECC508_EN || CALIB_ECC608_EN))
```

Enable CALIB\_SIGN\_EN to generate a signature using the ECDSA algorithm

Supported API's: calib\_sign

### 22.80.2.10 CALIB\_UPDATEEXTRA\_EN

```
#define CALIB_UPDATEEXTRA_EN (ATCAB_UPDATEEXTRA_EN && CALIB_FULL_FEATURE)
```

Enable CALIB\_UPDATEEXTRA\_EN to update the values of the two extra bytes within the configuration zone (bytes 84 and 85)

Supported API's: calib\_updateextra

### 22.80.2.11 CALIB\_VERIFY\_EN

```
#define CALIB_VERIFY_EN (ATCAB_VERIFY_EN && (CALIB_ECC108_EN || CALIB_ECC508_EN || CALIB_ECC608_↵_EN))
```

Enable CALIB\_VERIFY\_EN which takes an ECDSA [R,S] signature and verifies that it is correctly generated from a given message and public key. In all cases, the signature is an input to the command

Supported API's: calib\_verify

### 22.80.2.12 CALIB\_VERIFY\_MAC\_EN

```
#define CALIB_VERIFY_MAC_EN (ATCAB_VERIFY_MAC_EN && CALIB_ECC608_EN)
```

Requires: CALIB\_NONCE\_MODE\_ENCODING CALIB\_NONCE\_BASE ATCAH\_VERIFY\_MAC ATCAC\_SW\_↵SHA2\_256 CALIB\_VERIFY

Executes verification command with verification MAC for the External or Stored Verify modes

Supported API's: calib\_verify\_extern\_stored\_mac, calib\_verify\_extern\_mac, calib\_verify\_stored\_mac

### 22.80.2.13 CALIB\_VERIFY\_STORED\_EN

```
#define CALIB_VERIFY_STORED_EN (ATCAB_VERIFY_STORED_EN && CALIB_VERIFY_EN)
```

Requires: CALIB\_NONCE\_MODE\_ENCODING CALIB\_NONCE\_BASE CALIB\_VERIFY

Verifies a signature (ECDSA verify operation) with a public key stored in the device

Supported API's: calib\_verify\_stored

### 22.80.2.14 CALIB\_WRITE\_ENC\_EN

```
#define CALIB_WRITE_ENC_EN (ATCAB_WRITE_ENC_EN && CALIB_FULL_FEATURE)
```

Requires: CALIB\_NONCE\_MODE\_ENCODING CALIB\_NONCE\_BASE CALIB\_READ\_ZONE CALIB\_GENDIG ATCAH\_GENDIG ATCAH\_WRITE\_AUTH\_MAC ATCAH\_NONCE ATCAC\_SW\_SHA2\_256 CALIB\_WRITE ATCAH\_GEN\_SESSION\_KEY

Performs an encrypted write of a 32 byte block into given slot

Supported API's: calib\_write\_enc

## 22.81 calib\_counter.c File Reference

CryptoAuthLib Basic API methods for Counter command.

```
#include "cryptoauthlib.h"
```

### 22.81.1 Detailed Description

CryptoAuthLib Basic API methods for Counter command.

The Counter command reads or increments the binary count value for one of the two monotonic counters

#### Note

List of devices that support this command - ATECC508A and ATECC608A/B. There are differences in the modes that they support. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.82 calib\_delete.c File Reference

CryptoAuthLib Basic API methods for Delete command.

```
#include "cryptoauthlib.h"  
#include "host/atca_host.h"
```

### 22.82.1 Detailed Description

CryptoAuthLib Basic API methods for Delete command.

The Delete command, when executed, will clear all of the Data zone slots and set all bytes of each slot to 0xFF. The Configuration zone will be untouched, except for the value of the Primary\_Deleted byte.

#### Note

List of devices that support this command - ECC204, TA010, SHA10x. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.83 calib\_derivekey.c File Reference

CryptoAuthLib Basic API methods for DeriveKey command.

```
#include "cryptoauthlib.h"
```

### 22.83.1 Detailed Description

CryptoAuthLib Basic API methods for DeriveKey command.

The DeriveKey command combines the current value of a key with the nonce stored in TempKey using SHA-256 and derives a new key.

#### Note

List of devices that support this command - ATSHA204A, ATECC108A, ATECC508A, and ATECC608A/B. There are differences in the modes that they support. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.84 calib\_device.h File Reference

Microchip Crypto Auth Device Data.

```
#include <stdint.h>
#include "atca_compiler.h"
```

### Data Structures

- struct [atsha204a\\_config\\_s](#)
- struct [atecc508a\\_config\\_s](#)
- struct [atecc608\\_config\\_s](#)

## Macros

- `#define ATCA_AES_ENABLE_EN_SHIFT (0)`
- `#define ATCA_AES_ENABLE_EN_MASK (0x01u << ATCA_AES_ENABLE_EN_SHIFT)`
- `#define ATCA_I2C_ENABLE_EN_SHIFT (0)`
- `#define ATCA_I2C_ENABLE_EN_MASK (0x01u << ATCA_I2C_ENABLE_EN_SHIFT)`
- `#define ATCA_COUNTER_MATCH_EN_SHIFT (0)`
- `#define ATCA_COUNTER_MATCH_EN_MASK (0x01u << ATCA_COUNTER_MATCH_EN_SHIFT)`
- `#define ATCA_COUNTER_MATCH_KEY_SHIFT (4)`
- `#define ATCA_COUNTER_MATCH_KEY_MASK (0x0Fu << ATCA_COUNTER_MATCH_KEY_SHIFT)`
- `#define ATCA_COUNTER_MATCH_KEY(v) (ATCA_COUNTER_MATCH_KEY_MASK & (v << ATCA_COUNTER_MATCH_KEY_SHIFT))`
- `#define ATCA_CHIP_MODE_I2C_EXTRA_SHIFT (0)`
- `#define ATCA_CHIP_MODE_I2C_EXTRA_MASK (0x01u << ATCA_CHIP_MODE_I2C_EXTRA_SHIFT)`
- `#define ATCA_CHIP_MODE_TTL_EN_SHIFT (1)`
- `#define ATCA_CHIP_MODE_TTL_EN_MASK (0x01u << ATCA_CHIP_MODE_TTL_EN_SHIFT)`
- `#define ATCA_CHIP_MODE_WDG_LONG_SHIFT (2)`
- `#define ATCA_CHIP_MODE_WDG_LONG_MASK (0x01u << ATCA_CHIP_MODE_WDG_LONG_SHIFT)`
- `#define ATCA_CHIP_MODE_CLK_DIV_SHIFT (3)`
- `#define ATCA_CHIP_MODE_CLK_DIV_MASK (0x1Fu << ATCA_CHIP_MODE_CLK_DIV_SHIFT)`
- `#define ATCA_CHIP_MODE_CLK_DIV(v) (ATCA_CHIP_MODE_CLK_DIV_MASK & (v << ATCA_CHIP_MODE_CLK_DIV_SHIFT))`
- `#define ATCA_SLOT_CONFIG_READKEY_SHIFT (0)`
- `#define ATCA_SLOT_CONFIG_READKEY_MASK (0x0Fu << ATCA_SLOT_CONFIG_READKEY_SHIFT)`
- `#define ATCA_SLOT_CONFIG_READKEY(v) (ATCA_SLOT_CONFIG_READKEY_MASK & (v << ATCA_SLOT_CONFIG_READKEY_SHIFT))`
- `#define ATCA_SLOT_CONFIG_NOMAC_SHIFT (4)`
- `#define ATCA_SLOT_CONFIG_NOMAC_MASK (0x01u << ATCA_SLOT_CONFIG_NOMAC_SHIFT)`
- `#define ATCA_SLOT_CONFIG_LIMITED_USE_SHIFT (5)`
- `#define ATCA_SLOT_CONFIG_LIMITED_USE_MASK (0x01u << ATCA_SLOT_CONFIG_LIMITED_USE_SHIFT)`
- `#define ATCA_SLOT_CONFIG_ENC_READ_SHIFT (6)`
- `#define ATCA_SLOT_CONFIG_ENC_READ_MASK (0x01u << ATCA_SLOT_CONFIG_ENC_READ_SHIFT)`
- `#define ATCA_SLOT_CONFIG_IS_SECRET_SHIFT (7)`
- `#define ATCA_SLOT_CONFIG_IS_SECRET_MASK (0x01u << ATCA_SLOT_CONFIG_IS_SECRET_SHIFT)`
- `#define ATCA_SLOT_CONFIG_WRITE_KEY_SHIFT (8)`
- `#define ATCA_SLOT_CONFIG_WRITE_KEY_MASK (((uint32_t)0x0Fu << ATCA_SLOT_CONFIG_WRITE_KEY_SHIFT))`
- `#define ATCA_SLOT_CONFIG_WRITE_KEY(v) (ATCA_SLOT_CONFIG_WRITE_KEY_MASK & (v << ATCA_SLOT_CONFIG_WRITE_KEY_SHIFT))`
- `#define ATCA_SLOT_CONFIG_WRITE_CONFIG_SHIFT (12)`
- `#define ATCA_SLOT_CONFIG_WRITE_CONFIG_MASK (((uint32_t)0x0Fu << ATCA_SLOT_CONFIG_WRITE_CONFIG_SHIFT))`
- `#define ATCA_SLOT_CONFIG_WRITE_CONFIG(v) ((ATCA_SLOT_CONFIG_WRITE_CONFIG_MASK & ((uint32_t)v) << ATCA_SLOT_CONFIG_WRITE_CONFIG_SHIFT))`
- `#define ATCA_SLOT_CONFIG_EXT_SIG_SHIFT (0)`
- `#define ATCA_SLOT_CONFIG_EXT_SIG_MASK (0x01u << ATCA_SLOT_CONFIG_EXT_SIG_SHIFT)`
- `#define ATCA_SLOT_CONFIG_INT_SIG_SHIFT (1)`
- `#define ATCA_SLOT_CONFIG_INT_SIG_MASK (0x01u << ATCA_SLOT_CONFIG_INT_SIG_SHIFT)`
- `#define ATCA_SLOT_CONFIG_ECDH_SHIFT (2)`
- `#define ATCA_SLOT_CONFIG_ECDH_MASK (0x01u << ATCA_SLOT_CONFIG_ECDH_SHIFT)`
- `#define ATCA_SLOT_CONFIG_WRITE_ECDH_SHIFT (3)`

- `#define ATCA_SLOT_CONFIG_WRITE_ECDH_MASK (0x01u << ATCA_SLOT_CONFIG_WRITE_↵ ECDH_SHIFT)`
- `#define ATCA_SLOT_CONFIG_GEN_KEY_SHIFT (8)`
- `#define ATCA_SLOT_CONFIG_GEN_KEY_MASK (0x01u << ATCA_SLOT_CONFIG_GEN_KEY_SHIFT)`
- `#define ATCA_SLOT_CONFIG_PRIV_WRITE_SHIFT (9)`
- `#define ATCA_SLOT_CONFIG_PRIV_WRITE_MASK (0x01u << ATCA_SLOT_CONFIG_PRIV_WRITE_↵ _SHIFT)`
- `#define ATCA_USE_LOCK_ENABLE_SHIFT (0)`
- `#define ATCA_USE_LOCK_ENABLE_MASK (0x0Fu << ATCA_USE_LOCK_ENABLE_SHIFT)`
- `#define ATCA_USE_LOCK_KEY_SHIFT (4)`
- `#define ATCA_USE_LOCK_KEY_MASK (0x0Fu << ATCA_USE_LOCK_KEY_SHIFT)`
- `#define ATCA_VOL_KEY_PERM_SLOT_SHIFT (0)`
- `#define ATCA_VOL_KEY_PERM_SLOT_MASK (0x0Fu << ATCA_VOL_KEY_PERM_SLOT_SHIFT)`
- `#define ATCA_VOL_KEY_PERM_SLOT(v) (ATCA_VOL_KEY_PERM_SLOT_MASK & (v << ATCA_VOL_↵ _KEY_PERM_SLOT_SHIFT))`
- `#define ATCA_VOL_KEY_PERM_EN_SHIFT (7)`
- `#define ATCA_VOL_KEY_PERM_EN_MASK (0x01u << ATCA_VOL_KEY_PERM_EN_SHIFT)`
- `#define ATCA_SECURE_BOOT_MODE_SHIFT (0)`
- `#define ATCA_SECURE_BOOT_MODE_MASK (0x03u << ATCA_SECURE_BOOT_MODE_SHIFT)`
- `#define ATCA_SECURE_BOOT_MODE(v) (ATCA_SECURE_BOOT_MODE_MASK & (v << ATCA_↵ SECURE_BOOT_MODE_SHIFT))`
- `#define ATCA_SECURE_BOOT_PERSIST_EN_SHIFT (3)`
- `#define ATCA_SECURE_BOOT_PERSIST_EN_MASK (0x01u << ATCA_SECURE_BOOT_PERSIST_↵ EN_SHIFT)`
- `#define ATCA_SECURE_BOOT_RAND_NONCE_SHIFT (4)`
- `#define ATCA_SECURE_BOOT_RAND_NONCE_MASK (0x01u << ATCA_SECURE_BOOT_RAND_↵ NONCE_SHIFT)`
- `#define ATCA_SECURE_BOOT_DIGEST_SHIFT (8)`
- `#define ATCA_SECURE_BOOT_DIGEST_MASK (0x0Fu << ATCA_SECURE_BOOT_DIGEST_SHIFT)`
- `#define ATCA_SECURE_BOOT_DIGEST(v) (ATCA_SECURE_BOOT_DIGEST_MASK & (v << ATCA_↵ SECURE_BOOT_DIGEST_SHIFT))`
- `#define ATCA_SECURE_BOOT_PUB_KEY_SHIFT (12)`
- `#define ATCA_SECURE_BOOT_PUB_KEY_MASK (0x0Fu << ATCA_SECURE_BOOT_PUB_KEY_↵ SHIFT)`
- `#define ATCA_SECURE_BOOT_PUB_KEY(v) (ATCA_SECURE_BOOT_PUB_KEY_MASK & (v << ATCA_SECURE_BOOT_PUB_KEY_SHIFT))`
- `#define ATCA_SLOT_LOCKED(v) ((0x01 << v) & 0xFFFFu)`
- `#define ATCA_CHIP_OPT_POST_EN_SHIFT (0)`
- `#define ATCA_CHIP_OPT_POST_EN_MASK (0x01u << ATCA_CHIP_OPT_POST_EN_SHIFT)`
- `#define ATCA_CHIP_OPT_IO_PROT_EN_SHIFT (1)`
- `#define ATCA_CHIP_OPT_IO_PROT_EN_MASK (0x01u << ATCA_CHIP_OPT_IO_PROT_EN_SHIFT)`
- `#define ATCA_CHIP_OPT_KDF_AES_EN_SHIFT (2)`
- `#define ATCA_CHIP_OPT_KDF_AES_EN_MASK (0x01u << ATCA_CHIP_OPT_KDF_AES_EN_SHIFT)`
- `#define ATCA_CHIP_OPT_ECDH_PROT_SHIFT (8)`
- `#define ATCA_CHIP_OPT_ECDH_PROT_MASK (0x03u << ATCA_CHIP_OPT_ECDH_PROT_SHIFT)`
- `#define ATCA_CHIP_OPT_ECDH_PROT(v) (ATCA_CHIP_OPT_ECDH_PROT_MASK & (v << ATCA_↵ CHIP_OPT_ECDH_PROT_SHIFT))`
- `#define ATCA_CHIP_OPT_KDF_PROT_SHIFT (10)`
- `#define ATCA_CHIP_OPT_KDF_PROT_MASK (0x03u << ATCA_CHIP_OPT_KDF_PROT_SHIFT)`
- `#define ATCA_CHIP_OPT_KDF_PROT(v) (ATCA_CHIP_OPT_KDF_PROT_MASK & (v << ATCA_CHIP_↵ _OPT_KDF_PROT_SHIFT))`
- `#define ATCA_CHIP_OPT_IO_PROT_KEY_SHIFT (12)`
- `#define ATCA_CHIP_OPT_IO_PROT_KEY_MASK ((uint16_t)0x0Fu << ATCA_CHIP_OPT_IO_PROT_↵ KEY_SHIFT)`
- `#define ATCA_CHIP_OPT_IO_PROT_KEY(v) (ATCA_CHIP_OPT_IO_PROT_KEY_MASK & (v << ATCA_↵ _CHIP_OPT_IO_PROT_KEY_SHIFT))`

- `#define ATCA_KEY_CONFIG_OFFSET(x) (96UL + (x) * 2u)`
- `#define ATCA_KEY_CONFIG_PRIVATE_SHIFT (0)`
- `#define ATCA_KEY_CONFIG_PRIVATE_MASK (0x01u << ATCA_KEY_CONFIG_PRIVATE_SHIFT)`
- `#define ATCA_KEY_CONFIG_PUB_INFO_SHIFT (1)`
- `#define ATCA_KEY_CONFIG_PUB_INFO_MASK (0x01u << ATCA_KEY_CONFIG_PUB_INFO_SHIFT)`
- `#define ATCA_KEY_CONFIG_KEY_TYPE_SHIFT (2)`
- `#define ATCA_KEY_CONFIG_KEY_TYPE_MASK ((0x07u << ATCA_KEY_CONFIG_KEY_TYPE_SHIFT))`
- `#define ATCA_KEY_CONFIG_KEY_TYPE(v) ((ATCA_KEY_CONFIG_KEY_TYPE_MASK & ((v) << ATCA_KEY_CONFIG_KEY_TYPE_SHIFT)))`
- `#define ATCA_KEY_CONFIG_LOCKABLE_SHIFT (5)`
- `#define ATCA_KEY_CONFIG_LOCKABLE_MASK (0x01u << ATCA_KEY_CONFIG_LOCKABLE_SHIFT)`
- `#define ATCA_KEY_CONFIG_REQ_RANDOM_SHIFT (6)`
- `#define ATCA_KEY_CONFIG_REQ_RANDOM_MASK (0x01u << ATCA_KEY_CONFIG_REQ_RANDOM_SHIFT)`
- `#define ATCA_KEY_CONFIG_REQ_AUTH_SHIFT (7)`
- `#define ATCA_KEY_CONFIG_REQ_AUTH_MASK (0x01u << ATCA_KEY_CONFIG_REQ_AUTH_SHIFT)`
- `#define ATCA_KEY_CONFIG_AUTH_KEY_SHIFT (8)`
- `#define ATCA_KEY_CONFIG_AUTH_KEY_MASK (0x0Fu << ATCA_KEY_CONFIG_AUTH_KEY_SHIFT)`
- `#define ATCA_KEY_CONFIG_AUTH_KEY(v) (ATCA_KEY_CONFIG_AUTH_KEY_MASK & (v << ATCA_KEY_CONFIG_AUTH_KEY_SHIFT))`
- `#define ATCA_KEY_CONFIG_PERSIST_DIS_SHIFT (12)`
- `#define ATCA_KEY_CONFIG_PERSIST_DIS_MASK (0x01u << ATCA_KEY_CONFIG_PERSIST_DIS_SHIFT)`
- `#define ATCA_KEY_CONFIG_RFU_SHIFT (13)`
- `#define ATCA_KEY_CONFIG_RFU_MASK (0x01u << ATCA_KEY_CONFIG_RFU_SHIFT)`
- `#define ATCA_KEY_CONFIG_X509_ID_SHIFT (14)`
- `#define ATCA_KEY_CONFIG_X509_ID_MASK (0x03u << ATCA_KEY_CONFIG_X509_ID_SHIFT)`
- `#define ATCA_KEY_CONFIG_X509_ID(v) (ATCA_KEY_CONFIG_X509_ID_MASK & (v << ATCA_KEY_CONFIG_X509_ID_SHIFT))`

## Typedefs

- `typedef struct ATCA_PACKED atsha204a_config_s atsha204a_config_t`
- `typedef struct ATCA_PACKED atecc508a_config_s atecc508a_config_t`
- `typedef struct ATCA_PACKED atecc608_config_s atecc608_config_t`

## 22.84.1 Detailed Description

Microchip Crypto Auth Device Data.

### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.85 calib\_ecdh.c File Reference

CryptoAuthLib Basic API methods for ECDH command.

```
#include "cryptoauthlib.h"
#include "host/atca_host.h"
```

### 22.85.1 Detailed Description

CryptoAuthLib Basic API methods for ECDH command.

The ECDH command implements the Elliptic Curve Diffie-Hellman algorithm to combine an internal private key with an external public key to calculate a shared secret.

#### Note

List of devices that support this command - ATECC508A, ATECC608A/B. There are differences in the modes that they support. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.86 calib\_execution.c File Reference

Implements an execution handler that executes a given command on a device and returns the results.

```
#include "cryptoauthlib.h"
```

### Functions

- ATCA\_STATUS [calib\\_get\\_execution\\_time](#) (uint8\_t opcode, [ATCADevice](#) device)  
*return the typical execution time for the given command*
- ATCA\_STATUS [calib\\_execute\\_send](#) ([ATCADevice](#) device, uint8\_t word\_address, uint8\_t \*txdata, uint16\_t txlength)
- ATCA\_STATUS [calib\\_execute\\_receive](#) ([ATCADevice](#) device, uint8\_t device\_address, uint8\_t \*rxdata, uint16\_t \*rxlength)
- ATCA\_STATUS [calib\\_execute\\_command](#) ([ATCAPacket](#) \*packet, [ATCADevice](#) device)  
*Wakes up device, sends the packet, waits for command completion, receives response, and puts the device into the idle state.*

### 22.86.1 Detailed Description

Implements an execution handler that executes a given command on a device and returns the results.

This implementation wraps Polling and No polling (simple wait) schemes into a single method and use it across the library. Polling is used by default, however, by defining the ATCA\_NO\_POLL symbol the code will instead wait an estimated max execution time before requesting the result.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.86.2 Function Documentation

#### 22.86.2.1 calib\_execute\_command()

```
ATCA_STATUS calib_execute_command (  
    ATCAPacket * packet,  
    ATCADevice device )
```

Wakes up device, sends the packet, waits for command completion, receives response, and puts the device into the idle state.



Parameters

in, out	<i>packet</i>	As input, the packet to be sent. As output, the data buffer in the packet structure will contain the response.
in	<i>device</i>	CryptoAuthentication device to send the command to.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.86.2.2 calib\_get\_execution\_time()

```
ATCA_STATUS calib_get_execution_time (
    uint8_t opcode,
    ATCADevice device )
```

return the typical execution time for the given command

Parameters

in	<i>opcode</i>	Opcode value of the command
in	<i>ca_cmd</i>	Command object for which the execution times are associated

Returns

ATCA\_SUCCESS

22.87 calib\_execution.h File Reference

Defines an execution handler that executes a given command on a device and returns the results.

```
#include "atca_status.h"
#include "calib_command.h"
#include "atca_device.h"
#include "atca_config.h"
```

Data Structures

- struct `device_execution_time_t`  
*Structure to hold the device execution time and the opcode for the corresponding command.*

## Macros

- #define **ATCA\_UNSUPPORTED\_CMD** ((uint16\_t)0xFFFF)
- #define **CALIB\_SWI\_FLAG\_WAKE** 0x00  
*flag preceding a command*
- #define **CALIB\_SWI\_FLAG\_CMD** 0x77  
*flag preceding a command*
- #define **CALIB\_SWI\_FLAG\_TX** 0x88  
*flag requesting a response*
- #define **CALIB\_SWI\_FLAG\_IDLE** 0xBB  
*flag requesting to go into Idle mode*
- #define **CALIB\_SWI\_FLAG\_SLEEP** 0xCC  
*flag requesting to go into Sleep mode*

## Functions

- ATCA\_STATUS [calib\\_get\\_execution\\_time](#) (uint8\_t opcode, [ATCADevice](#) device)  
*return the typical execution time for the given command*
- ATCA\_STATUS **calib\_execute\_send** ([ATCADevice](#) device, uint8\_t word\_address, uint8\_t \*txdata, uint16\_t txlength)
- ATCA\_STATUS **calib\_execute\_receive** ([ATCADevice](#) device, uint8\_t device\_address, uint8\_t \*rxdata, uint16\_t \*rxlength)
- ATCA\_STATUS [calib\\_execute\\_command](#) ([ATCAPacket](#) \*packet, [ATCADevice](#) device)  
*Wakes up device, sends the packet, waits for command completion, receives response, and puts the device into the idle state.*

### 22.87.1 Detailed Description

Defines an execution handler that executes a given command on a device and returns the results.

The basic flow is to wake the device, send the command, wait/poll for completion, and finally receives the response from the device and does basic checks before returning to caller.

This handler supports the ATSHA and ATECC device family.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.87.2 Function Documentation

#### 22.87.2.1 calib\_execute\_command()

```
ATCA_STATUS calib_execute_command (  
    ATCAPacket * packet,  
    ATCADevice device )
```

Wakes up device, sends the packet, waits for command completion, receives response, and puts the device into the idle state.

Parameters

<code>in, out</code>	<code>packet</code>	As input, the packet to be sent. As output, the data buffer in the packet structure will contain the response.
<code>in</code>	<code>device</code>	CryptoAuthentication device to send the command to.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 22.87.2.2 calib\_get\_execution\_time()

```
ATCA_STATUS calib_get_execution_time (
    uint8_t opcode,
    ATCADevice device )
```

return the typical execution time for the given command

Parameters

<code>in</code>	<code>opcode</code>	Opcode value of the command
<code>in</code>	<code>ca_cmd</code>	Command object for which the execution times are associated

Returns

ATCA\_SUCCESS

## 22.88 calib\_gendig.c File Reference

CryptoAuthLib Basic API methods for GenDig command.

```
#include "cryptoauthlib.h"
```

### 22.88.1 Detailed Description

CryptoAuthLib Basic API methods for GenDig command.

The GenDig command uses SHA-256 to combine a stored value with the contents of TempKey, which must have been valid prior to the execution of this command.

Note

List of devices that support this command - ATSHA204A, ATECC108A, ATECC508A, and ATECC608A/B. There are differences in the modes that they support. Refer to device datasheets for full details.

Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.89 calib\_genkey.c File Reference

CryptoAuthLib Basic API methods for GenKey command.

```
#include "cryptoauthlib.h"
```

### 22.89.1 Detailed Description

CryptoAuthLib Basic API methods for GenKey command.

The GenKey command is used for creating ECC private keys, generating ECC public keys, and for digest calculations involving public keys.

#### Note

List of devices that support this command - ATECC108A, ATECC508A, ATECC608A/B. There are differences in the modes that they support. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.90 calib\_helpers.c File Reference

CryptoAuthLib Basic API - Helper Functions to.

```
#include "cryptoauthlib.h"
```

### Functions

- ATCA\_STATUS [calib\\_ca2\\_is\\_config\\_locked](#) ([ATCADevice](#) device, bool \*is\_locked)  
*Executes Read command, which reads the configuration zone to see if the specified slot is locked.*
- ATCA\_STATUS [calib\\_ca2\\_is\\_data\\_locked](#) ([ATCADevice](#) device, bool \*is\_locked)  
*Use Info command to check ECC204 Data zone lock status.*
- ATCA\_STATUS [calib\\_ca2\\_is\\_locked](#) ([ATCADevice](#) device, uint8\_t zone, bool \*is\_locked)  
*Use Info command to check config/data is locked or not.*
- ATCADeviceType [calib\\_get\\_devicetype](#) (uint8\_t revision[4])  
*Parse the revision field to get the device type.*
- ATCADeviceType [calib\\_get\\_devicetype\\_with\\_device\\_id](#) (uint8\_t device\_id, uint8\_t device\_revision)

### 22.90.1 Detailed Description

CryptoAuthLib Basic API - Helper Functions to.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.91 calib\_hmac.c File Reference

CryptoAuthLib Basic API methods for HMAC command.

```
#include "cryptoauthlib.h"
```

### 22.91.1 Detailed Description

CryptoAuthLib Basic API methods for HMAC command.

The HMAC command computes an HMAC/SHA-256 digest using a key stored in the device over a challenge stored in the TempKey register, and/or other information stored within the device.

#### Note

List of devices that support this command - ATSHA204A, ATECC108A, and ATECC508A . There are differences in the modes that they support. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.92 calib\_info.c File Reference

CryptoAuthLib Basic API methods for Info command.

```
#include "cryptoauthlib.h"
```

### Functions

- ATCA\_STATUS [calib\\_info\\_base](#) (ATCADevice device, uint8\_t mode, uint16\_t param2, uint8\_t \*out\_data)  
*Issues an Info command, which return internal device information and can control GPIO and the persistent latch.*
- ATCA\_STATUS [calib\\_info](#) (ATCADevice device, uint8\_t \*revision)  
*Use the Info command to get the device revision (DevRev).*
- ATCA\_STATUS [calib\\_info\\_privkey\\_valid](#) (ATCADevice device, uint16\_t key\_id, uint8\_t \*is\_valid)  
*Use Info command to check ECC Private key stored in key slot is valid or not.*
- ATCA\_STATUS [calib\\_info\\_lock\\_status](#) (ATCADevice device, uint16\_t param2, uint8\_t \*is\_locked)  
*Use Info command to ECC204,TA010 config/data zone lock status.*
- ATCA\_STATUS [calib\\_info\\_chip\\_status](#) (ATCADevice device, uint8\_t \*chip\_status)  
*Use Info command to get ECC204,TA010,SHA10x chip status.*

### 22.92.1 Detailed Description

CryptoAuthLib Basic API methods for Info command.

Info command returns a variety of static and dynamic information about the device and its state. Also is used to control the GPIO pin and the persistent latch.

#### Note

The ATSHA204A refers to this command as DevRev instead of Info, however, the OpCode and operation is the same.

List of devices that support this command - ATSHA204A, ATECC108A, ATECC508A & ATECC608A/B. There are differences in the modes that they support. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.93 calib\_kdf.c File Reference

CryptoAuthLib Basic API methods for KDF command.

```
#include "cryptoauthlib.h"
```

### 22.93.1 Detailed Description

CryptoAuthLib Basic API methods for KDF command.

The KDF command implements one of a number of Key Derivation Functions (KDF). Generally this function combines a source key with an input string and creates a result key/digest/array. Three algorithms are currently supported: PRF, HKDF and AES.

#### Note

List of devices that support this command - ATECC608A/B. Refer to device datasheet for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.94 calib\_lock.c File Reference

CryptoAuthLib Basic API methods for Lock command.

```
#include "cryptoauthlib.h"
```

### 22.94.1 Detailed Description

CryptoAuthLib Basic API methods for Lock command.

The Lock command prevents future modifications of the Configuration zone, enables configured policies for Data and OTP zones, and can render individual slots read-only regardless of configuration.

#### Note

List of devices that support this command - ATSHA204A, ATECC108A, ATECC508A, ATECC608A/B. There are differences in the modes that they support. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.95 calib\_mac.c File Reference

CryptoAuthLib Basic API methods for MAC command.

```
#include "cryptoauthlib.h"
```

### 22.95.1 Detailed Description

CryptoAuthLib Basic API methods for MAC command.

The MAC command computes a SHA-256 digest of a key stored in the device, a challenge, and other information on the device. The output of this command is the digest of this message.

#### Note

List of devices that support this command - ATSHA204A, ATECC108A, ATECC508A, and ATECC608A/B. There are differences in the modes that they support. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.96 calib\_nonce.c File Reference

CryptoAuthLib Basic API methods for Nonce command.

```
#include "cryptoauthlib.h"
```

### 22.96.1 Detailed Description

CryptoAuthLib Basic API methods for Nonce command.

The Nonce command generates a nonce for use by a subsequent commands of the device by combining an internally generated random number with an input value from the system.

#### Note

List of devices that support this command - ATSHA204A, ATECC108A, ATECC508A, and ATECC608A/B. There are differences in the modes that they support. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.97 calib\_privwrite.c File Reference

CryptoAuthLib Basic API methods for PrivWrite command.

```
#include "cryptoauthlib.h"
```

### 22.97.1 Detailed Description

CryptoAuthLib Basic API methods for PrivWrite command.

The PrivWrite command is used to write externally generated ECC private keys into the device.

#### Note

List of devices that support this command - ATECC108A, ATECC508A, and ATECC608A/B. There are differences in the modes that they support. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.98 calib\_random.c File Reference

CryptoAuthLib Basic API methods for Random command.

```
#include "cryptoauthlib.h"
```



### 22.98.1 Detailed Description

CryptoAuthLib Basic API methods for Random command.

The Random command generates a random number for use by the system.

#### Note

List of devices that support this command - ATSHA204A, ATECC108A, ATECC508A, ATECC608A/B. There are differences in the modes that they support. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.99 calib\_read.c File Reference

CryptoAuthLib Basic API methods for Read command.

```
#include "cryptoauthlib.h"
```

### 22.99.1 Detailed Description

CryptoAuthLib Basic API methods for Read command.

The Read command reads words either 4-byte words or 32-byte blocks from one of the memory zones of the device. The data may optionally be encrypted before being returned to the system.

#### Note

List of devices that support this command - ATSHA204A, ATECC108A, ATECC508A, ATECC608A/B. There are differences in the modes that they support. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.100 calib\_secureboot.c File Reference

CryptoAuthLib Basic API methods for SecureBoot command.

```
#include "cryptoauthlib.h"
```

### 22.100.1 Detailed Description

CryptoAuthLib Basic API methods for SecureBoot command.

The SecureBoot command provides support for secure boot of an external MCU or MPU.

#### Note

List of devices that support this command - ATECC608A/B. Refer to device datasheet for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.101 calib\_selftest.c File Reference

CryptoAuthLib Basic API methods for SelfTest command.

```
#include "cryptoauthlib.h"
```

### 22.101.1 Detailed Description

CryptoAuthLib Basic API methods for SelfTest command.

The SelfTest command performs a test of one or more of the cryptographic engines within the device.

#### Note

List of devices that support this command - ATECC608A/B. Refer to device datasheet for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.102 calib\_sha.c File Reference

CryptoAuthLib Basic API methods for SHA command.

```
#include "cryptoauthlib.h"
```

### 22.102.1 Detailed Description

CryptoAuthLib Basic API methods for SHA command.

The SHA command Computes a SHA-256 or HMAC/SHA digest for general purpose use by the host system.

#### Note

List of devices that support this command - ATSHA204A, ATECC108A, ATECC508A, and ATECC608A/B. There are differences in the modes that they support. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.103 calib\_sign.c File Reference

CryptoAuthLib Basic API methods for Sign command.

```
#include "cryptoauthlib.h"
```

### 22.103.1 Detailed Description

CryptoAuthLib Basic API methods for Sign command.

The Sign command generates a signature using the private key in slot with ECDSA algorithm.

#### Note

List of devices that support this command - ATECC108A, ATECC508A, and ATECC608A/B. There are differences in the modes that they support. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.104 calib\_updateextra.c File Reference

CryptoAuthLib Basic API methods for UpdateExtra command.

```
#include "cryptoauthlib.h"
```

### 22.104.1 Detailed Description

CryptoAuthLib Basic API methods for UpdateExtra command.

The UpdateExtra command is used to update the values of the two extra bytes within the Configuration zone after the Configuration zone has been locked.

#### Note

List of devices that support this command - ATSHA204A, ATECC108A, ATECC508A, and ATECC608A/B. There are differences in the modes that they support. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.105 calib\_verify.c File Reference

CryptoAuthLib Basic API methods for Verify command.

```
#include "cryptoauthlib.h"
#include "host/atca_host.h"
```

### 22.105.1 Detailed Description

CryptoAuthLib Basic API methods for Verify command.

The Verify command takes an ECDSA [R,S] signature and verifies that it is correctly generated given an input message digest and public key.

#### Note

List of devices that support this command - ATECC108A, ATECC508A, and ATECC608A/B. There are differences in the modes that they support. Refer to device datasheet for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.106 calib\_write.c File Reference

CryptoAuthLib Basic API methods for Write command.

```
#include "cryptoauthlib.h"
#include "host/atca_host.h"
```

### 22.106.1 Detailed Description

CryptoAuthLib Basic API methods for Write command.

The Write command writes either one 4-byte word or a 32-byte block to one of the EEPROM zones on the device. Depending upon the value of the WriteConfig byte for a slot, the data may be required to be encrypted by the system prior to being sent to the device

#### Note

List of devices that support this command - ATSHA204A, ATECC108A, ATECC508A, and ATECC608A/B. There are differences in the modes that they support. Refer to device datasheets for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.107 atca\_crypto\_hw\_aes.h File Reference

AES CTR, CBC & CMAC structure definitions.

```
#include "cryptoauthlib.h"
#include "crypto_hw_config_check.h"
```

### 22.107.1 Detailed Description

AES CTR, CBC & CMAC structure definitions.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.108 atca\_crypto\_hw\_aes\_cbc.c File Reference

CryptoAuthLib Basic API methods for AES CBC mode.

```
#include "cryptoauthlib.h"
#include "atca_crypto_hw_aes.h"
```

### 22.108.1 Detailed Description

CryptoAuthLib Basic API methods for AES CBC mode.

The AES command supports 128-bit AES encryption or decryption of small messages or data packets in ECB mode.

#### Note

List of devices that support this command - ATECC608A, ATECC608B, & TA10x. Refer to device datasheet for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.109 atca\_crypto\_hw\_aes\_cbcmac.c File Reference

CryptoAuthLib Basic API methods for AES CBC\_MAC mode.

```
#include "cryptoauthlib.h"
#include "crypto_hw_config_check.h"
```

### 22.109.1 Detailed Description

CryptoAuthLib Basic API methods for AES CBC\_MAC mode.

The AES command supports 128-bit AES encryption or decryption of small messages or data packets in ECB mode. Also can perform GFM (Galois Field Multiply) calculation in support of AES-GCM.

#### Note

List of devices that support this command - ATECC608A. Refer to device datasheet for full details.

#### Copyright

(c) 2015-2018 Microchip Technology Inc. and its subsidiaries.

## 22.110 atca\_crypto\_hw\_aes\_ccm.c File Reference

CryptoAuthLib Basic API methods for AES CCM mode.

```
#include "cryptoauthlib.h"
```

### 22.110.1 Detailed Description

CryptoAuthLib Basic API methods for AES CCM mode.

The AES command supports 128-bit AES encryption or decryption of small messages or data packets in ECB mode. CCM mode provides security and authenticity to the message being processed.

#### Note

List of devices that support this command - ATECC608A. Refer to device datasheet for full details.

#### Copyright

(c) 2015-2018 Microchip Technology Inc. and its subsidiaries.

## 22.111 atca\_crypto\_hw\_aes\_cmac.c File Reference

CryptoAuthLib Basic API methods for AES CBC\_MAC mode.

```
#include "cryptoauthlib.h"
#include "atca_crypto_hw_aes.h"
```

### 22.111.1 Detailed Description

CryptoAuthLib Basic API methods for AES CBC\_MAC mode.

The AES command supports 128-bit AES encryption or decryption of small messages or data packets in ECB mode.

#### Note

List of devices that support this command - ATECC608A, ATECC608B, & TA10x. Refer to device datasheet for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.112 atca\_crypto\_hw\_aes\_ctr.c File Reference

CryptoAuthLib Basic API methods for AES CTR mode.

```
#include "cryptoauthlib.h"
#include "atca_crypto_hw_aes.h"
```

### 22.112.1 Detailed Description

CryptoAuthLib Basic API methods for AES CTR mode.

The AES command supports 128-bit AES encryption or decryption of small messages or data packets in ECB mode.

#### Note

List of devices that support this command - ATECC608A, ATECC608B, & TA100. Refer to device datasheet for full details.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.113 atca\_crypto\_pad.c File Reference

Implementation of PKCS7 Padding for block encryption.

```
#include "cryptoauthlib.h"  
#include "atca_crypto_sw.h"
```

### 22.113.1 Detailed Description

Implementation of PKCS7 Padding for block encryption.

#### Copyright

(c) 2022 Microchip Technology Inc. and its subsidiaries.

## 22.114 atca\_crypto\_pbkdf2.c File Reference

Implementation of the PBKDF2 algorithm for use in generating password hashes.

```
#include "cryptoauthlib.h"  
#include "cal_internal.h"
```

### 22.114.1 Detailed Description

Implementation of the PBKDF2 algorithm for use in generating password hashes.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.



## 22.115 atca\_crypto\_sw.h File Reference

Common defines for CryptoAuthLib software crypto wrappers.

```
#include <stdint.h>
#include <stdlib.h>
#include "crypto/crypto_sw_config_check.h"
#include "atca_status.h"
```

### Macros

- #define **ATCA\_SHA1\_DIGEST\_SIZE** (20U)
- #define **ATCA\_SHA2\_256\_DIGEST\_SIZE** (32U)
- #define **ATCA\_SHA2\_256\_BLOCK\_SIZE** (64U)

### 22.115.1 Detailed Description

Common defines for CryptoAuthLib software crypto wrappers.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.116 atca\_crypto\_sw\_aes\_gcm.c File Reference

Common Wrapper for host side AES-GCM implementations that feature update APIs rather than an all at once implementation.

```
#include "atca_crypto_sw.h"
```

### 22.116.1 Detailed Description

Common Wrapper for host side AES-GCM implementations that feature update APIs rather than an all at once implementation.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.117 atca\_crypto\_sw\_sha1.c File Reference

Wrapper API for SHA 1 routines.

```
#include "atca_crypto_sw_sha1.h"
#include "hashes/sha1_routines.h"
#include "cryptoauthlib.h"
#include "cal_internal.h"
```

### 22.117.1 Detailed Description

Wrapper API for SHA 1 routines.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.118 atca\_crypto\_sw\_sha1.h File Reference

Wrapper API for SHA 1 routines.

```
#include "atca_crypto_sw.h"
#include <stddef.h>
#include <stdint.h>
```

### Functions

- ATCA\_STATUS **atcac\_sw\_sha1** (const uint8\_t \*data, size\_t data\_size, uint8\_t digest[(20U)])

### 22.118.1 Detailed Description

Wrapper API for SHA 1 routines.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.119 atca\_crypto\_sw\_sha2.c File Reference

Wrapper API for software SHA 256 routines.

```
#include "cryptoauthlib.h"
#include "atca_crypto_sw_sha2.h"
#include "cal_internal.h"
```

### 22.119.1 Detailed Description

Wrapper API for software SHA 256 routines.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.120 atca\_crypto\_sw\_sha2.h File Reference

Wrapper API for software SHA 256 routines.

```
#include "atca_crypto_sw.h"
#include <stddef.h>
#include <stdint.h>
```

### Functions

- ATCA\_STATUS **atcac\_sw\_sha2\_256** (const uint8\_t \*data, size\_t data\_size, uint8\_t digest[(32U)])
- ATCA\_STATUS **atcac\_sha256\_hmac\_ctr\_iteration** (struct [atcac\\_hmac\\_ctx](#) \*ctx, uint8\_t iteration, uint16\_t length, const uint8\_t \*label, size\_t label\_len, const uint8\_t \*data, size\_t data\_len, uint8\_t digest[(32U)])
- ATCA\_STATUS **atcac\_sha256\_hmac\_counter** (uint8\_t \*key, size\_t key\_len, const uint8\_t \*label, size\_t label\_len, const uint8\_t \*data, size\_t data\_len, uint8\_t \*digest, size\_t diglen)

### 22.120.1 Detailed Description

Wrapper API for software SHA 256 routines.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.121 crypto\_hw\_config\_check.h File Reference

Consistency checks for configuration options.

```
#include "atca_config_check.h"
#include "calib/calib_config_check.h"
#include "talib/talib_config_check.h"
```

### Macros

- #define [ATCAB\\_AES\\_EXTRAS\\_EN](#) (CALIB\_AES\_EN || TALIB\_AES\_EN)
- #define **ATCAB\_AES\_RANDOM\_IV\_EN** (ATCA\_HOSTLIB\_EN || CALIB\_RANDOM\_EN || TALIB\_RANDOM\_EN)
- #define [ATCAB\\_AES\\_UPDATE\\_EN](#) [ATCAB\\_AES\\_EXTRAS\\_EN](#)
- #define [ATCAB\\_AES\\_CBC\\_ENCRYPT\\_EN](#) [ATCAB\\_AES\\_EXTRAS\\_EN](#)
- #define [ATCAB\\_AES\\_CBC\\_DECRYPT\\_EN](#) [ATCAB\\_AES\\_EXTRAS\\_EN](#)
- #define **ATCAB\_AES\_CBC\_UPDATE\_EN** [ATCAB\\_AES\\_UPDATE\\_EN](#)
- #define [ATCAB\\_AES\\_CBCMAC\\_EN](#) [ATCAB\\_AES\\_CBC\\_ENCRYPT\\_EN](#)
- #define [ATCAB\\_AES\\_CTR\\_EN](#) [ATCAB\\_AES\\_EXTRAS\\_EN](#)
- #define [ATCAB\\_AES\\_CTR\\_RAND\\_IV\\_EN](#) ([ATCAB\\_AES\\_CTR\\_EN](#) && [ATCAB\\_AES\\_RANDOM\\_IV\\_EN](#))
- #define [ATCAB\\_AES\\_CCM\\_EN](#) ([ATCAB\\_AES\\_CBCMAC\\_EN](#) && [ATCAB\\_AES\\_CTR\\_EN](#))
- #define **ATCAB\_AES\_CCM\_RAND\_IV\_EN** ([ATCAB\\_AES\\_CCM\\_EN](#) && [ATCAB\\_AES\\_RANDOM\\_IV\\_EN](#))
- #define **ATCAB\_AES\_CMAC\_EN** [ATCAB\\_AES\\_CBC\\_ENCRYPT\\_EN](#)
- #define **ATCAC\_PKCS7\_PAD\_EN** [ATCAB\\_AES\\_EXTRAS\\_EN](#)

### 22.121.1 Detailed Description

Consistency checks for configuration options.

#### Copyright

(c) 2015-2021 Microchip Technology Inc. and its subsidiaries.

### 22.121.2 Macro Definition Documentation

#### 22.121.2.1 ATCAB\_AES\_CBC\_DECRYPT\_EN

```
#define ATCAB_AES_CBC_DECRYPT_EN ATCAB_AES_EXTRAS_EN
```

Requires: ATCAB\_AES\_EN

Enable ATCAB\_AES\_CBC\_DECRYPT to decrypt a block of data using CBC mode and a key within the device. atcab\_aes\_cbc\_init() should be called before the first use of this function

Supported API's: atcab\_aes\_cbc\_decrypt\_block, atcab\_aes\_cbc\_init\_ext, atcab\_aes\_cbc\_init

#### 22.121.2.2 ATCAB\_AES\_CBC\_ENCRYPT\_EN

```
#define ATCAB_AES_CBC_ENCRYPT_EN ATCAB_AES_EXTRAS_EN
```

Requires: ATCAB\_AES\_EN

Enable ATCAB\_AES\_CBC\_ENCRYPT\_EN to encrypt a block of data using CBC mode and a key within the device. atcab\_aes\_cbc\_init() should be called before the first use of this function

Supported API's: atcab\_aes\_cbc\_encrypt\_block , atcab\_aes\_cbc\_init\_ext, atcab\_aes\_cbc\_init

#### 22.121.2.3 ATCAB\_AES\_CBCMAC\_EN

```
#define ATCAB_AES_CBCMAC_EN ATCAB_AES_CBC_ENCRYPT_EN
```

Requires: ATCAB\_AES\_CBCMAC ATCAB\_AES\_CBC\_ENCRYPT ATCAB\_AES\_MODE\_ENCODING CALIB\_↔ AES\_MODE\_ENCODING CALIB\_AES

Enable ATCAB\_AES\_CBCMAC to initialize context for AES CBC-MAC operation Enable ATCAB\_AES\_CBCMAC to calculate AES CBC-MAC with key stored within ECC608 device Enable ATCAB\_AES\_CBCMAC to finish a CBC-↔ MAC operation returning the CBC-MAC value

Supported API's: atcab\_aes\_cbcmac\_init\_ext atcab\_aes\_cbcmac\_init, atcab\_aes\_cbcmac\_init\_update, atcab\_↔ aes\_cbcmac\_finish

#### 22.121.2.4 ATCAB\_AES\_CCM\_EN

```
#define ATCAB_AES_CCM_EN (ATCAB_AES_CBCMAC_EN && ATCAB_AES_CTR_EN)
```

Requires: ATCAB\_AES\_EN ATCAB\_AES\_CTR\_EN

Enable ATCAB\_AES\_CCM\_EN to enable AES CCM operation

#### 22.121.2.5 ATCAB\_AES\_CTR\_EN

```
#define ATCAB_AES_CTR_EN ATCAB_AES_EXTRAS_EN
```

Requires: ATCAB\_AES\_EN

Enable ATCAB\_AES\_CTR\_EN to support AES-CTR mode

#### 22.121.2.6 ATCAB\_AES\_CTR\_RANDOM\_IV\_EN

```
#define ATCAB_AES_CTR_RANDOM_IV_EN (ATCAB_AES_CTR_EN && ATCAB_AES_RANDOM_IV_EN)
```

Requires: ATCAB\_AES\_CTR\_EN ATCAB\_RANDOM\_EN

Enable ATCAB\_AES\_CTR\_RANDOM\_IV\_EN to initialize context for AES CTR operation with a random nonce and counter set to 0 as the IV, which is common when starting an encrypt operation

Supported API's: atcab\_aes\_ctr\_init\_rand\_ext, atcab\_aes\_ctr\_init\_rand

#### 22.121.2.7 ATCAB\_AES\_EXTRAS\_EN

```
#define ATCAB_AES_EXTRAS_EN (CALIB_AES_EN || TALIB_AES_EN)
```

Automatically set base on other configuration options but can be overridden to disable all CBC, CBCMAC, CTR, & CCM modes at once rather than individually

#### 22.121.2.8 ATCAB\_AES\_UPDATE\_EN

```
#define ATCAB_AES_UPDATE_EN ATCAB_AES_EXTRAS_EN
```

Enable update/finalize APIs for block ciphers

## 22.122 crypto\_sw\_config\_check.h File Reference

Consistency checks for configuration options.

```
#include "atca_config_check.h"
```

### Macros

- `#define ATCAC_SHA1_EN` (DEFAULT\_ENABLED)
- `#define ATCAC_SHA256_EN` (DEFAULT\_ENABLED)
- `#define ATCAC_SHA256_HMAC_EN` ATCAC\_SHA256\_EN
- `#define ATCAC_SHA256_HMAC_CTR_EN` ATCAC\_SHA256\_HMAC\_EN
- `#define ATCAC_RANDOM_EN` ATCA\_HOSTLIB\_EN
- `#define ATCAC_VERIFY_EN` ATCA\_HOSTLIB\_EN
- `#define ATCAC_SIGN_EN` ATCA\_HOSTLIB\_EN
- `#define ATCA_CRYPT_SHA1_EN` (ATCAC\_SHA1\_EN && !ATCA\_HOSTLIB\_EN)
- `#define ATCA_CRYPT_SHA2_EN` (ATCAC\_SHA256\_EN && !ATCA\_HOSTLIB\_EN)
- `#define ATCA_CRYPT_SHA2_HMAC_EN` (ATCAC\_SHA256\_HMAC\_EN && !ATCA\_HOSTLIB\_EN)
- `#define ATCA_CRYPT_SHA2_HMAC_CTR_EN` ATCAC\_SHA256\_HMAC\_CTR\_EN
- `#define ATCAC_PBKDF2_SHA256_EN` ATCAC\_SHA256\_HMAC\_EN
- `#define ATCAB_PBKDF2_SHA256_EN` (CALIB\_SHA\_HMAC\_EN || TALIB\_SHA\_HMAC\_EN)
- `#define ATCAC_AES_GCM_EN` (ATCA\_HOSTLIB\_EN)

### 22.122.1 Detailed Description

Consistency checks for configuration options.

#### Copyright

(c) 2015-2021 Microchip Technology Inc. and its subsidiaries.

### 22.122.2 Macro Definition Documentation

#### 22.122.2.1 ATCA\_CRYPT\_SHA1\_EN

```
#define ATCA_CRYPT_SHA1_EN (ATCAC_SHA1_EN && !ATCA_HOSTLIB_EN)
```

Enable ATCAC\_SHA1\_EN to enable sha1 host side api

Supported API's: atcab\_write

#### 22.122.2.2 ATCA\_CRYPT\_SHA2\_HMAC\_CTR\_EN

```
#define ATCA_CRYPT_SHA2_HMAC_CTR_EN ATCAC_SHA256_HMAC_CTR_EN
```

Requires: ATCAC\_SHA256\_HMAC\_EN

Enable ATCAC\_SHA256\_HMAC\_COUNTER to implement SHA256 HMAC-Counter per NIST SP 800-108 used for KDF like operations

Supported API's: atcac\_sha256\_hmac\_counter

### 22.122.2.3 ATCA\_CRYPT\_SHA2\_HMAC\_EN

```
#define ATCA_CRYPT_SHA2_HMAC_EN (ATCAC_SHA256_HMAC_EN && !ATCA_HOSTLIB_EN)
```

Requires: ATCAC\_SHA256\_EN

Enable ATCAC\_SHA256\_HMAC to initialize context for performing HMAC (sha256) in software

Supported API's: atcac\_sha256\_hmac\_init, atcac\_sha256\_hmac\_update, atcac\_sha256\_hmac\_finish

### 22.122.2.4 ATCAB\_PBKDF2\_SHA256\_EN

```
#define ATCAB_PBKDF2_SHA256_EN (CALIB_SHA_HMAC_EN || TALIB_SHA_HMAC_EN)
```

Requires: CALIB\_SHA\_HMAC\_EN

Enable ATCAB\_PBKDF2\_SHA256\_EN to calculate a PBKDF2 password hash using a stored key inside a device. The key length is determined by the device being used. ECCx08: 32 bytes, TA100: 16-64 bytes

Supported API's: atcab\_pbkdf2\_256, atcab\_pbkdf2\_256\_ext

### 22.122.2.5 ATCAC\_AES\_GCM\_EN

```
#define ATCAC_AES_GCM_EN (ATCA_HOSTLIB_EN)
```

Indicates if this module is a provider of an AES-GCM implementation

### 22.122.2.6 ATCAC\_PBKDF2\_SHA256\_EN

```
#define ATCAC_PBKDF2_SHA256_EN ATCAC_SHA256_HMAC_EN
```

Requires: ATCAC\_SHA256\_EN ATCAC\_SHA256\_HMAC\_EN

Enable ATCAC\_PBKDF2\_SHA256\_EN to calculate a PBKDF2 hash of a given password and salt

Supported API's: atcac\_pbkdf2\_256

### 22.122.2.7 ATCAC\_RANDOM\_EN

```
#define ATCAC_RANDOM_EN ATCA_HOSTLIB_EN
```

Requires: ATCA\_HOSTLIB\_EN

Enable ATCAC\_RANDOM\_EN get random numbers from the host's implementation - generally assumed to come from the host's cryptographic library or peripheral driver

### 22.122.2.8 ATCAC\_SHA1\_EN

```
#define ATCAC_SHA1_EN (DEFAULT_ENABLED)
```

Enable ATCAC\_SHA1\_EN to enable sha1 host side api

Supported API's: atcab\_write

### 22.122.2.9 ATCAC\_SHA256\_EN

```
#define ATCAC_SHA256_EN (DEFAULT_ENABLED)
```

Enable ATCAC\_SHA256\_EN to enable sha256 host side api

Supported API's: atcab\_write

### 22.122.2.10 ATCAC\_SIGN\_EN

```
#define ATCAC_SIGN_EN ATCA_HOSTLIB_EN
```

Requires: ATCA\_HOSTLIB\_EN

Enable ATCAC\_SIGN\_EN to use the host's sign functions. Generally assumed to come from the host's cryptographic library or peripheral driver.

### 22.122.2.11 ATCAC\_VERIFY\_EN

```
#define ATCAC_VERIFY_EN ATCA_HOSTLIB_EN
```

Requires: ATCA\_HOSTLIB\_EN

Enable ATCAC\_VERIFY\_EN to use the host's verify functions. Generally assumed to come from the host's cryptographic library or peripheral driver.

## 22.123 sha1\_routines.c File Reference

Software implementation of the SHA1 algorithm.

```
#include "sha1_routines.h"  
#include <string.h>  
#include "atca_compiler.h"  
#include "cryptoauthlib.h"
```

### 22.123.1 Detailed Description

Software implementation of the SHA1 algorithm.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.



## 22.124 sha1\_routines.h File Reference

Software implementation of the SHA1 algorithm.

```
#include "atca_compiler.h"
#include <stdio.h>
#include <stdlib.h>
#include <stddef.h>
#include <stdint.h>
```

### Data Structures

- struct [CL\\_HashContext](#)

### Macros

- #define **U8** uint8\_t
- #define **U16** uint16\_t
- #define **U32** uint32\_t
- #define **memcpy\_P** memmove
- #define **strcpy\_P** strcpy
- #define **\_WDRESET()**
- #define **\_NOP()**
- #define **leftRotate**(x, n) (x) = (((x) << (n)) | ((x) >> (32 - (n))))

### Functions

- void **shaEngine** (uint32\_t \*buf, uint32\_t \*h)
- void **CL\_hashInit** ([CL\\_HashContext](#) \*ctx)
- void **CL\_hashUpdate** ([CL\\_HashContext](#) \*ctx, const uint8\_t \*src, int nbytes)
- void **CL\_hashFinal** ([CL\\_HashContext](#) \*ctx, uint8\_t \*dest)
- void **CL\_hash** (uint8\_t \*msg, int msgBytes, uint8\_t \*dest)

### 22.124.1 Detailed Description

Software implementation of the SHA1 algorithm.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.125 sha2\_routines.c File Reference

Software implementation of the SHA256 algorithm.

```
#include "cryptoauthlib.h"
#include "sha2_routines.h"
```

### Macros

- #define **rotate\_right**(value, places) ((value >> places) | (value << (32 - places)))

### 22.125.1 Detailed Description

Software implementation of the SHA256 algorithm.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.126 sha2\_routines.h File Reference

Software implementation of the SHA256 algorithm.

```
#include <stdint.h>
```

### Data Structures

- struct [sw\\_sha256\\_ctx](#)

### Macros

- #define **SHA256\_DIGEST\_SIZE** (32)
- #define **SHA256\_BLOCK\_SIZE** (64)

### Functions

- void **sw\_sha256\_init** ([sw\\_sha256\\_ctx](#) \*ctx)
- void **sw\_sha256\_update** ([sw\\_sha256\\_ctx](#) \*ctx, const uint8\_t \*message, uint32\_t len)
- void **sw\_sha256\_final** ([sw\\_sha256\\_ctx](#) \*ctx, uint8\_t digest[(32)])
- void **sw\_sha256** (const uint8\_t \*message, unsigned int len, uint8\_t digest[(32)])

### 22.126.1 Detailed Description

Software implementation of the SHA256 algorithm.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.127 cryptoauthlib.h File Reference

Single aggregation point for all CryptoAuthLib header files.

```
#include <stdio.h>
#include <stdint.h>
#include <stddef.h>
#include <stdlib.h>
#include <string.h>
#include <stdarg.h>
#include "atca_config_check.h"
#include "atca_compiler.h"
#include "atca_version.h"
#include "atca_platform.h"
#include "atca_status.h"
#include "atca_debug.h"
#include "cal_buffer.h"
#include "atca_iface.h"
#include "atca_device.h"
#include "atca_helpers.h"
#include "hal/atca_hal.h"
#include "atca_cfgs.h"
#include "calib/calib_basic.h"
#include "calib/calib_command.h"
#include "calib/calib_aes_gcm.h"
#include "talib/talib_status.h"
#include "talib/talib_basic.h"
#include "atca_basic.h"
```

### Macros

- #define [ATCA\\_SHA256\\_BLOCK\\_SIZE](#) (64u)
- #define **ATCA\_SHA256\_DIGEST\_SIZE** (32u)
- #define **ATCA\_SHA384\_BLOCK\_SIZE** (128u)
- #define **ATCA\_SHA384\_DIGEST\_SIZE** (48u)
- #define **ATCA\_SHA512\_BLOCK\_SIZE** (128u)
- #define **ATCA\_SHA512\_DIGEST\_SIZE** (64u)
- #define **ATCA\_AES128\_BLOCK\_SIZE** (16u)
- #define **ATCA\_AES128\_KEY\_SIZE** (16)
- #define **ATCA\_AES256\_BLOCK\_SIZE** (16u)
- #define **ATCA\_AES256\_KEY\_SIZE** (32u)
- #define **ATCA\_ECCP256\_MSG\_SIZE** (32u)
- #define **ATCA\_KEY\_TYPE\_ECCP256** (0u)
- #define **ATCA\_ECCP256\_KEY\_SIZE** (32u)
- #define **ATCA\_ECCP256\_PUBKEY\_SIZE** (64u)
- #define **ATCA\_ECCP256\_SIG\_SIZE** (64u)
- #define **ATCA\_ECCP256\_OID\_SIZE** (10u)
- #define **ATCA\_ECCP256\_ASN1\_HDR\_SIZE** (27u)
- #define **ATCA\_ECC\_UNCOMPRESSEDED\_TYPE** ((uint8\_t)0x04)
- #define **ATCA\_ECC\_UNCOMPRESSEDED\_TYPE\_OFFSET** (1u)
- #define **ATCA\_ZONE\_CONFIG** ((uint8\_t)0x00)
- #define **ATCA\_ZONE\_OTP** ((uint8\_t)0x01)
- #define **ATCA\_ZONE\_DATA** ((uint8\_t)0x02)
- #define **DEVICE\_PRODUCT\_ID\_LOCATION** 0

- #define **DEVICE\_IDENTIFIER\_LOCATION** 1
- #define **DEVICE\_PART\_LOCATION** 2
- #define **DEVICE\_REVISION\_LOCATION** 3
- #define **ATCA\_ZONE\_CA2\_DATA** ((uint8\_t)0x00)
- #define **ATCA\_ZONE\_CA2\_CONFIG** ((uint8\_t)0x01)
- #define **ATCA\_ECC204\_DEVICE\_ID** ((uint8\_t)0x5A)
- #define **ATCA\_TA010\_DEVICE\_ID** ((uint8\_t)0x6A)
- #define **ATCA\_SHA104\_DEVICE\_ID** ((uint8\_t)0x35)
- #define **ATCA\_SHA105\_DEVICE\_ID** ((uint8\_t)0x3B)
- #define **SHA\_MODE\_TARGET\_TEMPKEY** ((uint8\_t)0x00)
- #define **SHA\_MODE\_TARGET\_MSGDIGBUF** ((uint8\_t)0x40)
- #define **SHA\_MODE\_TARGET\_OUT\_ONLY** ((uint8\_t)0xC0)
- #define **ATCA\_STRINGIFY**(x) #x
- #define **ATCA\_TOSTRING**(x) ATCA\_STRINGIFY(x)
- #define **ATCA\_TRACE**(s, m) atca\_trace(s)

### 22.127.1 Detailed Description

Single aggregation point for all CryptoAuthLib header files.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.127.2 Macro Definition Documentation

#### 22.127.2.1 ATCA\_SHA256\_BLOCK\_SIZE

```
#define ATCA_SHA256_BLOCK_SIZE (64u)
```

Library Configuration File - All build attributes should be included in atca\_config.h

#### 22.127.2.2 SHA\_MODE\_TARGET\_MSGDIGBUF

```
#define SHA_MODE_TARGET_MSGDIGBUF ((uint8_t)0x40)
```

Place resulting digest both in Output buffer and Message Digest Buffer

#### 22.127.2.3 SHA\_MODE\_TARGET\_OUT\_ONLY

```
#define SHA_MODE_TARGET_OUT_ONLY ((uint8_t)0xC0)
```

Place resulting digest both in Output buffer ONLY

#### 22.127.2.4 SHA\_MODE\_TARGET\_TEMPKEY

```
#define SHA_MODE_TARGET_TEMPKEY ((uint8_t)0x00)
```

Place resulting digest both in Output buffer and TempKey

## 22.128 atca\_hal.c File Reference

low-level HAL - methods used to setup indirection to physical layer interface. this level does the dirty work of abstracting the higher level ATCAIFace methods from the low-level physical interfaces. Its main goal is to keep low-level details from bleeding into the logical interface implementation.

```
#include "cryptoauthlib.h"
#include "atca_hal.h"
```

### Data Structures

- struct [atca\\_hal\\_list\\_entry\\_t](#)  
*Structure that holds the hal/phy mapping for different interface types.*

### Functions

- ATCA\_STATUS [hal\\_iface\\_register\\_hal](#) (ATCAIFaceType iface\_type, ATCAHAL\_t \*hal, ATCAHAL\_t \*\*old\_hal, ATCAHAL\_t \*phy, ATCAHAL\_t \*\*old\_phy)  
*Register/Replace a HAL with a.*
- ATCA\_STATUS [hal\\_iface\\_init](#) (ATCAIFaceCfg \*cfg, ATCAHAL\_t \*\*hal, ATCAHAL\_t \*\*phy)  
*Standard HAL API for ATCA to initialize a physical interface.*
- ATCA\_STATUS [hal\\_iface\\_release](#) (ATCAIFaceType iface\_type, void \*hal\_data)  
*releases a physical interface, HAL knows how to interpret hal\_data*
- ATCA\_STATUS [hal\\_check\\_wake](#) (const uint8\_t \*response, int response\_size)  
*Utility function for hal\_wake to check the reply.*
- uint8\_t [hal\\_is\\_command\\_word](#) (uint8\_t word\_address)  
*Utility function for hal\_wake to check the reply.*

#### 22.128.1 Detailed Description

low-level HAL - methods used to setup indirection to physical layer interface. this level does the dirty work of abstracting the higher level ATCAIFace methods from the low-level physical interfaces. Its main goal is to keep low-level details from bleeding into the logical interface implementation.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.129 atca\_hal.h File Reference

low-level HAL - methods used to setup indirection to physical layer interface

```
#include <stdlib.h>
#include "atca_config.h"
#include "atca_status.h"
#include "atca_iface.h"
```

### Data Structures

- struct [atca\\_hal\\_kit\\_phy\\_t](#)
- struct [atca\\_hal\\_shm\\_t](#)

### Macros

- **#define ATCA\_POLLING\_INIT\_TIME\_MSEC 1**
- **#define ATCA\_POLLING\_FREQUENCY\_TIME\_MSEC 2**
- **#define ATCA\_POLLING\_MAX\_TIME\_MSEC 2500**
- **#define ATCA\_HAL\_CONTROL\_WAKE (0U)**  
*Execute the hardware specific wake - generally only for kits.*
- **#define ATCA\_HAL\_CONTROL\_IDLE (1U)**  
*Execute the hardware specific idle - generally only for kits.*
- **#define ATCA\_HAL\_CONTROL\_SLEEP (2U)**  
*Execute the hardware specific sleep - generally only for kits.*
- **#define ATCA\_HAL\_CONTROL\_RESET (3U)**  
*Execute the hardware specific reset - generally only for kits.*
- **#define ATCA\_HAL\_CONTROL\_SELECT (4U)**  
*Select the device - assert CS, open device, etc.*
- **#define ATCA\_HAL\_CONTROL\_DESELECT (5U)**  
*Select the device - de-assert CS, release device, etc.*
- **#define ATCA\_HAL\_CHANGE\_BAUD (6U)**  
*Change the datarate of the phy.*
- **#define ATCA\_HAL\_FLUSH\_BUFFER (7U)**  
*If the phy has a buffer make sure all bytes are transmitted.*
- **#define ATCA\_HAL\_CONTROL\_DIRECTION (8U)**  
*Set the PIN mode (in vs out)*

### Typedefs

- typedef void \* **hal\_mutex\_t**  
*Generic mutex type definition for most systems.*

## Functions

- ATCA\_STATUS [hal\\_iface\\_init](#) (ATCAIfaceCfg \*cfg, ATCAHAL\_t \*\*hal, ATCAHAL\_t \*\*phy)  
*Standard HAL API for ATCA to initialize a physical interface.*
- ATCA\_STATUS [hal\\_iface\\_release](#) (ATCAIfaceType iface\_type, void \*hal\_data)  
*releases a physical interface, HAL knows how to interpret hal\_data*
- ATCA\_STATUS [hal\\_check\\_wake](#) (const uint8\_t \*response, int response\_size)  
*Utility function for hal\_wake to check the reply.*
- void [atca\\_delay\\_ms](#) (uint32\_t ms)  
*Timer API for legacy implementations.*
- void [atca\\_delay\\_us](#) (uint32\_t delay)  
*This function delays for a number of microseconds.*
- void [hal\\_delay\\_ms](#) (uint32\_t delay)  
*Timer API implemented at the HAL level.*
- void [hal\\_delay\\_us](#) (uint32\_t delay)  
*This function delays for a number of microseconds.*
- ATCA\_STATUS [hal\\_create\\_mutex](#) (void \*\*ppMutex, const char \*pName)  
*Optional hal interfaces.*
- ATCA\_STATUS [hal\\_init\\_mutex](#) (void \*pMutex, bool shared)
- ATCA\_STATUS [hal\\_destroy\\_mutex](#) (void \*pMutex)
- ATCA\_STATUS [hal\\_lock\\_mutex](#) (void \*pMutex)
- ATCA\_STATUS [hal\\_unlock\\_mutex](#) (void \*pMutex)
- ATCA\_STATUS [hal\\_alloc\\_shared](#) (void \*\*pShared, size\_t size, const char \*pName, bool \*initialized)
- ATCA\_STATUS [hal\\_free\\_shared](#) (void \*pShared, size\_t size)
- ATCA\_STATUS [hal\\_iface\\_register\\_hal](#) (ATCAIfaceType iface\_type, ATCAHAL\_t \*hal, ATCAHAL\_t \*\*old\_hal, ATCAHAL\_t \*phy, ATCAHAL\_t \*\*old\_phy)  
*Register/Replace a HAL with a.*
- uint8\_t [hal\\_is\\_command\\_word](#) (uint8\_t word\_address)  
*Utility function for hal\_wake to check the reply.*

### 22.129.1 Detailed Description

low-level HAL - methods used to setup indirection to physical layer interface

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.130 hal\_all\_platforms\_kit\_hidapi.c File Reference

HAL for kit protocol over HID for any platform.

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include "hidapi.h"
#include "atca_hal.h"
#include "hal/kit_protocol.h"
```

## Functions

- ATCA\_STATUS [hal\\_kit\\_hid\\_init](#) ([ATCAIface](#) iface, [ATCAIfaceCfg](#) \*cfg)  
*HAL implementation of Kit USB HID init.*
- ATCA\_STATUS [hal\\_kit\\_hid\\_post\\_init](#) ([ATCAIface](#) iface)  
*HAL implementation of Kit HID post init.*
- ATCA\_STATUS [hal\\_kit\\_hid\\_send](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*HAL implementation of kit protocol send over USB HID.*
- ATCA\_STATUS [hal\\_kit\\_hid\\_receive](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*HAL implementation of send over USB HID.*
- ATCA\_STATUS [hal\\_kit\\_hid\\_control](#) ([ATCAIface](#) iface, uint8\_t option, void \*param, size\_t paramlen)  
*Perform control operations for the kit protocol.*
- ATCA\_STATUS [hal\\_kit\\_hid\\_release](#) (void \*hal\_data)  
*Close the physical port for HID.*

### 22.130.1 Detailed Description

HAL for kit protocol over HID for any platform.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.131 hal\_freertos.c File Reference

FreeRTOS Hardware/OS Abstraction Layer.

```
#include "atca_hal.h"
#include "FreeRTOS.h"
#include "semphr.h"
#include "task.h"
```

## Macros

- #define **ATCA\_MUTEX\_TIMEOUT** portMAX\_DELAY

## Functions

- void \* **hal\_malloc** (size\_t size)
- void **hal\_free** (void \*ptr)
- void [hal\\_rtos\\_delay\\_ms](#) (uint32\_t delay)  
*This function delays for a number of milliseconds.*
- ATCA\_STATUS [hal\\_create\\_mutex](#) (void \*\*ppMutex, const char \*pName)  
*Optional hal interfaces.*
- ATCA\_STATUS **hal\_destroy\_mutex** (void \*pMutex)
- ATCA\_STATUS **hal\_lock\_mutex** (void \*pMutex)
- ATCA\_STATUS **hal\_unlock\_mutex** (void \*pMutex)



### 22.131.1 Detailed Description

FreeRTOS Hardware/OS Abstraction Layer.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.132 hal\_gpio\_harmony.c File Reference

ATCA Hardware abstraction layer for GPIO.

```
#include "atca_hal.h"
```

### Functions

- ATCA\_STATUS [hal\\_gpio\\_init](#) ([ATCAIface](#) iface, [ATCAIfaceCfg](#) \*cfg)  
*Initialize a gpio interface using given config.*
- ATCA\_STATUS [hal\\_gpio\\_post\\_init](#) ([ATCAIface](#) iface)  
*Post Init for gpio hal.*
- ATCA\_STATUS [hal\\_gpio\\_send](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*pin\_state, int unused\_↔ param)  
*Set the state of the pin.*
- ATCA\_STATUS [hal\\_gpio\\_receive](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*pin\_state, uint16\_↔ t \*unused\_param)  
*Read the state of the pin.*
- ATCA\_STATUS [hal\\_gpio\\_control](#) ([ATCAIface](#) iface, uint8\_t option, void \*param, size\_t paramlen)
- ATCA\_STATUS [hal\\_gpio\\_release](#) (void \*hal\_data)  
*Release and clean up the HAL.*

### 22.132.1 Detailed Description

ATCA Hardware abstraction layer for GPIO.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.132.2 Function Documentation

### 22.132.2.1 hal\_gpio\_init()

```
ATCA_STATUS hal_gpio_init (
    ATCAIface iface,
    ATCAIfaceCfg * cfg )
```

Initialize a gpio interface using given config.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 22.132.2.2 hal\_gpio\_post\_init()

```
ATCA_STATUS hal_gpio_post_init (
    ATCAIface iface )
```

Post Init for gpio hal.

#### Returns

ATCA\_SUCCESS

### 22.132.2.3 hal\_gpio\_receive()

```
ATCA_STATUS hal_gpio_receive (
    ATCAIface iface,
    uint8_t word_address,
    uint8_t * pin_state,
    uint16_t * unused_param )
```

Read the state of the pin.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### Parameters

<i>iface</i>	Interface context
<i>word_address</i>	Unused parameter
<i>pin_state</i>	Pin state to output
<i>unused_param</i>	Unused parameter

### 22.132.2.4 hal\_gpio\_release()

```
ATCA_STATUS hal_gpio_release (
    void * hal_data )
```

Release and clean up the HAL.

Parameters

in	hal_data	opaque pointer to hal data structure - known only to the HAL implementation
----	----------	---

Returns

ATCA\_SUCCESS

### 22.132.2.5 hal\_gpio\_send()

```
ATCA_STATUS hal_gpio_send (
    ATCAIface iface,
    uint8_t word_address,
    uint8_t * pin_state,
    int unused_param )
```

Set the state of the pin.

Returns

ATCA\_SUCCESS

Parameters

iface	Interface context
word_address	Unused parameter
pin_state	Pin state to output
unused_param	Unused parameter

## 22.133 hal\_i2c\_harmony.c File Reference

ATCA Hardware abstraction layer for SAMD21 I2C over Harmony PLIB.

```
#include <string.h>
#include <stdio.h>
#include "cryptoauthlib.h"
```

## Functions

- ATCA\_STATUS [hal\\_i2c\\_discover\\_buses](#) (int i2c\_buses[], int max\_buses)  
*discover i2c buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-prior knowledge*
- ATCA\_STATUS [hal\\_i2c\\_discover\\_devices](#) (int bus\_num, [ATCAIfaceCfg](#) cfg[], int \*found)  
*discover any CryptoAuth devices on a given logical bus number*
- ATCA\_STATUS [hal\\_i2c\\_init](#) ([ATCAIface](#) iface, [ATCAIfaceCfg](#) \*cfg)  
*hal\_i2c\_init manages requests to initialize a physical interface. it manages use counts so when an interface has released the physical layer, it will disable the interface for some other use. You can have multiple ATCAIface instances using the same bus, and you can have multiple ATCAIface instances on multiple i2c buses, so hal\_i2c\_init manages these things and ATCAIface is abstracted from the physical details.*
- ATCA\_STATUS [hal\\_i2c\\_post\\_init](#) ([ATCAIface](#) iface)  
*HAL implementation of I2C post init.*
- ATCA\_STATUS [hal\\_i2c\\_send](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*HAL implementation of I2C send over START.*
- ATCA\_STATUS [hal\\_i2c\\_receive](#) ([ATCAIface](#) iface, uint8\_t address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*HAL implementation of I2C receive function for START I2C.*
- ATCA\_STATUS [change\\_i2c\\_speed](#) ([ATCAIface](#) iface, uint32\_t speed)  
*method to change the bus speed of I2C*
- ATCA\_STATUS [hal\\_i2c\\_control](#) ([ATCAIface](#) iface, uint8\_t option, void \*param, size\_t paramlen)  
*Perform control operations for the kit protocol.*
- ATCA\_STATUS [hal\\_i2c\\_release](#) (void \*hal\_data)  
*manages reference count on given bus and releases resource if no more references exist*

### 22.133.1 Detailed Description

ATCA Hardware abstraction layer for SAMD21 I2C over Harmony PLIB.

This code is structured in two parts. Part 1 is the connection of the ATCA HAL API to the physical I2C implementation. Part 2 is the Harmony I2C primitives to set up the interface.

Prerequisite: add SERCOM I2C Master Polled support to application in Atmel Studio

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.134 hal\_i2c\_start.c File Reference

ATCA Hardware abstraction layer for SAMD21 I2C over START drivers.

```
#include <string.h>
#include <stdio.h>
#include <atmel_start.h>
#include <hal_gpio.h>
#include <hal_delay.h>
#include "hal_i2c_start.h"
#include "atca_start_config.h"
#include "atca_start_iface.h"
#include "cryptoauthlib.h"
```

## Functions

- ATCA\_STATUS [hal\\_i2c\\_discover\\_buses](#) (int i2c\_buses[], int max\_buses)  
*discover i2c buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-prior knowledge*
- ATCA\_STATUS [hal\\_i2c\\_discover\\_devices](#) (int bus\_num, [ATCAIfaceCfg](#) cfg[], int \*found)  
*discover any CryptoAuth devices on a given logical bus number*
- ATCA\_STATUS [hal\\_i2c\\_init](#) (void \*hal, [ATCAIfaceCfg](#) \*cfg)  
*hal\_i2c\_init manages requests to initialize a physical interface. it manages use counts so when an interface has released the physical layer, it will disable the interface for some other use. You can have multiple ATCAIface instances using the same bus, and you can have multiple ATCAIface instances on multiple i2c buses, so hal\_i2c\_init manages these things and ATCAIface is abstracted from the physical details.*
- ATCA\_STATUS [hal\\_i2c\\_post\\_init](#) ([ATCAIface](#) iface)  
*HAL implementation of I2C post init.*
- ATCA\_STATUS [hal\\_i2c\\_send](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*HAL implementation of I2C send over START.*
- ATCA\_STATUS [hal\\_i2c\\_receive](#) ([ATCAIface](#) iface, uint8\_t address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*HAL implementation of I2C receive function for START I2C.*
- ATCA\_STATUS [hal\\_i2c\\_wake](#) ([ATCAIface](#) iface)  
*wake up CryptoAuth device using I2C bus*
- ATCA\_STATUS [hal\\_i2c\\_idle](#) ([ATCAIface](#) iface)  
*idle CryptoAuth device using I2C bus*
- ATCA\_STATUS [hal\\_i2c\\_sleep](#) ([ATCAIface](#) iface)  
*sleep CryptoAuth device using I2C bus*
- ATCA\_STATUS [hal\\_i2c\\_release](#) (void \*hal\_data)  
*manages reference count on given bus and releases resource if no more references exist*

### 22.134.1 Detailed Description

ATCA Hardware abstraction layer for SAMD21 I2C over START drivers.

This code is structured in two parts. Part 1 is the connection of the ATCA HAL API to the physical I2C implementation. Part 2 is the START I2C primitives to set up the interface.

Prerequisite: add SERCOM I2C Master Polled support to application in Atmel Studio

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.135 hal\_i2c\_start.h File Reference

ATCA Hardware abstraction layer for SAMD21 I2C over START drivers.

```
#include "atmel_start.h"
#include <stdlib.h>
#include "cryptoauthlib.h"
```

## Data Structures

- struct [i2c\\_start\\_instance](#)

## Typedefs

- typedef void(\* **start\_change\_baudrate**) ([ATCAIface](#) iface, uint32\_t speed)
- typedef struct [i2c\\_start\\_instance](#) **i2c\_start\_instance\_t**

### 22.135.1 Detailed Description

ATCA Hardware abstraction layer for SAMD21 I2C over START drivers.

Prerequisite: add SERCOM I2C Master Polled support to application in Atmel Studio

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.136 hal\_kit\_bridge.c File Reference

Kit Bridging HAL for cryptoauthlib. This is not intended to be a zero copy driver. It should work with any interface that confirms to a few basic requirements: a) will accept an arbitrary number of bytes and packetize it if necessary for transmission, b) will block for the duration of the transmit.

```
#include "cryptoauthlib.h"
#include "atca_hal.h"
#include "hal_kit_bridge.h"
```

## Functions

- ATCA\_STATUS [hal\\_kit\\_attach\\_phy](#) ([ATCAIfaceCfg](#) \*cfg, [atca\\_hal\\_kit\\_phy\\_t](#) \*phy)  
*Helper function that connects a physical layer context structure that will be used by the kit protocol bridge.*
- ATCA\_STATUS [hal\\_kit\\_init](#) ([ATCAIface](#) iface, [ATCAIfaceCfg](#) \*cfg)  
*HAL implementation of Kit USB HID init.*
- ATCA\_STATUS [hal\\_kit\\_post\\_init](#) ([ATCAIface](#) iface)  
*HAL implementation of Kit HID post init.*
- ATCA\_STATUS [hal\\_kit\\_send](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*HAL implementation of kit protocol send over USB HID.*
- ATCA\_STATUS [hal\\_kit\\_receive](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*rxdata, uint16\_t \*rxsize)  
*HAL implementation of send over USB HID.*
- ATCA\_STATUS [hal\\_kit\\_control](#) ([ATCAIface](#) iface, uint8\_t option, void \*param, size\_t paramlen)  
*Kit Protocol Control.*
- ATCA\_STATUS [hal\\_kit\\_release](#) (void \*hal\_data)  
*Close the physical port for HID.*

## 22.136.1 Detailed Description

Kit Bridging HAL for cryptoauthlib. This is not intended to be a zero copy driver. It should work with any interface that confirms to a few basic requirements: a) will accept an arbitrary number of bytes and packetize it if necessary for transmission, b) will block for the duration of the transmit.

### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.137 hal\_kit\_bridge.h File Reference

Kit Bridging HAL for cryptoauthlib. This is not intended to be a zero copy driver. It should work with any interface that confirms to a few basic requirements: a) will accept an arbitrary number of bytes and packetize it if necessary for transmission, b) will block for the duration of the transmit.

### Macros

- #define **BRIDGE\_PROTOCOL\_VERSION** (2)
- #define **HAL\_KIT\_COMMAND\_SEND** 0x01
- #define **HAL\_KIT\_COMMAND\_RECV** 0x02
- #define **HAL\_KIT\_COMMAND\_WAKE** 0x03
- #define **HAL\_KIT\_COMMAND\_IDLE** 0x04
- #define **HAL\_KIT\_COMMAND\_SLEEP** 0x05
- #define **HAL\_KIT\_HEADER\_LEN** (3)

### Functions

- ATCA\_STATUS [hal\\_kit\\_attach\\_phy](#) ([ATCAIfaceCfg](#) \*cfg, [atca\\_hal\\_kit\\_phy\\_t](#) \*phy)

*Helper function that connects a physical layer context structure that will be used by the kit protocol bridge.*

## 22.137.1 Detailed Description

Kit Bridging HAL for cryptoauthlib. This is not intended to be a zero copy driver. It should work with any interface that confirms to a few basic requirements: a) will accept an arbitrary number of bytes and packetize it if necessary for transmission, b) will block for the duration of the transmit.

### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.138 hal\_linux.c File Reference

Timer Utility Functions for Linux.

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <stdint.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <fcntl.h>
#include <errno.h>
#include "atca_hal.h"
```

### Functions

- void [hal\\_delay\\_us](#) (uint32\_t delay)  
*This function delays for a number of microseconds.*
- void [hal\\_delay\\_ms](#) (uint32\_t delay)  
*Timer API implemented at the HAL level.*
- ATCA\_STATUS [hal\\_create\\_mutex](#) (void \*\*ppMutex, const char \*pName)  
*Optional hal interfaces.*
- ATCA\_STATUS [hal\\_destroy\\_mutex](#) (void \*pMutex)
- ATCA\_STATUS [hal\\_lock\\_mutex](#) (void \*pMutex)
- ATCA\_STATUS [hal\\_unlock\\_mutex](#) (void \*pMutex)
- ATCA\_STATUS [hal\\_check\\_pid](#) (hal\_pid\_t pid)  
*Check if the pid exists in the system.*

### 22.138.1 Detailed Description

Timer Utility Functions for Linux.

#### Copyright

(c) 2015-2018 Microchip Technology Inc. and its subsidiaries.

## 22.139 hal\_linux\_i2c\_userspace.c File Reference

ATCA Hardware abstraction layer for Linux using I2C.

```
#include <cryptoauthlib.h>
#include <linux/i2c-dev.h>
#include <unistd.h>
#include <sys/ioctl.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <fcntl.h>
#include <errno.h>
#include <string.h>
#include <stdint.h>
#include <stdio.h>
#include <stdlib.h>
#include <limits.h>
#include "atca_hal.h"
```



## Data Structures

- struct [atca\\_i2c\\_host\\_s](#)

## Typedefs

- typedef struct [atca\\_i2c\\_host\\_s](#) [atca\\_i2c\\_host\\_t](#)

## Functions

- ATCA\_STATUS [hal\\_i2c\\_init](#) ([ATCAIface](#) iface, [ATCAIfaceCfg](#) \*cfg)  
*hal\_i2c\_init manages requests to initialize a physical interface. it manages use counts so when an interface has released the physical layer, it will disable the interface for some other use. You can have multiple ATCAIface instances using the same bus, and you can have multiple ATCAIface instances on multiple i2c buses, so hal\_i2c\_init manages these things and ATCAIface is abstracted from the physical details.*
- ATCA\_STATUS [hal\\_i2c\\_post\\_init](#) ([ATCAIface](#) iface)  
*HAL implementation of I2C post init.*
- ATCA\_STATUS [hal\\_i2c\\_send](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*HAL implementation of I2C send over START.*
- ATCA\_STATUS [hal\\_i2c\\_receive](#) ([ATCAIface](#) iface, uint8\_t address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*HAL implementation of I2C receive function for START I2C.*
- ATCA\_STATUS [hal\\_i2c\\_control](#) ([ATCAIface](#) iface, uint8\_t option, void \*param, size\_t paramlen)  
*Perform control operations for the kit protocol.*
- ATCA\_STATUS [hal\\_i2c\\_release](#) (void \*hal\_data)  
*manages reference count on given bus and releases resource if no more references exist*

### 22.139.1 Detailed Description

ATCA Hardware abstraction layer for Linux using I2C.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.140 hal\_linux\_uart\_userspace.c File Reference

ATCA Hardware abstraction layer for Linux using UART.

```
#include "cryptoauthlib.h"
#include "atca_hal.h"
#include <unistd.h>
#include <fcntl.h>
#include <sys/ioctl.h>
#include <termios.h>
```

## Data Structures

- struct [atca\\_uart\\_host\\_s](#)

## Typedefs

- typedef struct [atca\\_uart\\_host\\_s](#) [atca\\_uart\\_host\\_t](#)

## Functions

- ATCA\_STATUS [hal\\_uart\\_init](#) ([ATCAIface](#) iface, [ATCAIfaceCfg](#) \*cfg)  
*HAL implementation of UART init.*
- ATCA\_STATUS [hal\\_uart\\_post\\_init](#) ([ATCAIface](#) iface)  
*HAL implementation of UART post init.*
- ATCA\_STATUS [hal\\_uart\\_send](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*HAL implementation of UART send.*
- ATCA\_STATUS [hal\\_uart\\_receive](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*HAL implementation of UART receive function.*
- ATCA\_STATUS [hal\\_uart\\_control](#) ([ATCAIface](#) iface, uint8\_t option, void \*param, size\_t paramlen)  
*Perform control operations for the UART.*
- ATCA\_STATUS [hal\\_uart\\_release](#) (void \*hal\_data)  
*manages reference count on given bus and releases resource if no more references exist*

### 22.140.1 Detailed Description

ATCA Hardware abstraction layer for Linux using UART.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.140.2 Function Documentation

#### 22.140.2.1 [hal\\_uart\\_control\(\)](#)

```
ATCA_STATUS hal_uart_control (  
    ATCAIface iface,  
    uint8_t option,  
    void * param,  
    size_t paramlen )
```

Perform control operations for the UART.

#### Parameters

in	<i>iface</i>	Interface to interact with.
in	<i>option</i>	Control parameter identifier
in	<i>param</i>	Optional pointer to parameter value
in	<i>paramlen</i>	Length of the parameter

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.140.2.2 hal\_uart\_init()

```
ATCA_STATUS hal_uart_init (
    ATCAIface iface,
    ATCAIfaceCfg * cfg )
```

HAL implementation of UART init.

this implementation assumes UART SERIAL PORT peripheral has been enabled by user . It only initialize an UART interface using given config.

Parameters

in	hal	pointer to HAL specific data that is maintained by this HAL
in	cfg	pointer to HAL specific configuration data that is used to initialize this HAL

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.140.2.3 hal\_uart\_post\_init()

```
ATCA_STATUS hal_uart_post_init (
    ATCAIface iface )
```

HAL implementation of UART post init.

Parameters

in	iface	instance
----	-------	----------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.140.2.4 hal\_uart\_receive()

```
ATCA_STATUS hal_uart_receive (
    ATCAIface iface,
```

```
uint8_t word_address,
uint8_t * rxdata,
uint16_t * rxlength )
```

HAL implementation of UART receive function.

Parameters

in	<i>iface</i>	Device to interact with.
in	<i>word_address</i>	device transaction type
out	<i>rxdata</i>	Data received will be returned here.
in, out	<i>rxlength</i>	As input, the size of the rxdata buffer. As output, the number of bytes received.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.140.2.5 hal\_uart\_release()

```
ATCA_STATUS hal_uart_release (
    void * hal_data )
```

manages reference count on given bus and releases resource if no more refences exist

Parameters

in	<i>hal_data</i>	- opaque pointer to hal data structure - known only to the HAL implementation
----	-----------------	---

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.140.2.6 hal\_uart\_send()

```
ATCA_STATUS hal_uart_send (
    ATCAIface iface,
    uint8_t word_address,
    uint8_t * txdata,
    int txlength )
```

HAL implementation of UART send.

Parameters

in	<i>iface</i>	instance
in	<i>word_address</i>	transaction type
in	<i>txdata</i>	data to be send to device
in	<i>txlength</i>	pointer to space to bytes to send

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

**22.141 hal\_sam0\_i2c\_asf.c File Reference**

ATCA Hardware abstraction layer for SAMD21 I2C over ASF drivers.

```
#include <asf.h>
#include <string.h>
#include <stdio.h>
#include "hal_sam0_i2c_asf.h"
#include "cryptoauthlib.h"
```

**Functions**

- ATCA\_STATUS [hal\\_i2c\\_discover\\_buses](#) (int i2c\_buses[], int max\_buses)  
*discover i2c buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-prior knowledge*
- ATCA\_STATUS [hal\\_i2c\\_discover\\_devices](#) (int bus\_num, [ATCAIfaceCfg](#) cfg[], int \*found)  
*discover any CryptoAuth devices on a given logical bus number*
- ATCA\_STATUS [hal\\_i2c\\_init](#) (void \*hal, [ATCAIfaceCfg](#) \*cfg)  
*hal\_i2c\_init manages requests to initialize a physical interface. it manages use counts so when an interface has released the physical layer, it will disable the interface for some other use. You can have multiple ATCAIface instances using the same bus, and you can have multiple ATCAIface instances on multiple i2c buses, so hal\_i2c\_init manages these things and ATCAIface is abstracted from the physical details.*
- ATCA\_STATUS [hal\\_i2c\\_post\\_init](#) ([ATCAIface](#) iface)  
*HAL implementation of I2C post init.*
- ATCA\_STATUS [hal\\_i2c\\_send](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*HAL implementation of I2C send over START.*
- ATCA\_STATUS [hal\\_i2c\\_receive](#) ([ATCAIface](#) iface, uint8\_t address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*HAL implementation of I2C receive function for START I2C.*
- ATCA\_STATUS [hal\\_i2c\\_wake](#) ([ATCAIface](#) iface)  
*wake up CryptoAuth device using I2C bus*
- ATCA\_STATUS [hal\\_i2c\\_idle](#) ([ATCAIface](#) iface)  
*idle CryptoAuth device using I2C bus*
- ATCA\_STATUS [hal\\_i2c\\_sleep](#) ([ATCAIface](#) iface)  
*sleep CryptoAuth device using I2C bus*
- ATCA\_STATUS [hal\\_i2c\\_release](#) (void \*hal\_data)  
*manages reference count on given bus and releases resource if no more references exist*

**22.141.1 Detailed Description**

ATCA Hardware abstraction layer for SAMD21 I2C over ASF drivers.

This code is structured in two parts. Part 1 is the connection of the ATCA HAL API to the physical I2C implementation. Part 2 is the ASF I2C primitives to set up the interface.

Prerequisite: add SERCOM I2C Master Polled support to application in Atmel Studio

**Copyright**

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.142 hal\_sam0\_i2c\_asf.h File Reference

ATCA Hardware abstraction layer for SAMD21 I2C over ASF drivers.

```
#include <asf.h>
#include "cryptoauthlib.h"
```

#### Data Structures

- struct [i2c\\_sam0\\_instance](#)

#### Typedefs

- typedef void(\* [sam0\\_change\\_baudrate](#)) ([ATCAIface](#) iface, uint32\_t speed)
- typedef struct [i2c\\_sam0\\_instance](#) [i2c\\_sam0\\_instance\\_t](#)

#### 22.142.1 Detailed Description

ATCA Hardware abstraction layer for SAMD21 I2C over ASF drivers.

Prerequisite: add SERCOM I2C Master Polled support to application in Atmel Studio

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.143 hal\_sam\_i2c\_asf.c File Reference

ATCA Hardware abstraction layer for SAM flexcom & twi I2C over ASF drivers.

```
#include <asf.h>
#include <string.h>
#include <stdio.h>
#include "cryptoauthlib.h"
#include "hal_sam_i2c_asf.h"
```

## Functions

- ATCA\_STATUS [hal\\_i2c\\_discover\\_buses](#) (int i2c\_buses[], int max\_buses)  
*discover i2c buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-prior knowledge*
- ATCA\_STATUS [hal\\_i2c\\_discover\\_devices](#) (int bus\_num, [ATCAIfaceCfg](#) cfg[], int \*found)  
*discover any CryptoAuth devices on a given logical bus number*
- ATCA\_STATUS [hal\\_i2c\\_init](#) (void \*hal, [ATCAIfaceCfg](#) \*cfg)  
*hal\_i2c\_init manages requests to initialize a physical interface. it manages use counts so when an interface has released the physical layer, it will disable the interface for some other use. You can have multiple ATCAIface instances using the same bus, and you can have multiple ATCAIface instances on multiple i2c buses, so hal\_i2c\_init manages these things and ATCAIface is abstracted from the physical details.*
- ATCA\_STATUS [hal\\_i2c\\_post\\_init](#) ([ATCAIface](#) iface)  
*HAL implementation of I2C post init.*
- ATCA\_STATUS [hal\\_i2c\\_send](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*HAL implementation of I2C send over START.*
- ATCA\_STATUS [hal\\_i2c\\_receive](#) ([ATCAIface](#) iface, uint8\_t address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*HAL implementation of I2C receive function for START I2C.*
- ATCA\_STATUS [hal\\_i2c\\_wake](#) ([ATCAIface](#) iface)  
*wake up CryptoAuth device using I2C bus*
- ATCA\_STATUS [hal\\_i2c\\_idle](#) ([ATCAIface](#) iface)  
*idle CryptoAuth device using I2C bus*
- ATCA\_STATUS [hal\\_i2c\\_sleep](#) ([ATCAIface](#) iface)  
*sleep CryptoAuth device using I2C bus*
- ATCA\_STATUS [hal\\_i2c\\_release](#) (void \*hal\_data)  
*manages reference count on given bus and releases resource if no more references exist*

### 22.143.1 Detailed Description

ATCA Hardware abstraction layer for SAM flexcom & twi I2C over ASF drivers.

This code is structured in two parts. Part 1 is the connection of the ATCA HAL API to the physical I2C implementation. Part 2 is the ASF I2C primitives to set up the interface.

Prerequisite: add "TWI - Two-Wire Interface (Common API) (service)" module to application in Atmel Studio

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.144 hal\_sam\_i2c\_asf.h File Reference

ATCA Hardware abstraction layer for SAMG55 I2C over ASF drivers.

```
#include <asf.h>
#include "cryptoauthlib.h"
```

## Data Structures

- struct [i2c\\_sam\\_instance](#)

### Typedefs

- typedef void(\* **sam\_change\_baudrate**) ([ATCAIface](#) iface, uint32\_t speed)
- typedef struct [i2c\\_sam\\_instance](#) **i2c\_sam\_instance\_t**

### 22.144.1 Detailed Description

ATCA Hardware abstraction layer for SAMG55 I2C over ASF drivers.

Prerequisite: add "TWI - Two-Wire Interface (Common API) (service)" module to application in Atmel Studio

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.145 hal\_sam\_timer\_asf.c File Reference

ATCA Hardware abstraction layer for SAMD21 timer/delay over ASF drivers.

```
#include <asf.h>
#include <delay.h>
#include "atca_hal.h"
```

### Functions

- void [atca\\_delay\\_10us](#) (uint32\_t delay)  
*This function delays for a number of tens of microseconds.*
- void [atca\\_delay\\_us](#) (uint32\_t delay)  
*This function delays for a number of microseconds.*
- void [atca\\_delay\\_ms](#) (uint32\_t ms)  
*Timer API for legacy implementations.*

### 22.145.1 Detailed Description

ATCA Hardware abstraction layer for SAMD21 timer/delay over ASF drivers.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.



## 22.146 hal\_spi\_harmony.c File Reference

ATCA Hardware abstraction layer for SPI over Harmony PLIB.

```
#include <string.h>
#include <stdio.h>
#include "atca_config.h"
#include "cryptoauthlib.h"
#include "atca_hal.h"
#include "atca_device.h"
#include "definitions.h"
#include "talib/talib_defines.h"
#include "talib/talib_fce.h"
```

### Functions

- ATCA\_STATUS [hal\\_spi\\_discover\\_buses](#) (int spi\_buses[], int max\_buses)  
*discover spi buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-priori knowledge*
- ATCA\_STATUS [hal\\_spi\\_discover\\_devices](#) (int bus\_num, ATCAIfaceCfg cfg[], int \*found)  
*discover any TA10x devices on a given logical bus number*
- ATCA\_STATUS [hal\\_spi\\_init](#) (ATCAIface iface, ATCAIfaceCfg \*cfg)  
*initialize an SPI interface using given config*
- ATCA\_STATUS [hal\\_spi\\_post\\_init](#) (ATCAIface iface)  
*HAL implementation of SPI post init.*
- ATCA\_STATUS [hal\\_spi\\_select](#) (ATCAIface iface)  
*HAL implementation to assert the device chip select.*
- ATCA\_STATUS [hal\\_spi\\_deselect](#) (ATCAIface iface)  
*HAL implementation to deassert the device chip select.*
- ATCA\_STATUS [hal\\_spi\\_send](#) (ATCAIface iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*HAL implementation of SPI send over Harmony.*
- ATCA\_STATUS [hal\\_spi\\_receive](#) (ATCAIface iface, uint8\_t word\_address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*HAL implementation of SPI receive function for HARMONY SPI.*
- ATCA\_STATUS [hal\\_spi\\_control](#) (ATCAIface iface, uint8\_t option, void \*param, size\_t paramlen)  
*Perform control operations for the kit protocol.*
- ATCA\_STATUS [hal\\_spi\\_release](#) (void \*hal\_data)  
*manages reference count on given bus and releases resource if no more refences exist*

### 22.146.1 Detailed Description

ATCA Hardware abstraction layer for SPI over Harmony PLIB.

This code is structured in two parts. Part 1 is the connection of the ATCA HAL API to the physical SPI implementation. Part 2 is the Harmony SPI primitives to set up the interface.

Prerequisite: add SERCOM SPI Master Interrupt support to application in Mplab Harmony 3

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.147 hal\_swi\_gpio.c File Reference

ATCA Hardware abstraction layer for 1WIRE or SWI over GPIO.

```
#include "cryptoauthlib.h"
#include "hal_swi_gpio.h"
```

### Functions

- ATCA\_STATUS [hal\\_swi\\_gpio\\_init](#) ([ATCAIface](#) iface, [ATCAIfaceCfg](#) \*cfg)  
*initialize an GPIO interface using given config*
- ATCA\_STATUS [hal\\_swi\\_gpio\\_post\\_init](#) ([ATCAIface](#) iface)  
*HAL implementation of GPIO post init.*
- ATCA\_STATUS [hal\\_swi\\_gpio\\_send](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*HAL implementation of bit banging send over Harmony.*
- ATCA\_STATUS [hal\\_swi\\_gpio\\_receive](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*HAL implementation of bit banging receive from HARMONY.*
- ATCA\_STATUS [hal\\_swi\\_gpio\\_control](#) ([ATCAIface](#) iface, uint8\_t option, void \*param, size\_t paramlen)  
*Perform control operations.*
- ATCA\_STATUS [hal\\_swi\\_gpio\\_release](#) (void \*hal\_data)  
*releases resource if no more communication*

### 22.147.1 Detailed Description

ATCA Hardware abstraction layer for 1WIRE or SWI over GPIO.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.147.2 Function Documentation

#### 22.147.2.1 hal\_swi\_gpio\_control()

```
ATCA_STATUS hal_swi_gpio_control (
    ATCAIface iface,
    uint8_t option,
    void * param,
    size_t paramlen )
```

Perform control operations.

Parameters

in	<i>iface</i>	Interface to interact with.
in	<i>option</i>	Control parameter identifier
in	<i>param</i>	Optional pointer to parameter value
in	<i>paramlen</i>	Length of the parameter

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.147.2.2 hal\_swi\_gpio\_init()

```
ATCA_STATUS hal_swi_gpio_init (
    ATCAIface iface,
    ATCAIfaceCfg * cfg )
```

initialize an GPIO interface using given config

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.147.2.3 hal\_swi\_gpio\_post\_init()

```
ATCA_STATUS hal_swi_gpio_post_init (
    ATCAIface iface )
```

HAL implementation of GPIO post init.

Parameters

in	<i>iface</i>	ATCAIface instance
----	--------------	--------------------

Returns

ATCA\_SUCCESS

22.147.2.4 hal\_swi\_gpio\_receive()

```
ATCA_STATUS hal_swi_gpio_receive (
    ATCAIface iface,
```

## 22.147 hal\_swi\_gpio.c File Reference

---

```
uint8_t word_address,  
uint8_t * rxdata,  
uint16_t * rxlength )
```

HAL implementation of bit banging receive from HARMONY.

### Parameters

in	<i>iface</i>	Device to interact with.
in	<i>word_address</i>	device transaction type
out	<i>rxdata</i>	Data received will be returned here.
in, out	<i>rxlength</i>	As input, the size of the rxdata buffer. As output, the number of bytes received.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 22.147.2.5 hal\_swi\_gpio\_release()

```
ATCA_STATUS hal_swi_gpio_release (  
    void * hal_data )
```

releases resource if no more communication

### Parameters

in	<i>hal_data</i>	- opaque pointer to hal data structure - known only to the HAL implementation
----	-----------------	---

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 22.147.2.6 hal\_swi\_gpio\_send()

```
ATCA_STATUS hal_swi_gpio_send (  
    ATCAIface iface,  
    uint8_t word_address,  
    uint8_t * txdata,  
    int txlength )
```

HAL implementation of bit banging send over Harmony.

### Parameters

in	<i>iface</i>	instance
in	<i>word_address</i>	device transaction type
in	<i>txdata</i>	pointer to space to bytes to send
in	<i>txlength</i>	number of bytes to send

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

**22.148 hal\_swi\_gpio.h File Reference**

ATCA Hardware abstraction layer for SWI over GPIO drivers.

```
#include <stdlib.h>
#include "cryptoauthlib.h"
#include "atca_status.h"
#include "atca_hal.h"
#include "atca_config.h"
```

**Macros****Macros for Bit-Banged 1WIRE Timing**

*Times to drive bits at 230.4 kbps.*

- #define **tPUP** 0
- #define **tDSCHG** 150
- #define **tRESET** 96
- #define **tRRT** 1
- #define **tDRR** 1
- #define **tMSDR** 2
- #define **tHTSS** 150
- #define **tDACK** 2
- #define **tDACK\_DLY** atca\_delay\_us(tDACK)
- #define **tRRT\_DLY** atca\_delay\_ms(tRRT)
- #define **tDRR\_DLY** atca\_delay\_us(tDRR)
- #define **tMSDR\_DLY** atca\_delay\_us(tMSDR)
- #define **tDSCHG\_DLY** atca\_delay\_us(tDSCHG)
- #define **tRESET\_DLY** atca\_delay\_us(tRESET)
- #define **tHTSS\_DLY** atca\_delay\_us(tHTSS)
- #define **tLOW0\_MIN** 6
- #define **tLOW0\_MAX** 16
- #define **tLOW1\_MIN** 1
- #define **tLOW1\_MAX** 2
- #define **tRCV\_MIN** 4
- #define **tRCV\_MAX** 6
- #define **tBIT\_MIN** (tLOW0\_MIN + tPUP + tRCV\_MIN)
- #define **tBIT\_MAX** 75
- #define **tWAKEUP** 1
- #define **tLOW0\_TYPICAL** (tLOW0\_MIN + ((tLOW0\_MAX - tLOW0\_MIN) / 2))
- #define **tLOW1\_TYPICAL** (tLOW1\_MIN + ((tLOW1\_MAX - tLOW1\_MIN) / 2))
- #define **tBIT\_TYPICAL** (tBIT\_MIN + ((tBIT\_MAX - tBIT\_MIN) / 2))
- #define **tLOW0\_HDLY** atca\_delay\_us(11)
- #define **tRD\_HDLY** atca\_delay\_us(1)
- #define **tLOW1\_HDLY** atca\_delay\_us(1)
- #define **tRCV0\_HDLY** atca\_delay\_us(11)
- #define **tRCV1\_HDLY** atca\_delay\_us(14)
- #define **tRD\_DLY** atca\_delay\_us(1)
- #define **tHIGH\_SPEED\_DLY** atca\_delay\_us(1)
- #define **tSWIN\_DLY** atca\_delay\_us(1)
- #define **tLOW0\_DLY** atca\_delay\_us(tLOW0\_TYPICAL)
- #define **tLOW1\_DLY** atca\_delay\_us(tLOW1\_TYPICAL)
- #define **tBIT\_DLY** atca\_delay\_us(tBIT\_TYPICAL)
- #define **tRCV0\_DLY** atca\_delay\_us(tBIT\_TYPICAL - tLOW0\_TYPICAL)

- `#define tRCV1_DLY atca_delay_us(tBIT_TYPICAL - tLOW1_TYPICAL)`
- `#define send_logic0_1wire(...) send_logic_bit(__VA_ARGS__, ATCA_GPIO_LOGIC_BIT0)`
- `#define send_logic1_1wire(...) send_logic_bit(__VA_ARGS__, ATCA_GPIO_LOGIC_BIT1)`
- `#define send_ACK_1wire(...) send_logic0_1wire(__VA_ARGS__)`
- `#define send_NACK_1wire(...) send_logic1_1wire(__VA_ARGS__)`
- `#define ATCA_1WIRE_RESET_WORD_ADDR 0x00`
- `#define ATCA_1WIRE_SLEEP_WORD_ADDR 0x01`
- `#define ATCA_1WIRE_SLEEP_WORD_ADDR_ALTERNATE 0x02`
- `#define ATCA_1WIRE_COMMAND_WORD_ADDR 0x03`
- `#define ATCA_1WIRE_RESPONSE_LENGTH_SIZE 0x01`
- `#define ATCA_1WIRE_BIT_MASK 0x80`
- `#define ATCA_GPIO_WRITE 0`
- `#define ATCA_GPIO_READ 1`
- `#define ATCA_GPIO_INPUT_DIR 0`
- `#define ATCA_GPIO_OUTPUT_DIR 1`
- `#define ATCA_GPIO_LOGIC_BIT0 0`
- `#define ATCA_GPIO_LOGIC_BIT1 1`
- `#define ATCA_GPIO_ACK ATCA_GPIO_LOGIC_BIT0`
- `#define ATCA_GPIO_CLEAR 0`
- `#define ATCA_GPIO_SET 1`
- `#define ATCA_MIN_RESPONSE_LENGTH 4`
- `#define PIN_INPUT_DIR(pin) PORT_GroupInputEnable(GET_PORT_GROUP(pin), GET_PIN_↔  
MASK(pin))`
- `#define PIN_OUTPUT_DIR(pin) PORT_GroupOutputEnable(GET_PORT_GROUP(pin), GET_PIN_↔  
MASK(pin))`

## Macros for Bit-Banged SWI Timing

Times to drive bits at 230.4 kbps.

- `#define BIT_DELAY_1L atca_delay_us(4)`
- `#define BIT_DELAY_1H atca_delay_us(4)`  
*should be 4.34 us, is 4.05us*
- `#define BIT_DELAY_5 atca_delay_us(26)`
- `#define BIT_DELAY_7 atca_delay_us(34)`
- `#define RX_TX_DELAY atca_delay_us(65)`
- `#define ATCA_SWI_WAKE_WORD_ADDR ((uint8_t)0x00)`
- `#define ATCA_SWI_CMD_WORD_ADDR ((uint8_t)0x77)`
- `#define ATCA_SWI_TX_WORD_ADDR ((uint8_t)0x88)`
- `#define ATCA_SWI_IDLE_WORD_ADDR ((uint8_t)0xBB)`
- `#define ATCA_SWI_SLEEP_WORD_ADDR ((uint8_t)0xCC)`
- `#define ATCA_SWI_BIT_MASK 0x01`
- `enum protocol_type { ATCA_PROTOCOL_1WIRE , ATCA_PROTOCOL_SWI , NO_OF_PROTOCOL }`
- `enum delay_type {  
LOGIC0_1 , LOGIC0_2 , LOGIC0_3 , LOGIC0_4 ,  
LOGIC1_1 , LOGIC1_2 , NO_OF_DELAYS }`

### 22.148.1 Detailed Description

ATCA Hardware abstraction layer for SWI over GPIO drivers.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.148.2 Macro Definition Documentation

### 22.148.2.1 ATCA\_SWI\_WAKE\_WORD\_ADDR

```
#define ATCA_SWI_WAKE_WORD_ADDR ((uint8_t)0x00)
```

SWI WORD Address

### 22.148.2.2 BIT\_DELAY\_1L

```
#define BIT_DELAY_1L atca_delay_us(4)
```

delay macro for width of one pulse (start pulse or zero pulse) should be 4.34 us, is 4.05 us

### 22.148.2.3 BIT\_DELAY\_5

```
#define BIT_DELAY_5 atca_delay_us(26)
```

time to keep pin high for five pulses plus stop bit (used to bit-bang CryptoAuth 'zero' bit) should be 26.04 us, is 26.92 us

### 22.148.2.4 BIT\_DELAY\_7

```
#define BIT_DELAY_7 atca_delay_us(34)
```

time to keep pin high for seven bits plus stop bit (used to bit-bang CryptoAuth 'one' bit) should be 34.72 us, is 35.13 us

### 22.148.2.5 RX\_TX\_DELAY

```
#define RX_TX_DELAY atca_delay_us(65)
```

turn around time when switching from receive to transmit should be 93 us (Setting little less value as there would be other process before these steps)

## 22.149 hal\_swi\_uart.c File Reference

ATCA Hardware abstraction layer for SWI over UART drivers.

```
#include "cryptoauthlib.h"
```

## Functions

- ATCA\_STATUS [hal\\_swi\\_init](#) ([ATCAIface](#) iface, [ATCAIfaceCfg](#) \*cfg)  
*initialize an SWI interface using given config*
- ATCA\_STATUS [hal\\_swi\\_post\\_init](#) ([ATCAIface](#) iface)  
*HAL implementation of SWI post init.*
- ATCA\_STATUS [hal\\_swi\\_send](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*HAL implementation of SWI send command over UART.*
- ATCA\_STATUS [hal\\_swi\\_receive](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*HAL implementation of SWI receive function over UART.*
- ATCA\_STATUS [hal\\_swi\\_wake](#) ([ATCAIface](#) iface)  
*Send Wake flag via SWI.*
- ATCA\_STATUS [hal\\_swi\\_sleep](#) ([ATCAIface](#) iface)  
*Send Sleep flag via SWI.*
- ATCA\_STATUS [hal\\_swi\\_idle](#) ([ATCAIface](#) iface)  
*Send Idle flag via SWI.*
- ATCA\_STATUS [hal\\_swi\\_control](#) ([ATCAIface](#) iface, uint8\_t option, void \*param, size\_t paramlen)  
*Perform control operations for the kit protocol.*
- ATCA\_STATUS [hal\\_swi\\_release](#) (void \*hal\_data)  
*manages reference count on given bus and releases resource if no more references exist*

### 22.149.1 Detailed Description

ATCA Hardware abstraction layer for SWI over UART drivers.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.150 hal\_timer\_start.c File Reference

ATCA Hardware abstraction layer for SAMD21 I2C over START drivers.

```
#include <hal_delay.h>
#include "atca_hal.h"
```

## Functions

- void [atca\\_delay\\_us](#) (uint32\_t delay)  
*This function delays for a number of microseconds.*
- void [atca\\_delay\\_10us](#) (uint32\_t delay)  
*This function delays for a number of tens of microseconds.*
- void [atca\\_delay\\_ms](#) (uint32\_t ms)  
*Timer API for legacy implementations.*



## 22.150.1 Detailed Description

ATCA Hardware abstraction layer for SAMD21 I2C over START drivers.

Prerequisite: add SERCOM I2C Master Polled support to application in Atmel Studio

### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.151 hal\_uart\_harmony.c File Reference

ATCA Hardware abstraction layer for SWI uart over Harmony PLIB.

```
#include "atca_config.h"
#include "cryptoauthlib.h"
```

### Functions

- ATCA\_STATUS [hal\\_uart\\_init](#) ([ATCAIface](#) iface, [ATCAIfaceCfg](#) \*cfg)  
*Initialize an uart interface using given config.*
- ATCA\_STATUS [hal\\_uart\\_post\\_init](#) ([ATCAIface](#) iface)  
*HAL implementation of SWI post init.*
- ATCA\_STATUS [hal\\_uart\\_send](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*Send byte(s) via SWI.*
- ATCA\_STATUS [hal\\_uart\\_receive](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*Receive byte(s) via SWI.*
- ATCA\_STATUS [hal\\_uart\\_control](#) ([ATCAIface](#) iface, uint8\_t option, void \*param, size\_t paramlen)
- ATCA\_STATUS [hal\\_uart\\_release](#) (void \*hal\_data)  
*Manages reference count on given bus and releases resource if no more reference(s) exist.*

### Variables

- PLIB\_SWI\_SERIAL\_SETUP [serial\\_setup](#)

## 22.151.1 Detailed Description

ATCA Hardware abstraction layer for SWI uart over Harmony PLIB.

This code is structured in two parts. Part 1 is the connection of the ATCA HAL API to the physical I2C implementation. Part 2 is the Harmony UART (ring buffer mode) primitives to set up the interface.

### Copyright

(c) 2015-2018 Microchip Technology Inc. and its subsidiaries.

### 22.151.2 Function Documentation

#### 22.151.2.1 hal\_uart\_init()

```
ATCA_STATUS hal_uart_init (
    ATCAIface iface,
    ATCAIfaceCfg * cfg )
```

Initialize an uart interface using given config.

Parameters

in	<i>hal</i>	opaque pointer to HAL data
in	<i>cfg</i>	interface configuration

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.151.2.2 hal\_uart\_post\_init()

```
ATCA_STATUS hal_uart_post_init (
    ATCAIface iface )
```

HAL implementation of SWI post init.

Parameters

in	<i>iface</i>	ATCAIface instance
----	--------------	--------------------

Returns

ATCA\_SUCCESS

22.151.2.3 hal\_uart\_receive()

```
ATCA_STATUS hal_uart_receive (
    ATCAIface iface,
    uint8_t word_address,
    uint8_t * rxdata,
    uint16_t * rxlength )
```

Receive byte(s) via SWI.

Parameters

in	<i>iface</i>	Device to interact with.
in	<i>word_address</i>	device transaction type
out	<i>rxdata</i>	Data received will be returned here.
in, out	<i>rxlength</i>	As input, the size of the rxdata buffer. As output, the number of bytes received.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.151.2.4 hal\_uart\_release()

```
ATCA_STATUS hal_uart_release (
    void * hal_data )
```

Manages reference count on given bus and releases resource if no more reference(s) exist.

Parameters

in	hal_data	opaque pointer to hal data structure - known only to the HAL implementation
----	----------	---

Returns

ATCA\_SUCCESS

22.151.2.5 hal\_uart\_send()

```
ATCA_STATUS hal_uart_send (
    ATCAIface iface,
    uint8_t word_address,
    uint8_t * txdata,
    int txlength )
```

Send byte(s) via SWI.

Parameters

in	iface	interface of the logical device to send data to
in	word_address	device transaction type
in	txdata	pointer to bytes to send
in	txlength	number of bytes to send

Returns

ATCA\_SUCCESS

22.151.3 Variable Documentation

22.151.3.1 serial\_setup

```
PLIB_SWI_SERIAL_SETUP serial_setup
```

**Initial value:**

```
= {
    .parity      = PLIB_SWI_PARITY_NONE,
    .dataWidth   = PLIB_SWI_DATA_WIDTH,
    .stopBits    = PLIB_SWI_STOP_BIT
}
```

## 22.152 hal\_uc3\_i2c\_asf.c File Reference

ATCA Hardware abstraction layer for SAMV71 I2C over ASF drivers.

```
#include <asf.h>
#include <string.h>
#include <stdio.h>
#include "cryptoauthlib.h"
#include "hal_uc3_i2c_asf.h"
```

### Functions

- ATCA\_STATUS [hal\\_i2c\\_discover\\_buses](#) (int i2c\_buses[], int max\_buses)  
*discover i2c buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-prior knowledge*
- ATCA\_STATUS [hal\\_i2c\\_discover\\_devices](#) (int bus\_num, [ATCAIfaceCfg](#) cfg[], int \*found)  
*discover any CryptoAuth devices on a given logical bus number*
- ATCA\_STATUS [hal\\_i2c\\_init](#) (void \*hal, [ATCAIfaceCfg](#) \*cfg)  
*hal\_i2c\_init manages requests to initialize a physical interface. it manages use counts so when an interface has released the physical layer, it will disable the interface for some other use. You can have multiple ATCAIface instances using the same bus, and you can have multiple ATCAIface instances on multiple i2c buses, so hal\_i2c\_init manages these things and ATCAIface is abstracted from the physical details.*
- ATCA\_STATUS [hal\\_i2c\\_post\\_init](#) ([ATCAIface](#) iface)  
*HAL implementation of I2C post init.*
- ATCA\_STATUS [hal\\_i2c\\_send](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*HAL implementation of I2C send over START.*
- ATCA\_STATUS [hal\\_i2c\\_receive](#) ([ATCAIface](#) iface, uint8\_t address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*HAL implementation of I2C receive function for START I2C.*
- ATCA\_STATUS [change\\_i2c\\_speed](#) ([ATCAIface](#) iface, uint32\_t speed)  
*method to change the bus speed of I2C*
- ATCA\_STATUS [hal\\_i2c\\_wake](#) ([ATCAIface](#) iface)  
*wake up CryptoAuth device using I2C bus*
- ATCA\_STATUS [hal\\_i2c\\_idle](#) ([ATCAIface](#) iface)  
*idle CryptoAuth device using I2C bus*
- ATCA\_STATUS [hal\\_i2c\\_sleep](#) ([ATCAIface](#) iface)  
*sleep CryptoAuth device using I2C bus*
- ATCA\_STATUS [hal\\_i2c\\_release](#) (void \*hal\_data)  
*manages reference count on given bus and releases resource if no more references exist*

### 22.152.1 Detailed Description

ATCA Hardware abstraction layer for SAMV71 I2C over ASF drivers.

This code is structured in two parts. Part 1 is the connection of the ATCA HAL API to the physical I2C implementation. Part 2 is the ASF I2C primitives to set up the interface.

Prerequisite: add SERCOM I2C Master Polled support to application in Atmel Studio

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.153 hal\_uc3\_i2c\_asf.h File Reference

ATCA Hardware abstraction layer for SAMV71 I2C over ASF drivers.

```
#include <asf.h>
#include "twi.h"
```

### Data Structures

- struct [atcal2Cmaster](#)  
*this is the hal\_data for ATCA HAL for ASF SERCOM*

### Macros

- #define **MAX\_I2C\_BUSES** 3

### Typedefs

- typedef struct [atcal2Cmaster](#) **ATCAI2CMaster\_t**  
*this is the hal\_data for ATCA HAL for ASF SERCOM*

### Functions

- ATCA\_STATUS [change\\_i2c\\_speed](#) ([ATCAIface](#) iface, uint32\_t speed)  
*method to change the bus speed of I2C*

### 22.153.1 Detailed Description

ATCA Hardware abstraction layer for SAMV71 I2C over ASF drivers.

Prerequisite: add SERCOM I2C Master Polled support to application in Atmel Studio

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.154 hal\_uc3\_timer\_asf.c File Reference

ATCA Hardware abstraction layer for SAM4S I2C over ASF drivers.

```
#include <asf.h>
#include <delay.h>
#include "atca_hal.h"
```

### Functions

- void [atca\\_delay\\_us](#) (uint32\_t delay)  
*This function delays for a number of microseconds.*
- void [atca\\_delay\\_10us](#) (uint32\_t delay)  
*This function delays for a number of tens of microseconds.*
- void [atca\\_delay\\_ms](#) (uint32\_t ms)  
*Timer API for legacy implementations.*

### 22.154.1 Detailed Description

ATCA Hardware abstraction layer for SAM4S I2C over ASF drivers.

Prerequisite: add "Delay routines (service)" module to application in Atmel Studio

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.155 hal\_windows.c File Reference

ATCA Hardware abstraction layer for windows timer functions.

```
#include "atca_hal.h"
#include <windows.h>
#include <math.h>
```

### Functions

- void [hal\\_delay\\_us](#) (uint32\_t delay)  
*This function delays for a number of microseconds.*
- void [hal\\_delay\\_ms](#) (uint32\_t delay)  
*Timer API implemented at the HAL level.*
- ATCA\_STATUS [hal\\_create\\_mutex](#) (void \*\*ppMutex, const char \*pName)  
*Optional hal interfaces.*
- ATCA\_STATUS [hal\\_destroy\\_mutex](#) (void \*pMutex)
- ATCA\_STATUS [hal\\_lock\\_mutex](#) (void \*pMutex)
- ATCA\_STATUS [hal\\_unlock\\_mutex](#) (void \*pMutex)
- ATCA\_STATUS [hal\\_check\\_pid](#) (hal\_pid\_t pid)  
*Check if the pid exists in the system.*

### 22.155.1 Detailed Description

ATCA Hardware abstraction layer for windows timer functions.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.156 hal\_windows\_kit\_uart.c File Reference

ATCA Hardware abstraction layer for Windows using UART.

```
#include "cryptoauthlib.h"
#include "atca_hal.h"
#include <windows.h>
#include <stdio.h>
#include <conio.h>
#include <math.h>
#include <string.h>
```

### Data Structures

- struct [atca\\_uart\\_host\\_s](#)

### Typedefs

- typedef struct [atca\\_uart\\_host\\_s](#) [atca\\_uart\\_host\\_t](#)

### Functions

- ATCA\_STATUS [hal\\_uart\\_init](#) ([ATCAIface](#) iface, [ATCAIfaceCfg](#) \*cfg)  
*HAL implementation of UART init.*
- ATCA\_STATUS [hal\\_uart\\_post\\_init](#) ([ATCAIface](#) iface)  
*HAL implementation of UART post init.*
- ATCA\_STATUS [hal\\_uart\\_send](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)  
*HAL implementation of UART send.*
- ATCA\_STATUS [hal\\_uart\\_receive](#) ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*rxdata, uint16\_t \*rxlength)  
*HAL implementation of UART receive function.*
- ATCA\_STATUS [hal\\_uart\\_control](#) ([ATCAIface](#) iface, uint8\_t option, void \*param, size\_t paramlen)  
*Perform control operations for the UART.*
- ATCA\_STATUS [hal\\_uart\\_release](#) (void \*hal\_data)  
*manages reference count on given bus and releases resource if no more references exist*



### 22.156.1 Detailed Description

ATCA Hardware abstraction layer for Windows using UART.

Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.156.2 Function Documentation

#### 22.156.2.1 hal\_uart\_control()

```
ATCA_STATUS hal_uart_control (
    ATCAIface iface,
    uint8_t option,
    void * param,
    size_t paramlen )
```

Perform control operations for the UART.

Parameters

in	<i>iface</i>	Interface to interact with.
in	<i>option</i>	Control parameter identifier
in	<i>param</i>	Optional pointer to parameter value
in	<i>paramlen</i>	Length of the parameter

Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### 22.156.2.2 hal\_uart\_init()

```
ATCA_STATUS hal_uart_init (
    ATCAIface iface,
    ATCAIfaceCfg * cfg )
```

HAL implementation of UART init.

this implementation assumes UART SERIAL PORT peripheral has been enabled by user . It only initialize an UART interface using given config.

Parameters

in	<i>hal</i>	pointer to HAL specific data that is maintained by this HAL
in	<i>cfg</i>	pointer to HAL specific configuration data that is used to initialize this HAL

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.156.2.3 hal\_uart\_post\_init()

```
ATCA_STATUS hal_uart_post_init (
    ATCAIface iface )
```

HAL implementation of UART post init.

Parameters

in	iface	instance
----	-------	----------

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.156.2.4 hal\_uart\_receive()

```
ATCA_STATUS hal_uart_receive (
    ATCAIface iface,
    uint8_t word_address,
    uint8_t * rxdata,
    uint16_t * rxlength )
```

HAL implementation of UART receive function.

Parameters

in	iface	Device to interact with.
in	word_address	device transaction type
out	rxdata	Data received will be returned here.
in, out	rxlength	As input, the size of the rxdata buffer. As output, the number of bytes received.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.156.2.5 hal\_uart\_release()

```
ATCA_STATUS hal_uart_release (
    void * hal_data )
```

manages reference count on given bus and releases resource if no more refences exist

Parameters

in	<i>hal_data</i>	- opaque pointer to hal data structure - known only to the HAL implementation
----	-----------------	---

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.156.2.6 hal\_uart\_send()

```
ATCA_STATUS hal_uart_send (
    ATCAIface iface,
    uint8_t word_address,
    uint8_t * txdata,
    int txlength )
```

HAL implementation of UART send.

Parameters

in	<i>iface</i>	instance
in	<i>word_address</i>	transaction type
in	<i>txdata</i>	data to be send to device
in	<i>txdata</i>	pointer to space to bytes to send
in	<i>len</i>	number of bytes to send

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.157 kit\_protocol.c File Reference

Microchip Crypto Auth hardware interface object.

```
#include <stdlib.h>
#include <stdio.h>
#include <limits.h>
#include "atca_compiler.h"
#include "kit_protocol.h"
#include "atca_helpers.h"
```

Macros

- #define KIT\_MAX\_SCAN\_COUNT 8
- #define KIT\_MAX\_TX\_BUF 32

## Functions

- const char \* [kit\\_id\\_from\\_devtype](#) (ATCADeviceType devtype)
- const char \* [kit\\_interface\\_from\\_kittype](#) (ATCAKitType kittype)
- const char \* [kit\\_interface](#) (ATCAKitType kittype)

### 22.157.1 Detailed Description

Microchip Crypto Auth hardware interface object.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.158 kit\_protocol.h File Reference

```
#include "cryptoauthlib.h"
```

## Macros

- #define **KIT\_TX\_WRAP\_SIZE** (10)
- #define **KIT\_MSG\_SIZE** (32u)
- #define **KIT\_RX\_WRAP\_SIZE** (KIT\_MSG\_SIZE + 6u)

## Functions

- ATCA\_STATUS **kit\_init** ([ATCAIface](#) iface, [ATCAIfaceCfg](#) \*cfg)
- ATCA\_STATUS **kit\_post\_init** ([ATCAIface](#) iface)
- ATCA\_STATUS **kit\_send** ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*txdata, int txlength)
- ATCA\_STATUS **kit\_receive** ([ATCAIface](#) iface, uint8\_t word\_address, uint8\_t \*rxdata, uint16\_t \*rxsize)
- ATCA\_STATUS **kit\_control** ([ATCAIface](#) iface, uint8\_t option, void \*param, size\_t paramlen)
- ATCA\_STATUS **kit\_release** (void \*hal\_data)
- ATCA\_STATUS **kit\_wrap\_cmd** ([ATCAIface](#) iface, uint8\_t word\_address, const uint8\_t \*txdata, int txlen, char \*pkitcmd, int \*nkitcmd)
- ATCA\_STATUS **kit\_parse\_rsp** (const char \*pkitbuf, int nkitbuf, uint8\_t \*kitstatus, uint8\_t \*rxdata, int \*datasize)
- ATCA\_STATUS **kit\_wake** ([ATCAIface](#) iface)
- ATCA\_STATUS **kit\_idle** ([ATCAIface](#) iface)
- ATCA\_STATUS **kit\_sleep** ([ATCAIface](#) iface)
- ATCA\_STATUS **kit\_phy\_send** ([ATCAIface](#) iface, uint8\_t \*txdata, int txlength)
- ATCA\_STATUS **kit\_phy\_receive** ([ATCAIface](#) iface, uint8\_t \*rxdata, int \*rxsize)
- const char \* [kit\\_id\\_from\\_devtype](#) (ATCADeviceType devtype)
- const char \* [kit\\_interface\\_from\\_kittype](#) (ATCAKitType kittype)
- const char \* [kit\\_interface](#) (ATCAKitType kittype)

### 22.158.1 Detailed Description

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.159 swi\_uart\_samd21\_asf.c File Reference

ATXMEGA's ATCA Hardware abstraction layer for SWI interface over UART drivers.

```
#include <stdlib.h>
#include <stdio.h>
#include "swi_uart_samd21_asf.h"
#include "atca_helpers.h"
```

### Functions

- ATCA\_STATUS [swi\\_uart\\_init](#) ([ATCASWIMaster\\_t](#) \*instance)  
*Implementation of SWI UART init.*
- ATCA\_STATUS [swi\\_uart\\_deinit](#) ([ATCASWIMaster\\_t](#) \*instance)  
*Implementation of SWI UART deinit.*
- void [swi\\_uart\\_setbaud](#) ([ATCASWIMaster\\_t](#) \*instance, uint32\_t baudrate)  
*implementation of SWI UART change baudrate.*
- void [swi\\_uart\\_mode](#) ([ATCASWIMaster\\_t](#) \*instance, uint8\_t mode)  
*implementation of SWI UART change mode.*
- void [swi\\_uart\\_discover\\_buses](#) (int swi\_uart\_buses[], int max\_buses)  
*discover UART buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-priori knowledge*
- ATCA\_STATUS [swi\\_uart\\_send\\_byte](#) ([ATCASWIMaster\\_t](#) \*instance, uint8\_t data)  
*HAL implementation of SWI UART send byte over ASF. This function send one byte over UART.*
- ATCA\_STATUS [swi\\_uart\\_receive\\_byte](#) ([ATCASWIMaster\\_t](#) \*instance, uint8\_t \*data)  
*HAL implementation of SWI UART receive bytes over ASF. This function receive one byte over UART.*

### Variables

- struct port\_config [pin\\_conf](#)

### 22.159.1 Detailed Description

ATXMEGA's ATCA Hardware abstraction layer for SWI interface over UART drivers.

Prerequisite: add UART Polled support to application in Atmel Studio

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.160 swi\_uart\_samd21\_asf.h File Reference

ATXMEGA's ATCA Hardware abstraction layer for SWI interface over UART drivers.

```
#include <asf.h>
#include "cryptoauthlib.h"
```

### Data Structures

- struct [atcaSWImaster](#)  
*this is the hal\_data for ATCA HAL for ASF SERCOM*

### Macros

- #define [MAX\\_SWI\\_BUSES](#) 6
- #define [RECEIVE\\_MODE](#) 0
- #define [TRANSMIT\\_MODE](#) 1
- #define [RX\\_DELAY](#) 10
- #define [TX\\_DELAY](#) 90
- #define [DEBUG\\_PIN\\_1](#) EXT2\_PIN\_5
- #define [DEBUG\\_PIN\\_2](#) EXT2\_PIN\_6

### Typedefs

- typedef struct [atcaSWImaster](#) [ATCASWIMaster\\_t](#)  
*this is the hal\_data for ATCA HAL for ASF SERCOM*

### Functions

- ATCA\_STATUS [swi\\_uart\\_init](#) ([ATCASWIMaster\\_t](#) \*instance)  
*Implementation of SWI UART init.*
- ATCA\_STATUS [swi\\_uart\\_deinit](#) ([ATCASWIMaster\\_t](#) \*instance)  
*Implementation of SWI UART deinit.*
- void [swi\\_uart\\_setbaud](#) ([ATCASWIMaster\\_t](#) \*instance, uint32\_t baudrate)  
*implementation of SWI UART change baudrate.*
- void [swi\\_uart\\_mode](#) ([ATCASWIMaster\\_t](#) \*instance, uint8\_t mode)  
*implementation of SWI UART change mode.*
- void [swi\\_uart\\_discover\\_buses](#) (int swi\_uart\_buses[], int max\_buses)  
*discover UART buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-priori knowledge*
- ATCA\_STATUS [swi\\_uart\\_send\\_byte](#) ([ATCASWIMaster\\_t](#) \*instance, uint8\_t data)  
*HAL implementation of SWI UART send byte over ASF. This function send one byte over UART.*
- ATCA\_STATUS [swi\\_uart\\_receive\\_byte](#) ([ATCASWIMaster\\_t](#) \*instance, uint8\_t \*data)  
*HAL implementation of SWI UART receive bytes over ASF. This function receive one byte over UART.*

### 22.160.1 Detailed Description

ATXMEGA's ATCA Hardware abstraction layer for SWI interface over UART drivers.

Prerequisite: add UART Polled support to application in Atmel Studio

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.161 swi\_uart\_start.c File Reference

```
#include <stdlib.h>
#include <stdio.h>
#include <peripheral_clk_config.h>
#include "swi_uart_start.h"
#include "atca_helpers.h"
```

### Macros

- #define **USART\_BAUD\_RATE**(baud, sercom\_freq) (65536 - ((65536 \* 16.0F \* baud) / sercom\_freq))

### Functions

- ATCA\_STATUS [swi\\_uart\\_init](#) ([ATCASWIMaster\\_t](#) \*instance)  
*Implementation of SWI UART init.*
- ATCA\_STATUS [swi\\_uart\\_deinit](#) ([ATCASWIMaster\\_t](#) \*instance)  
*Implementation of SWI UART deinit.*
- void [swi\\_uart\\_setbaud](#) ([ATCASWIMaster\\_t](#) \*instance, uint32\_t baudrate)  
*implementation of SWI UART change baudrate.*
- void [swi\\_uart\\_mode](#) ([ATCASWIMaster\\_t](#) \*instance, uint8\_t mode)  
*implementation of SWI UART change mode.*
- void [swi\\_uart\\_discover\\_buses](#) (int swi\_uart\_buses[], int max\_buses)  
*discover UART buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-priori knowledge*
- ATCA\_STATUS [swi\\_uart\\_send\\_byte](#) ([ATCASWIMaster\\_t](#) \*instance, uint8\_t data)  
*HAL implementation of SWI UART send byte over ASF. This function send one byte over UART.*
- ATCA\_STATUS [swi\\_uart\\_receive\\_byte](#) ([ATCASWIMaster\\_t](#) \*instance, uint8\_t \*data)  
*HAL implementation of SWI UART receive bytes over ASF. This function receive one byte over UART.*

### 22.161.1 Detailed Description

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.



## 22.162 swi\_uart\_start.h File Reference

```
#include <stdlib.h>
#include "atmel_start.h"
#include "cryptoauthlib.h"
```

### Data Structures

- struct [atcaSWImaster](#)  
*this is the hal\_data for ATCA HAL for ASF SERCOM*

### Macros

- #define [MAX\\_SWI\\_BUSES](#) 6
- #define [RECEIVE\\_MODE](#) 0
- #define [TRANSMIT\\_MODE](#) 1
- #define [RX\\_DELAY](#) 10
- #define [TX\\_DELAY](#) 93

### Typedefs

- typedef struct [atcaSWImaster](#) [ATCASWIMaster\\_t](#)  
*this is the hal\_data for ATCA HAL for ASF SERCOM*

### Functions

- ATCA\_STATUS [swi\\_uart\\_init](#) ([ATCASWIMaster\\_t](#) \*instance)  
*Implementation of SWI UART init.*
- ATCA\_STATUS [swi\\_uart\\_deinit](#) ([ATCASWIMaster\\_t](#) \*instance)  
*Implementation of SWI UART deinit.*
- void [swi\\_uart\\_setbaud](#) ([ATCASWIMaster\\_t](#) \*instance, uint32\_t baudrate)  
*implementation of SWI UART change baudrate.*
- void [swi\\_uart\\_mode](#) ([ATCASWIMaster\\_t](#) \*instance, uint8\_t mode)  
*implementation of SWI UART change mode.*
- void [swi\\_uart\\_discover\\_buses](#) (int swi\_uart\_buses[], int max\_buses)  
*discover UART buses available for this hardware this maintains a list of logical to physical bus mappings freeing the application of the a-priori knowledge*
- ATCA\_STATUS [swi\\_uart\\_send\\_byte](#) ([ATCASWIMaster\\_t](#) \*instance, uint8\_t data)  
*HAL implementation of SWI UART send byte over ASF. This function send one byte over UART.*
- ATCA\_STATUS [swi\\_uart\\_receive\\_byte](#) ([ATCASWIMaster\\_t](#) \*instance, uint8\_t \*data)  
*HAL implementation of SWI UART receive bytes over ASF. This function receive one byte over UART.*

### 22.162.1 Detailed Description

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.163 atca\_host.c File Reference

Host side methods to support CryptoAuth computations.

```
#include "atca_host.h"
#include "crypto/atca_crypto_sw_sha2.h"
#include "cal_internal.h"
```

### 22.163.1 Detailed Description

Host side methods to support CryptoAuth computations.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.164 atca\_host.h File Reference

Definitions and Prototypes for ATCA Utility Functions.

```
#include <stdint.h>
#include "cryptoauthlib.h"
#include "calib/calib_basic.h"
#include "atca_host_config_check.h"
```

### Data Structures

- struct [atca\\_temp\\_key](#)  
*Structure to hold TempKey fields.*
- struct [atca\\_include\\_data\\_in\\_out](#)  
*Input / output parameters for function atca\_include\_data().*
- struct [atca\\_nonce\\_in\\_out](#)  
*Input/output parameters for function atca\_nonce().*
- struct [atca\\_io\\_decrypt\\_in\\_out](#)
- struct [atca\\_verify\\_mac](#)
- struct [atca\\_secureboot\\_enc\\_in\\_out](#)
- struct [atca\\_secureboot\\_mac\\_in\\_out](#)
- struct [atca\\_mac\\_in\\_out](#)  
*Input/output parameters for function atca\_mac().*
- struct [atca\\_hmac\\_in\\_out](#)  
*Input/output parameters for function atca\_hmac().*
- struct [atca\\_gen\\_dig\\_in\\_out](#)  
*Input/output parameters for function atcah\_gen\_dig().*
- struct [atca\\_diversified\\_key\\_in\\_out](#)  
*Input/output parameters for function atcah\_gendivkey().*
- struct [atca\\_write\\_mac\\_in\\_out](#)  
*Input/output parameters for function atcah\_write\_auth\_mac() and atcah\_privwrite\_auth\_mac().*

- struct [atca\\_derive\\_key\\_in\\_out](#)  
*Input/output parameters for function atcah\_derive\_key().*
- struct [atca\\_derive\\_key\\_mac\\_in\\_out](#)  
*Input/output parameters for function atcah\_derive\_key\_mac().*
- struct [atca\\_decrypt\\_in\\_out](#)  
*Input/output parameters for function atca\_decrypt().*
- struct [atca\\_check\\_mac\\_in\\_out](#)  
*Input/output parameters for function atcah\_check\_mac().*
- struct [atca\\_resp\\_mac\\_in\\_out](#)  
*Input/Output parameters for calculating the output response mac in SHA105 device. Used with the atcah\_gen\_↔  
output\_resp\_mac() function.*
- struct [atca\\_verify\\_in\\_out](#)  
*Input/output parameters for function atcah\_verify().*
- struct [atca\\_gen\\_key\\_in\\_out](#)  
*Input/output parameters for calculating the PubKey digest put into TempKey by the GenKey command with the atcah\_↔  
\_gen\_key\_msg() function.*
- struct [atca\\_sign\\_internal\\_in\\_out](#)  
*Input/output parameters for calculating the message and digest used by the Sign(internal) command. Used with the  
atcah\_sign\_internal\_msg() function.*
- struct [atca\\_session\\_key\\_in\\_out](#)  
*Input/Output paramters for calculating the session key by the nonce command. Used with the atcah\_gen\_session\_↔  
\_key() function.*
- struct [atca\\_delete\\_in\\_out](#)  
*Input/Output paramters for calculating the mac.Used with Delete command.*

## Macros

### Definitions for ATECC Message Sizes to Calculate a SHA256 Hash

"||" is the concatenation operator. The number in braces is the length of the hash input value in bytes.

- #define **ATCA\_MSG\_SIZE\_NONCE** (55)  
*RandOut{32} || NumIn{20} || OpCode{1} || Mode{1} || LSB of Param2{1}.*
- #define **ATCA\_MSG\_SIZE\_MAC** (88)  
*(Key or TempKey){32} || (Challenge or TempKey){32} || OpCode{1} || Mode{1} || Param2{2} || (OTP0\_7 or 0){8} ||  
(OTP8\_10 or 0){3} || SN8{1} || (SN4\_7 or 0){4} || SN0\_1{2} || (SN2\_3 or 0){2}*
- #define **ATCA\_MSG\_SIZE\_HMAC** (88u)
- #define **ATCA\_MSG\_SIZE\_GEN\_DIG** (96)  
*KeyId{32} || OpCode{1} || Param1{1} || Param2{2} || SN8{1} || SN0\_1{2} || 0{25} || TempKey{32}.*
- #define **ATCA\_MSG\_SIZE\_DIVERSIFIED\_KEY** (96)  
*ParentKey{32} || OtherData{4} || SN8{1} || SN0\_1{2} || 0{25} || InputData{32}.*
- #define **ATCA\_MSG\_SIZE\_DERIVE\_KEY** (96)  
*KeyId{32} || OpCode{1} || Param1{1} || Param2{2} || SN8{1} || SN0\_1{2} || 0{25} || TempKey{32}.*
- #define **ATCA\_MSG\_SIZE\_DERIVE\_KEY\_MAC** (39)  
*KeyId{32} || OpCode{1} || Param1{1} || Param2{2} || SN8{1} || SN0\_1{2}.*
- #define **ATCA\_MSG\_SIZE\_ENCRYPT\_MAC** (96)  
*KeyId{32} || OpCode{1} || Param1{1} || Param2{2} || SN8{1} || SN0\_1{2} || 0{25} || TempKey{32}.*
- #define **ATCA\_MSG\_SIZE\_SESSION\_KEY** (96)  
*TransportKey{32} || 0x15{1} || 0x00{1} || KeyId{2} || SN8{1} || SN0\_1{2} || 0{25} || Nonce{32}.*
- #define **ATCA\_MSG\_SIZE\_DELETE\_MAC** (96)  
*Hmac/SecretKey{32} || 0x13{1} || 0x00{1} || 0x0000{2} || SN8{1} || SN0\_1{2} || 0{25} || Nonce{32}.*
- #define **ATCA\_MSG\_SIZE\_RESPONSE\_MAC** (97)  
*SlotKey{32} || Opcode{1} || Param1{1} || Param2{2} || SN8{1} || SN0\_1{2} || 0{25} || client\_Resp{32} ||  
checkmac\_result{1}.*
- #define **ATCA\_MSG\_SIZE\_PRIVWRITE\_MAC** (96)  
*KeyId{32} || OpCode{1} || Param1{1} || Param2{2} || SN8{1} || SN0\_1{2} || 0{21} || PlainText{36}.*

- #define **ATCA\_COMMAND\_HEADER\_SIZE** ( 4)
- #define **ATCA\_GENDIG\_ZEROS\_SIZE** (25)
- #define **ATCA\_GENDIVKEY\_ZEROS\_SIZE** (25)
- #define **ATCA\_WRITE\_MAC\_ZEROS\_SIZE** (25)
- #define **ATCA\_DELETE\_MAC\_ZEROS\_SIZE** (25)
- #define **ATCA\_RESP\_MAC\_ZEROS\_SIZE** (25)
- #define **ATCA\_PRIVWRITE\_MAC\_ZEROS\_SIZE** (21)
- #define **ATCA\_PRIVWRITE\_PLAIN\_TEXT\_SIZE** (36)
- #define **ATCA\_DERIVE\_KEY\_ZEROS\_SIZE** (25)
- #define **ATCA\_HMAC\_BLOCK\_SIZE** (64u)
- #define **ATCA\_ENCRYPTION\_KEY\_SIZE** (64)

### Definition for TempKey Mode

- #define **MAC\_MODE\_USE\_TEMPKEY\_MASK** ((uint8\_t)0x03)  
*mode mask for MAC command when using TempKey*

## Typedefs

- typedef struct [atca\\_temp\\_key](#) **atca\_temp\_key\_t**  
*Structure to hold TempKey fields.*
- typedef struct [atca\\_nonce\\_in\\_out](#) **atca\_nonce\_in\_out\_t**
- typedef struct [atca\\_io\\_decrypt\\_in\\_out](#) **atca\_io\_decrypt\_in\_out\_t**
- typedef struct [atca\\_verify\\_mac](#) **atca\_verify\_mac\_in\_out\_t**
- typedef struct [atca\\_secureboot\\_enc\\_in\\_out](#) **atca\_secureboot\_enc\_in\_out\_t**
- typedef struct [atca\\_secureboot\\_mac\\_in\\_out](#) **atca\_secureboot\_mac\_in\_out\_t**
- typedef struct [atca\\_mac\\_in\\_out](#) **atca\_mac\_in\_out\_t**
- typedef struct [atca\\_gen\\_dig\\_in\\_out](#) **atca\_gen\_dig\_in\_out\_t**  
*Input/output parameters for function atcah\_gen\_dig().*
- typedef struct [atca\\_diversified\\_key\\_in\\_out](#) **atca\_diversified\_key\_in\_out\_t**  
*Input/output parameters for function atcah\_gendivkey().*
- typedef struct [atca\\_write\\_mac\\_in\\_out](#) **atca\_write\_mac\_in\_out\_t**  
*Input/output parameters for function atcah\_write\_auth\_mac() and atcah\_privwrite\_auth\_mac().*
- typedef struct [atca\\_check\\_mac\\_in\\_out](#) **atca\_check\_mac\_in\_out\_t**  
*Input/output parameters for function atcah\_check\_mac().*
- typedef struct [atca\\_resp\\_mac\\_in\\_out](#) **atca\_resp\_mac\_in\_out\_t**  
*Input/Output parameters for calculating the output response mac in SHA105 device. Used with the atcah\_gen↔  
output\_resp\_mac() function.*
- typedef struct [atca\\_verify\\_in\\_out](#) **atca\_verify\_in\_out\_t**
- typedef struct [atca\\_gen\\_key\\_in\\_out](#) **atca\_gen\_key\_in\_out\_t**  
*Input/output parameters for calculating the PubKey digest put into TempKey by the GenKey command with the atcah↔  
\_gen\_key\_msg() function.*
- typedef struct [atca\\_sign\\_internal\\_in\\_out](#) **atca\_sign\_internal\_in\_out\_t**  
*Input/output parameters for calculating the message and digest used by the Sign(internal) command. Used with the  
atcah\_sign\_internal\_msg() function.*
- typedef struct [atca\\_session\\_key\\_in\\_out](#) **atca\_session\_key\_in\_out\_t**  
*Input/Output paramters for calculating the session key by the nonce command. Used with the atcah\_gen\_session↔  
\_key() function.*
- typedef struct [atca\\_delete\\_in\\_out](#) **atca\_delete\_in\_out\_t**  
*Input/Output paramters for calculating the mac.Used with Delete command.*

## Functions

- ATCA\_STATUS **atcah\_nonce** (struct [atca\\_nonce\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_mac** (struct [atca\\_mac\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_check\_mac** (struct [atca\\_check\\_mac\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_hmac** (struct [atca\\_hmac\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_gen\_dig** (struct [atca\\_gen\\_dig\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_gendivkey** (struct [atca\\_diversified\\_key\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_gen\_mac** (struct [atca\\_gen\\_dig\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_write\_auth\_mac** (struct [atca\\_write\\_mac\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_privwrite\_auth\_mac** (struct [atca\\_write\\_mac\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_derive\_key** (struct [atca\\_derive\\_key\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_derive\_key\_mac** (struct [atca\\_derive\\_key\\_mac\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_decrypt** (struct [atca\\_decrypt\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_sha256** (uint32\_t len, const uint8\_t \*message, uint8\_t \*digest)
- uint8\_t \* **atcah\_include\_data** (struct [atca\\_include\\_data\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_gen\_key\_msg** (struct [atca\\_gen\\_key\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_config\_to\_sign\_internal** (ATCADeviceType device\_type, struct [atca\\_sign\\_internal\\_in\\_out](#) \*param, const uint8\_t \*config)
- ATCA\_STATUS **atcah\_sign\_internal\_msg** (ATCADeviceType device\_type, struct [atca\\_sign\\_internal\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_verify\_mac** ([atca\\_verify\\_mac\\_in\\_out\\_t](#) \*param)
- ATCA\_STATUS **atcah\_secureboot\_enc** ([atca\\_secureboot\\_enc\\_in\\_out\\_t](#) \*param)
- ATCA\_STATUS **atcah\_secureboot\_mac** ([atca\\_secureboot\\_mac\\_in\\_out\\_t](#) \*param)
- ATCA\_STATUS **atcah\_encode\_counter\_match** (uint32\_t counter\_value, uint8\_t \*counter\_match\_value)
- ATCA\_STATUS **atcah\_io\_decrypt** (struct [atca\\_io\\_decrypt\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_ecc204\_write\_auth\_mac** (struct [atca\\_write\\_mac\\_in\\_out](#) \*param)
- ATCA\_STATUS **atcah\_gen\_session\_key** ([atca\\_session\\_key\\_in\\_out\\_t](#) \*param)
- ATCA\_STATUS **atcah\_gen\_output\_resp\_mac** (struct [atca\\_resp\\_mac\\_in\\_out](#) \*param)

### 22.164.1 Detailed Description

Definitions and Prototypes for ATCA Utility Functions.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.165 atca\_host\_config\_check.h File Reference

Consistency checks for configuration options.

## Macros

- #define [ATCAH\\_INCLUDE\\_DATA](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_NONCE](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_IO\\_DECRYPT](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_VERIFY\\_MAC](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_SECUREBOOT\\_ENC](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_SECUREBOOT\\_MAC](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_MAC](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_CHECK\\_MAC](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_GEN\\_OUTPUT\\_RESP\\_MAC](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_HMAC](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_GENDIG](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_GENDIVKEY](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_GEN\\_MAC](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_WRITE\\_AUTH\\_MAC](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_PRIVWRITE\\_AUTH\\_MAC](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_DERIVE\\_KEY](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_DERIVE\\_KEY\\_MAC](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_DECRYPT](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_SHA256](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_GEN\\_KEY\\_MSG](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_CONFIG\\_TO\\_SIGN\\_INTERNAL](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_SIGN\\_INTERNAL\\_MSG](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_ENCODE\\_COUNTER\\_MATCH](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_GEN\\_SESSION\\_KEY](#) (DEFAULT\_ENABLED)
- #define [ATCAH\\_DELETE\\_MAC](#) (CALIB\_DELETE\_EN)
- #define [ATCAC\\_SW\\_SHA2\\_256](#) (DEFAULT\_ENABLED)

### 22.165.1 Detailed Description

Consistency checks for configuration options.

#### Copyright

(c) 2015-2021 Microchip Technology Inc. and its subsidiaries.

### 22.165.2 Macro Definition Documentation

#### 22.165.2.1 ATCAH\_CHECK\_MAC

```
#define ATCAH_CHECK_MAC (DEFAULT_ENABLED)
```

Requires: [ATCAH\\_CHECK\\_MAC](#) [ATCAC\\_SW\\_SHA2\\_256](#)

Supported API's: [atcah\\_check\\_mac](#)

Enable [ATCAH\\_CHECK\\_MAC](#) to perform the checkmac operation to generate client response on the host side

### 22.165.2.2 ATCAH\_CONFIG\_TO\_SIGN\_INTERNAL

```
#define ATCAH_CONFIG_TO_SIGN_INTERNAL (DEFAULT_ENABLED)
```

Requires: ATCAH\_CONFIG\_TO\_SIGN\_INTERNAL

Supported API's: atcah\_config\_to\_sign\_internal

Enable ATCAH\_CONFIG\_TO\_SIGN\_INTERNAL to populate the slot\_config, key\_config, and is\_slot\_locked fields in the [atca\\_sign\\_internal\\_in\\_out](#) structure from the provided config zone

### 22.165.2.3 ATCAH\_DECRYPT

```
#define ATCAH_DECRYPT (DEFAULT_ENABLED)
```

Requires: ATCAH\_DECRYPT

Supported API's: atcah\_decrypt

Enable ATCAH\_DECRYPT to decrypt 32-byte encrypted data received with the Read command

### 22.165.2.4 ATCAH\_DELETE\_MAC

```
#define ATCAH_DELETE_MAC (CALIB_DELETE_EN)
```

Requires: ATCAH\_DELETE\_MAC ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_delete\_mac

Enable ATCAH\_DELETE\_MAC to calculate the mac

### 22.165.2.5 ATCAH\_DERIVE\_KEY

```
#define ATCAH_DERIVE_KEY (DEFAULT_ENABLED)
```

Requires: ATCAH\_DERIVE\_KEY ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_derive\_key

Enable ATCAH\_DERIVE\_KEY to derive a key with a key and TempKey

### 22.165.2.6 ATCAH\_DERIVE\_KEY\_MAC

```
#define ATCAH_DERIVE_KEY_MAC (DEFAULT_ENABLED)
```

Requires: ATCAH\_DERIVE\_KEY\_MAC ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_derive\_key\_mac

Enable ATCAH\_DERIVE\_KEY\_MAC to calculate the input MAC for a DeriveKey command

### 22.165.2.7 ATCAH\_ENCODE\_COUNTER\_MATCH

```
#define ATCAH_ENCODE_COUNTER_MATCH (DEFAULT_ENABLED)
```

Requires: ATCAH\_ENCODE\_COUNTER\_MATCH

Supported API's: atcah\_encode\_counter\_match

Enable ATCAH\_ENCODE\_COUNTER\_MATCH to build the counter match value that needs to be stored in a slot

### 22.165.2.8 ATCAH\_GEN\_KEY\_MSG

```
#define ATCAH_GEN_KEY_MSG (DEFAULT_ENABLED)
```

Requires: ATCAH\_SHA256 ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_gen\_key\_msg

Enable ATCAH\_GEN\_KEY\_MSG to calculate the PubKey digest created by GenKey and saved to TempKey

### 22.165.2.9 ATCAH\_GEN\_MAC

```
#define ATCAH_GEN_MAC (DEFAULT_ENABLED)
```

Requires: ATCAH\_GEN\_MAC ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_gen\_mac

Enable ATCAH\_GEN\_MAC to generate mac with session key with a plain text

### 22.165.2.10 ATCAH\_GEN\_OUTPUT\_RESP\_MAC

```
#define ATCAH_GEN_OUTPUT_RESP_MAC (DEFAULT_ENABLED)
```

Requires: ATCAH\_GEN\_OUTPUT\_RESP\_MAC ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_gen\_output\_resp\_mac

Enable ATCAH\_GEN\_OUTPUT\_RESP\_MAC to generate output response mac

### 22.165.2.11 ATCAH\_GEN\_SESSION\_KEY

```
#define ATCAH_GEN_SESSION_KEY (DEFAULT_ENABLED)
```

Requires: ATCAH\_GEN\_SESSION\_KEY ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_gen\_session\_key

Enable ATCAH\_GEN\_SESSION\_KEY to calculate the session key for the ECC204



**22.165.2.12 ATCAH\_GENDIG**

```
#define ATCAH_GENDIG (DEFAULT_ENABLED)
```

Requires: ATCAH\_GENDIG ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_gen\_dig

Enable ATCAH\_GENDIG to combine the current TempKey with a stored value

**22.165.2.13 ATCAH\_GENDIVKEY**

```
#define ATCAH_GENDIVKEY (DEFAULT_ENABLED)
```

Requires: ATCAH\_GENDIVKEY ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_gendivkey

Enable ATCAH\_GENDIVKEY to generate the diversified key

**22.165.2.14 ATCAH\_HMAC**

```
#define ATCAH_HMAC (DEFAULT_ENABLED)
```

Requires: ATCAH\_HMAC ATCAC\_SW\_SHA2\_256 ATCAH\_INCLUDE\_DATA

Supported API's: atcah\_hmac

Enable ATCAH\_HMAC to generate an HMAC / SHA-256 hash of a key and other information

**22.165.2.15 ATCAH\_INCLUDE\_DATA**

```
#define ATCAH_INCLUDE_DATA (DEFAULT_ENABLED)
```

Requires: ATCAH\_INCLUDE\_DATA

Supported API's: atcah\_include\_data

Enable ATCAH\_INCLUDE\_DATA to copy otp and sn data into a command buffer

**22.165.2.16 ATCAH\_IO\_DECRYPT**

```
#define ATCAH_IO_DECRYPT (DEFAULT_ENABLED)
```

Requires: ATCAH\_IO\_DECRYPT ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_io\_decrypt

Enable ATCAH\_IO\_DECRYPT to decrypt data that's been encrypted by the IO protection key. The ECDH and KDF commands on the ATECC608 are the only ones that support this operation

### 22.165.2.17 ATCAH\_MAC

```
#define ATCAH_MAC (DEFAULT_ENABLED)
```

Requires: ATCAH\_MAC ATCAC\_SW\_SHA2\_256 ATCAH\_INCLUDE\_DATA

Supported API's: atcah\_mac

Enable ATCAH\_MAC to generate an SHA-256 digest (MAC) of a key, challenge, and other information

### 22.165.2.18 ATCAH\_NONCE

```
#define ATCAH_NONCE (DEFAULT_ENABLED)
```

Requires: ATCAH\_NONCE ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_nonce

Enable ATCAH\_NONCE to calculate host side nonce with the parameters passed

### 22.165.2.19 ATCAH\_PRIVWRITE\_AUTH\_MAC

```
#define ATCAH_PRIVWRITE_AUTH_MAC (DEFAULT_ENABLED)
```

Requires: ATCAH\_PRIVWRITE\_AUTH\_MAC ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_privwrite\_auth\_mac

Enable ATCAH\_PRIVWRITE\_AUTH\_MAC to calculate the input MAC for the PrivWrite command

### 22.165.2.20 ATCAH\_SECUREBOOT\_ENC

```
#define ATCAH_SECUREBOOT_ENC (DEFAULT_ENABLED)
```

Requires: ATCAH\_SECUREBOOT\_ENC ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_secureboot\_enc

Enable ATCAH\_SECUREBOOT\_ENC to encrypt the digest for the SecureBoot command when using the encrypted digest / validating mac option

### 22.165.2.21 ATCAH\_SECUREBOOT\_MAC

```
#define ATCAH_SECUREBOOT_MAC (DEFAULT_ENABLED)
```

Requires: ATCAH\_SECUREBOOT\_MAC ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_secureboot\_mac

Enable ATCAH\_SECUREBOOT\_MAC to calculates the expected MAC returned from the SecureBoot command when verification is a success

### 22.165.2.22 ATCAH\_SHA256

```
#define ATCAH_SHA256 (DEFAULT_ENABLED)
```

Requires: ATCAH\_SHA256 ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_sha256

Enable ATCAH\_SHA256 to create a SHA256 digest on a little-endian system

### 22.165.2.23 ATCAH\_SIGN\_INTERNAL\_MSG

```
#define ATCAH_SIGN_INTERNAL_MSG (DEFAULT_ENABLED)
```

Requires: ATCAH\_SIGN\_INTERNAL\_MSG ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_sign\_internal\_msg

Enable ATCAH\_SIGN\_INTERNAL\_MSG to build the full message that would be signed by the Sign(Internal) command

### 22.165.2.24 ATCAH\_VERIFY\_MAC

```
#define ATCAH_VERIFY_MAC (DEFAULT_ENABLED)
```

Requires: ATCAH\_VERIFY\_MAC ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_verify\_mac

Enable ATCAH\_VERIFY\_MAC to calculate the expected MAC on the host side for the Verify command

### 22.165.2.25 ATCAH\_WRITE\_AUTH\_MAC

```
#define ATCAH_WRITE_AUTH_MAC (DEFAULT_ENABLED)
```

Requires: ATCAH\_WRITE\_AUTH\_MAC ATCAC\_SW\_SHA2\_256

Supported API's: atcah\_write\_auth\_mac ECC204 specific API's: atcah\_ecc204\_write\_auth\_mac

Enable ATCAH\_WRITE\_AUTH\_MAC to calculate the input MAC for the Write command

## 22.166 atca\_jwt.c File Reference

Utilities to create and verify a JSON Web Token (JWT)

```
#include "cryptoauthlib.h"
#include "atca_helpers.h"
#include "crypto/atca_crypto_sw_sha2.h"
#include "jwt/atca_jwt.h"
#include <stdio.h>
```

### 22.166.1 Detailed Description

Utilities to create and verify a JSON Web Token (JWT)

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.167 atca\_jwt.h File Reference

Utilities to create and verify a JSON Web Token (JWT)

```
#include "cryptoauthlib.h"
```

### 22.167.1 Detailed Description

Utilities to create and verify a JSON Web Token (JWT)

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.168 atca\_mbedtls\_interface.h File Reference

Configuration Check for MbedTLS Integration Support.

```
#include "atca_config_check.h"
```

### Data Structures

- struct [atcac\\_x509\\_ctx](#)

### Macros

- #define [ATCAC\\_SHA1\\_EN](#) (DEFAULT\_ENABLED)
- #define [ATCAC\\_SHA256\\_EN](#) (DEFAULT\_ENABLED)
- #define [ATCAC\\_AES\\_CMAC\\_EN](#) (DEFAULT\_ENABLED)
- #define [ATCAC\\_AES\\_GCM\\_EN](#) (DEFAULT\_ENABLED)
- #define [ATCAC\\_PKEY\\_EN](#) (DEFAULT\_ENABLED)
- #define [HOSTLIB\\_CERT\\_EN](#) (DEFAULT\_ENABLED)

### Typedefs

- typedef struct [atcac\\_x509\\_ctx](#) [atcac\\_x509\\_ctx\\_t](#)

## 22.168.1 Detailed Description

Configuration Check for MbedTLS Integration Support.

### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.168.2 Macro Definition Documentation

### 22.168.2.1 ATCAC\_AES\_CMAC\_EN

```
#define ATCAC_AES_CMAC_EN (DEFAULT_ENABLED)
```

Indicates if this module is a provider of an AES-CMAC implementation

### 22.168.2.2 ATCAC\_AES\_GCM\_EN

```
#define ATCAC_AES_GCM_EN (DEFAULT_ENABLED)
```

Indicates if this module is a provider of an AES-GCM implementation

### 22.168.2.3 ATCAC\_PKEY\_EN

```
#define ATCAC_PKEY_EN (DEFAULT_ENABLED)
```

Indicates if this module is a provider of a generic asymmetric cryptography implementation

### 22.168.2.4 ATCAC\_SHA1\_EN

```
#define ATCAC_SHA1_EN (DEFAULT_ENABLED)
```

Indicates if this module is a provider of a SHA1 implementation

### 22.168.2.5 ATCAC\_SHA256\_EN

```
#define ATCAC_SHA256_EN (DEFAULT_ENABLED)
```

Indicates if this module is a provider of a SHA256 implementation

### 22.168.2.6 HOSTLIB\_CERT\_EN

```
#define HOSTLIB_CERT_EN (DEFAULT_ENABLED)
```

Indicates if this module is a provider of x509 certificate handling

## 22.169 atca\_mbedtls\_wrap.c File Reference

Wrapper functions to replace cryptoauthlib software crypto functions with the mbedtls equivalent.

```
#include "atca_config_check.h"
#include "mbedtls/config.h"
#include <stdlib.h>
#include "mbedtls/cmac.h"
#include "mbedtls/ctr_drbg.h"
#include "mbedtls/pk.h"
#include "mbedtls/ecdh.h"
#include "mbedtls/ecp.h"
#include "mbedtls/entropy.h"
#include "mbedtls/x509_crt.h"
#include "mbedtls/oid.h"
#include "cryptoauthlib.h"
#include "atca_mbedtls_wrap.h"
#include "atca_mbedtls_patch.h"
#include "crypto/atca_crypto_sw.h"
#include "atcacert/atcacert_client.h"
#include "atcacert/atcacert_def.h"
#include "mbedtls/pk_internal.h"
#include "atcacert/atcacert_der.h"
```

### Macros

- #define **mbedtls\_calloc** calloc
- #define **mbedtls\_free** free

### Functions

- ATCA\_STATUS [atcac\\_sw\\_random](#) (uint8\_t \*data, size\_t data\_size)  
*Return Random Bytes.*
- ATCA\_STATUS [atcac\\_aes\\_gcm\\_aad\\_update](#) (struct [atcac\\_aes\\_gcm\\_ctx](#) \*ctx, const uint8\_t \*aad, const size\_t aad\_len)  
*Update the GCM context with additional authentication data (AAD)*
- ATCA\_STATUS [atcac\\_aes\\_gcm\\_encrypt\\_start](#) (struct [atcac\\_aes\\_gcm\\_ctx](#) \*ctx, const uint8\_t \*key, const uint8\_t key\_len, const uint8\_t \*iv, const uint8\_t iv\_len)  
*Initialize an AES-GCM context.*
- ATCA\_STATUS [atcac\\_aes\\_gcm\\_encrypt\\_update](#) (struct [atcac\\_aes\\_gcm\\_ctx](#) \*ctx, const uint8\_t \*plaintext, const size\_t pt\_len, uint8\_t \*ciphertext, size\_t ct\_len)  
*Encrypt a data using the initialized context.*
- ATCA\_STATUS [atcac\\_aes\\_gcm\\_encrypt\\_finish](#) (struct [atcac\\_aes\\_gcm\\_ctx](#) \*ctx, uint8\_t \*tag, size\_t tag\_len)  
*Get the AES-GCM tag and free the context.*
- ATCA\_STATUS [atcac\\_aes\\_gcm\\_decrypt\\_start](#) (struct [atcac\\_aes\\_gcm\\_ctx](#) \*ctx, const uint8\_t \*key, const uint8\_t key\_len, const uint8\_t \*iv, const uint8\_t iv\_len)  
*Initialize an AES-GCM context for decryption.*
- ATCA\_STATUS [atcac\\_aes\\_gcm\\_decrypt\\_update](#) (struct [atcac\\_aes\\_gcm\\_ctx](#) \*ctx, const uint8\_t \*ciphertext, const size\_t ct\_len, uint8\_t \*plaintext, size\_t pt\_len)  
*Decrypt ciphertext using the initialized context.*
- ATCA\_STATUS [atcac\\_aes\\_gcm\\_decrypt\\_finish](#) (struct [atcac\\_aes\\_gcm\\_ctx](#) \*ctx, const uint8\_t \*tag, size\_t tag\_len, bool \*is\_verified)

- Compare the AES-GCM tag and free the context.*
- ATCA\_STATUS [atcac\\_sw\\_sha1\\_init](#) (struct [atcac\\_sha1\\_ctx](#) \*ctx)
- Initialize context for performing SHA1 hash in software.*
- ATCA\_STATUS [atcac\\_sw\\_sha1\\_update](#) (struct [atcac\\_sha1\\_ctx](#) \*ctx, const uint8\_t \*data, size\_t data\_size)
- Add data to a SHA1 hash.*
- ATCA\_STATUS [atcac\\_sw\\_sha1\\_finish](#) (struct [atcac\\_sha1\\_ctx](#) \*ctx, uint8\_t digest[ATCA\_SHA1\_DIGEST\_SIZE])
- Complete the SHA1 hash in software and return the digest.*
- ATCA\_STATUS [atcac\\_sw\\_sha2\\_256\\_init](#) (struct [atcac\\_sha2\\_256\\_ctx](#) \*ctx)
- Initialize context for performing SHA256 hash in software.*
- ATCA\_STATUS [atcac\\_sw\\_sha2\\_256\\_update](#) (struct [atcac\\_sha2\\_256\\_ctx](#) \*ctx, const uint8\_t \*data, size\_t data\_size)
- Add data to a SHA256 hash.*
- ATCA\_STATUS [atcac\\_sw\\_sha2\\_256\\_finish](#) (struct [atcac\\_sha2\\_256\\_ctx](#) \*ctx, uint8\_t digest[ATCA\_SHA2\_256\_DIGEST\_SIZE])
- Complete the SHA256 hash in software and return the digest.*
- ATCA\_STATUS [atcac\\_aes\\_cmac\\_init](#) (struct [atcac\\_aes\\_cmac\\_ctx](#) \*ctx, const uint8\_t \*key, const uint8\_t key\_len)
- Initialize context for performing CMAC in software.*
- ATCA\_STATUS [atcac\\_aes\\_cmac\\_update](#) (struct [atcac\\_aes\\_cmac\\_ctx](#) \*ctx, const uint8\_t \*data, const size\_t data\_size)
- Update CMAC context with input data.*
- ATCA\_STATUS [atcac\\_aes\\_cmac\\_finish](#) (struct [atcac\\_aes\\_cmac\\_ctx](#) \*ctx, uint8\_t \*cmac, size\_t \*cmac\_size)
- Finish CMAC calculation and clear the CMAC context.*
- ATCA\_STATUS [atcac\\_sha256\\_hmac\\_init](#) (struct [atcac\\_hmac\\_ctx](#) \*ctx, struct [atcac\\_sha2\\_256\\_ctx](#) \*sha256\_ctx, const uint8\_t \*key, const uint8\_t key\_len)
- Initialize context for performing HMAC (sha256) in software.*
- ATCA\_STATUS [atcac\\_sha256\\_hmac\\_update](#) (struct [atcac\\_hmac\\_ctx](#) \*ctx, const uint8\_t \*data, size\_t data\_size)
- Update HMAC context with input data.*
- ATCA\_STATUS [atcac\\_sha256\\_hmac\\_finish](#) (struct [atcac\\_hmac\\_ctx](#) \*ctx, uint8\_t \*digest, size\_t \*digest\_len)
- Finish CMAC calculation and clear the HMAC context.*
- ATCA\_STATUS [atcac\\_pk\\_init](#) (struct [atcac\\_pk\\_ctx](#) \*ctx, const uint8\_t \*buf, size\_t buflen, uint8\_t key\_type, bool pubkey)
- Set up a public/private key structure for use in asymmetric cryptographic functions.*
- ATCA\_STATUS [atcac\\_pk\\_init\\_pem](#) (struct [atcac\\_pk\\_ctx](#) \*ctx, const uint8\_t \*buf, size\_t buflen, bool pubkey)
- Set up a public/private key structure for use in asymmetric cryptographic functions.*
- ATCA\_STATUS [atcac\\_pk\\_free](#) (struct [atcac\\_pk\\_ctx](#) \*ctx)
- Free a public/private key structure.*
- ATCA\_STATUS [atcac\\_pk\\_public](#) (struct [atcac\\_pk\\_ctx](#) \*ctx, uint8\_t \*buf, size\_t \*buflen)
- Get the public key from the context.*
- ATCA\_STATUS [atcac\\_pk\\_sign](#) (struct [atcac\\_pk\\_ctx](#) \*ctx, const uint8\_t \*digest, size\_t dig\_len, uint8\_t \*signature, size\_t \*sig\_len)
- Perform a signature with the private key in the context.*
- ATCA\_STATUS [atcac\\_pk\\_verify](#) (struct [atcac\\_pk\\_ctx](#) \*ctx, const uint8\_t \*digest, size\_t dig\_len, const uint8\_t \*signature, size\_t sig\_len)
- Perform a verify using the public key in the provided context.*
- ATCA\_STATUS [atcac\\_pk\\_derive](#) (struct [atcac\\_pk\\_ctx](#) \*private\_ctx, struct [atcac\\_pk\\_ctx](#) \*public\_ctx, uint8\_t \*buf, size\_t \*buflen)
- Execute the key agreement protocol for the provided keys (if they can)*
- int [atca\\_mbedtls\\_pk\\_init\\_ext](#) (ATCADevice device, mbedtls\_pk\_context \*pkey, const uint16\_t slotid)
- Initializes an mbedtls pk context for use with EC operations.*

- int [atca\\_mbedtls\\_pk\\_init](#) (mbedtls\_pk\_context \*pkey, const uint16\_t slotid)  
*Initializes an mbedtls pk context for use with EC operations.*
- ATCA\_STATUS [atcac\\_parse\\_der](#) (struct [atcac\\_x509\\_ctx](#) \*\*cert, [cal\\_buffer](#) \*der)
- ATCA\_STATUS [atcac\\_get\\_subject](#) (const struct [atcac\\_x509\\_ctx](#) \*cert, [cal\\_buffer](#) \*cert\_subject)
- ATCA\_STATUS [atcac\\_get\\_subj\\_public\\_key](#) (const struct [atcac\\_x509\\_ctx](#) \*cert, [cal\\_buffer](#) \*subj\_public\_key)
- ATCA\_STATUS [atcac\\_get\\_subj\\_key\\_id](#) (const struct [atcac\\_x509\\_ctx](#) \*cert, [cal\\_buffer](#) \*subj\_public\_key\_id)
- ATCA\_STATUS [atcac\\_get\\_issue\\_date](#) (const struct [atcac\\_x509\\_ctx](#) \*cert, [cal\\_buffer](#) \*not\_before, uint8\_t \*fmt)
- ATCA\_STATUS [atcac\\_get\\_expire\\_date](#) (const struct [atcac\\_x509\\_ctx](#) \*cert, [cal\\_buffer](#) \*not\_after, uint8\_t \*fmt)
- ATCA\_STATUS [atcac\\_get\\_issuer](#) (const struct [atcac\\_x509\\_ctx](#) \*cert, [cal\\_buffer](#) \*issuer\_buf)
- ATCA\_STATUS [atcac\\_get\\_cert\\_sn](#) (const struct [atcac\\_x509\\_ctx](#) \*cert, [cal\\_buffer](#) \*cert\_sn)
- ATCA\_STATUS [atcac\\_get\\_auth\\_key\\_id](#) (const struct [atcac\\_x509\\_ctx](#) \*cert, [cal\\_buffer](#) \*auth\_key\_id)
- void [atcac\\_x509\\_free](#) (void \*cert)

Variables

- const mbedtls\_pk\_info\_t [atca\\_mbedtls\\_eckey\\_info](#)

22.169.1 Detailed Description

Wrapper functions to replace cryptoauthlib software crypto functions with the mbedtls equivalent.

Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

22.169.2 Function Documentation

22.169.2.1 atcac\_aes\_cmac\_finish()

```
ATCA_STATUS atcac_aes_cmac_finish (  
    struct atcac\_aes\_cmac\_ctx * ctx,  
    uint8_t * cmac,  
    size_t * cmac_size )
```

Finish CMAC calculation and clear the CMAC context.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>ctx</i>	pointer to a aes-cmac context
out	<i>cmac</i>	cmac value
in, out	<i>cmac_size</i>	length of cmac



### 22.169.2.2 atcac\_aes\_cmac\_init()

```
ATCA_STATUS atcac_aes_cmac_init (
    struct atcac_aes_cmac_ctx * ctx,
    const uint8_t * key,
    const uint8_t key_len )
```

Initialize context for performing CMAC in software.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### Parameters

in	<i>ctx</i>	pointer to a aes-cmac context
in	<i>key</i>	key value to use
in	<i>key_len</i>	length of the key

### 22.169.2.3 atcac\_aes\_cmac\_update()

```
ATCA_STATUS atcac_aes_cmac_update (
    struct atcac_aes_cmac_ctx * ctx,
    const uint8_t * data,
    const size_t data_size )
```

Update CMAC context with input data.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### Parameters

in	<i>ctx</i>	pointer to a aes-cmac context
in	<i>data</i>	input data
in	<i>data_size</i>	length of input data

### 22.169.2.4 atcac\_aes\_gcm\_aad\_update()

```
ATCA_STATUS atcac_aes_gcm_aad_update (
    struct atcac_aes_gcm_ctx * ctx,
```

```
const uint8_t * aad,  
const size_t aad_len )
```

Update the GCM context with additional authentication data (AAD)

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>ctx</i>	AES-GCM Context
in	<i>aad</i>	Additional Authentication Data
in	<i>aad_len</i>	Length of AAD

22.169.2.5 atcac\_aes\_gcm\_decrypt\_finish()

```
ATCA_STATUS atcac_aes_gcm_decrypt_finish (  
    struct atcac_aes_gcm_ctx * ctx,  
    const uint8_t * tag,  
    size_t tag_len,  
    bool * is_verified )
```

Compare the AES-GCM tag and free the context.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>ctx</i>	AES-GCM Context
in	<i>tag</i>	GCM Tag to Verify
in	<i>tag_len</i>	Length of the GCM tag
out	<i>is_verified</i>	Tag verified as matching

22.169.2.6 atcac\_aes\_gcm\_decrypt\_start()

```
ATCA_STATUS atcac_aes_gcm_decrypt_start (  
    struct atcac_aes_gcm_ctx * ctx,  
    const uint8_t * key,  
    const uint8_t key_len,  
    const uint8_t * iv,  
    const uint8_t iv_len )
```

Initialize an AES-GCM context for decryption.

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

**Parameters**

in	<i>ctx</i>	AES-GCM Context
in	<i>key</i>	AES Key
in	<i>key_len</i>	Length of the AES key - should be 16 or 32
in	<i>iv</i>	Initialization vector input
in	<i>iv_len</i>	Length of the initialization vector

**22.169.2.7 atcac\_aes\_gcm\_decrypt\_update()**

```
ATCA_STATUS atcac_aes_gcm_decrypt_update (
    struct atcac_aes_gcm_ctx * ctx,
    const uint8_t * ciphertext,
    const size_t ct_len,
    uint8_t * plaintext,
    size_t * pt_len )
```

Decrypt ciphertext using the initialized context.

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

**Parameters**

in	<i>ctx</i>	AES-GCM Context
in	<i>ciphertext</i>	Ciphertext to decrypt
in	<i>ct_len</i>	Length of the ciphertext
out	<i>plaintext</i>	Resulting decrypted plaintext
in, out	<i>pt_len</i>	Length of the plaintext buffer

**22.169.2.8 atcac\_aes\_gcm\_encrypt\_finish()**

```
ATCA_STATUS atcac_aes_gcm_encrypt_finish (
    struct atcac_aes_gcm_ctx * ctx,
    uint8_t * tag,
    size_t tag_len )
```

Get the AES-GCM tag and free the context.

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

## Parameters

in	<i>ctx</i>	AES-GCM Context
out	<i>tag</i>	GCM Tag Result
in	<i>tag_len</i>	Length of the GCM tag

**22.169.2.9 atcac\_aes\_gcm\_encrypt\_start()**

```
ATCA_STATUS atcac_aes_gcm_encrypt_start (
    struct atcac_aes_gcm_ctx * ctx,
    const uint8_t * key,
    const uint8_t key_len,
    const uint8_t * iv,
    const uint8_t iv_len )
```

Initialize an AES-GCM context.

## Returns

ATCA\_SUCCESS on success, otherwise an error code.

## Parameters

in	<i>ctx</i>	AES-GCM Context
in	<i>key</i>	AES Key
in	<i>key_len</i>	Length of the AES key - should be 16 or 32
in	<i>iv</i>	Initialization vector input
in	<i>iv_len</i>	Length of the initialization vector

**22.169.2.10 atcac\_aes\_gcm\_encrypt\_update()**

```
ATCA_STATUS atcac_aes_gcm_encrypt_update (
    struct atcac_aes_gcm_ctx * ctx,
    const uint8_t * plaintext,
    const size_t pt_len,
    uint8_t * ciphertext,
    size_t * ct_len )
```

Encrypt a data using the initialized context.

## Returns

ATCA\_SUCCESS on success, otherwise an error code.

## Parameters

in	<i>ctx</i>	AES-GCM Context
in	<i>plaintext</i>	Input buffer to encrypt
in	<i>pt_len</i>	Length of the input
out	<i>ciphertext</i>	Output buffer
in, out	<i>ct_len</i>	Length of the ciphertext buffer

**22.169.2.11 atcac\_pk\_derive()**

```

ATCA_STATUS atcac_pk_derive (
    struct atcac_pk_ctx * private_ctx,
    struct atcac_pk_ctx * public_ctx,
    uint8_t * buf,
    size_t * buflen )

```

Execute the key agreement protocol for the provided keys (if they can)

## Returns

ATCA\_SUCCESS on success, otherwise an error code.

**22.169.2.12 atcac\_pk\_free()**

```

ATCA_STATUS atcac_pk_free (
    struct atcac_pk_ctx * ctx )

```

Free a public/private key structure.

## Returns

ATCA\_SUCCESS on success, otherwise an error code.

## Parameters

in	<i>ctx</i>	pointer to a pk context
----	------------	-------------------------

**22.169.2.13 atcac\_pk\_init()**

```

ATCA_STATUS atcac_pk_init (
    struct atcac_pk_ctx * ctx,

```

```
const uint8_t * buf,  
size_t buflen,  
uint8_t key_type,  
bool pubkey )
```

Set up a public/private key structure for use in asymmetric cryptographic functions.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>ctx</i>	pointer to a pk context
in	<i>buf</i>	buffer containing a pem encoded key
in	<i>buflen</i>	length of the input buffer
in	<i>pubkey</i>	buffer is a public key

22.169.2.14 atcac\_pk\_init\_pem()

```
ATCA_STATUS atcac_pk_init_pem (  
    struct atcac_pk_ctx * ctx,  
    const uint8_t * buf,  
    size_t buflen,  
    bool pubkey )
```

Set up a public/private key structure for use in asymmetric cryptographic functions.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>ctx</i>	pointer to a pk context
in	<i>buf</i>	buffer containing a pem encoded key
in	<i>buflen</i>	length of the input buffer
in	<i>pubkey</i>	buffer is a public key

22.169.2.15 atcac\_pk\_public()

```
ATCA_STATUS atcac_pk_public (  
    struct atcac_pk_ctx * ctx,  
    uint8_t * buf,  
    size_t * buflen )
```

Get the public key from the context.

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

**22.169.2.16 atcac\_pk\_sign()**

```
ATCA_STATUS atcac_pk_sign (
    struct atcac_pk_ctx * ctx,
    const uint8_t * digest,
    size_t dig_len,
    uint8_t * signature,
    size_t * sig_len )
```

Perform a signature with the private key in the context.

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

**22.169.2.17 atcac\_pk\_verify()**

```
ATCA_STATUS atcac_pk_verify (
    struct atcac_pk_ctx * ctx,
    const uint8_t * digest,
    size_t dig_len,
    const uint8_t * signature,
    size_t sig_len )
```

Perform a verify using the public key in the provided context.

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

**22.169.2.18 atcac\_sha256\_hmac\_finish()**

```
ATCA_STATUS atcac_sha256_hmac_finish (
    struct atcac_hmac_ctx * ctx,
    uint8_t * digest,
    size_t * digest_len )
```

Finish CMAC calculation and clear the HMAC context.

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

### Parameters

in	<i>ctx</i>	pointer to a sha256-hmac context
out	<i>digest</i>	hmac value
in, out	<i>digest_len</i>	length of hmac

### 22.169.2.19 atcac\_sha256\_hmac\_init()

```
ATCA_STATUS atcac_sha256_hmac_init (
    struct atcac_hmac_ctx * ctx,
    struct atcac_sha2_256_ctx * sha256_ctx,
    const uint8_t * key,
    const uint8_t key_len )
```

Initialize context for performing HMAC (sha256) in software.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### Parameters

in	<i>ctx</i>	pointer to a sha256-hmac context
in	<i>sha256_ctx</i>	pointer to a sha256 context
in	<i>key</i>	key value to use
in	<i>key_len</i>	length of the key

### 22.169.2.20 atcac\_sha256\_hmac\_update()

```
ATCA_STATUS atcac_sha256_hmac_update (
    struct atcac_hmac_ctx * ctx,
    const uint8_t * data,
    size_t data_size )
```

Update HMAC context with input data.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### Parameters

in	<i>ctx</i>	pointer to a sha256-hmac context
in	<i>data</i>	input data
in	<i>data_size</i>	length of input data



### 22.169.2.21 atcac\_sw\_random()

```
ATCA_STATUS atcac_sw_random (
    uint8_t * data,
    size_t data_size )
```

Return Random Bytes.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### 22.169.2.22 atcac\_sw\_sha1\_finish()

```
ATCA_STATUS atcac_sw_sha1_finish (
    struct atcac_sha1_ctx * ctx,
    uint8_t digest[ATCA_SHA1_DIGEST_SIZE] )
```

Complete the SHA1 hash in software and return the digest.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

#### Parameters

in	<i>ctx</i>	pointer to a hash context
out	<i>digest</i>	output buffer (20 bytes)

### 22.169.2.23 atcac\_sw\_sha1\_init()

```
ATCA_STATUS atcac_sw_sha1_init (
    struct atcac_sha1_ctx * ctx )
```

Initialize context for performing SHA1 hash in software.

#### Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>ctx</i>	pointer to a hash context
----	------------	---------------------------

22.169.2.24 atcac\_sw\_sha1\_update()

```
ATCA_STATUS atcac_sw_sha1_update (
    struct atcac_sha1_ctx * ctx,
    const uint8_t * data,
    size_t data_size )
```

Add data to a SHA1 hash.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>ctx</i>	pointer to a hash context
in	<i>data</i>	input data buffer
in	<i>data_size</i>	input data length

22.169.2.25 atcac\_sw\_sha2\_256\_finish()

```
ATCA_STATUS atcac_sw_sha2_256_finish (
    struct atcac_sha2_256_ctx * ctx,
    uint8_t digest[ATCA_SHA2_256_DIGEST_SIZE] )
```

Complete the SHA256 hash in software and return the digest.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>ctx</i>	pointer to a hash context
out	<i>digest</i>	output buffer (32 bytes)

22.169.2.26 atcac\_sw\_sha2\_256\_init()

```
ATCA_STATUS atcac_sw_sha2_256_init (
    struct atcac_sha2_256_ctx * ctx )
```

Initialize context for performing SHA256 hash in software.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	ctx	pointer to a hash context
----	-----	---------------------------

22.169.2.27 atcac\_sw\_sha2\_256\_update()

```
ATCA_STATUS atcac_sw_sha2_256_update (
    struct atcac_sha2_256_ctx * ctx,
    const uint8_t * data,
    size_t data_size )
```

Add data to a SHA256 hash.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	ctx	pointer to a hash context
in	data	input data buffer
in	data_size	input data length

22.169.3 Variable Documentation

22.169.3.1 atca\_mbedtls\_eckey\_info

```
const mbedtls_pk_info_t atca_mbedtls_eckey_info
```

Initial value:

```
= {
    MBEDTLS_PK_ECKEY,
    "EC",
```

```
atca_mbedtls_eckey_get_bitlen,  
atca_mbedtls_eckey_can_do,  
atca_mbedtls_eckey_verify,  
atca_mbedtls_eckey_sign,  
NULL,  
NULL,  
atca_mbedtls_eckey_check_pair,  
atca_mbedtls_eckey_alloc,  
atca_mbedtls_eckey_free,  
atca_mbedtls_eckey_debug,  
}
```

## 22.170 atca\_openssl\_interface.c File Reference

Crypto abstraction functions for external host side cryptography.

```
#include "cryptoauthlib.h"  
#include "crypto/atca_crypto_sw.h"  
#include <openssl/bn.h>  
#include <openssl/bio.h>  
#include <openssl/cmac.h>  
#include <openssl/ec.h>  
#include <openssl/evp.h>  
#include <openssl/hmac.h>  
#include <openssl/pem.h>  
#include <openssl/rand.h>  
#include <openssl/x509.h>  
#include <openssl/x509v3.h>
```

### Data Structures

- struct [atca\\_evp\\_ctx](#)

### Functions

- ATCA\_STATUS [atcac\\_sw\\_random](#) (uint8\_t \*data, size\_t data\_size)  
*Return Random Bytes.*
- ATCA\_STATUS [atcac\\_aes\\_gcm\\_aad\\_update](#) (struct [atcac\\_aes\\_gcm\\_ctx](#) \*ctx, const uint8\_t \*aad, const size\_t aad\_len)  
*Update the GCM context with additional authentication data (AAD)*
- ATCA\_STATUS [atcac\\_aes\\_gcm\\_encrypt\\_start](#) (struct [atcac\\_aes\\_gcm\\_ctx](#) \*ctx, const uint8\_t \*key, const uint8\_t key\_len, const uint8\_t \*iv, const uint8\_t iv\_len)  
*Initialize an AES-GCM context.*
- ATCA\_STATUS [atcac\\_aes\\_gcm\\_encrypt\\_update](#) (struct [atcac\\_aes\\_gcm\\_ctx](#) \*ctx, const uint8\_t \*plaintext, const size\_t pt\_len, uint8\_t \*ciphertext, size\_t \*ct\_len)  
*Encrypt a data using the initialized context.*
- ATCA\_STATUS [atcac\\_aes\\_gcm\\_encrypt\\_finish](#) (struct [atcac\\_aes\\_gcm\\_ctx](#) \*ctx, uint8\_t \*tag, size\_t tag\_len)  
*Get the AES-GCM tag and free the context.*
- ATCA\_STATUS [atcac\\_aes\\_gcm\\_decrypt\\_start](#) (struct [atcac\\_aes\\_gcm\\_ctx](#) \*ctx, const uint8\_t \*key, const uint8\_t key\_len, const uint8\_t \*iv, const uint8\_t iv\_len)  
*Initialize an AES-GCM context for decryption.*
- ATCA\_STATUS [atcac\\_aes\\_gcm\\_decrypt\\_update](#) (struct [atcac\\_aes\\_gcm\\_ctx](#) \*ctx, const uint8\_t \*ciphertext, const size\_t ct\_len, uint8\_t \*plaintext, size\_t \*pt\_len)

- Decrypt ciphertext using the initialized context.*
- ATCA\_STATUS [atcac\\_aes\\_gcm\\_decrypt\\_finish](#) (struct [atcac\\_aes\\_gcm\\_ctx](#) \*ctx, const uint8\_t \*tag, size\_t tag\_len, bool \*is\_verified)
- Compare the AES-GCM tag and free the context.*
- ATCA\_STATUS [atcac\\_sw\\_sha1\\_init](#) (struct [atcac\\_sha1\\_ctx](#) \*ctx)
- Initialize context for performing SHA1 hash in software.*
- ATCA\_STATUS [atcac\\_sw\\_sha1\\_update](#) (struct [atcac\\_sha1\\_ctx](#) \*ctx, const uint8\_t \*data, size\_t data\_size)
- Add data to a SHA1 hash.*
- ATCA\_STATUS [atcac\\_sw\\_sha1\\_finish](#) (struct [atcac\\_sha1\\_ctx](#) \*ctx, uint8\_t digest[ATCA\_SHA1\_DIGEST\_SIZE])
- Complete the SHA1 hash in software and return the digest.*
- ATCA\_STATUS [atcac\\_sw\\_sha2\\_256\\_init](#) (struct [atcac\\_sha2\\_256\\_ctx](#) \*ctx)
- Initialize context for performing SHA256 hash in software.*
- ATCA\_STATUS [atcac\\_sw\\_sha2\\_256\\_update](#) (struct [atcac\\_sha2\\_256\\_ctx](#) \*ctx, const uint8\_t \*data, size\_t data\_size)
- Add data to a SHA256 hash.*
- ATCA\_STATUS [atcac\\_sw\\_sha2\\_256\\_finish](#) (struct [atcac\\_sha2\\_256\\_ctx](#) \*ctx, uint8\_t digest[ATCA\_SHA2\_256\_DIGEST\_SIZE])
- Complete the SHA256 hash in software and return the digest.*
- ATCA\_STATUS [atcac\\_aes\\_cmac\\_init](#) (struct [atcac\\_aes\\_cmac\\_ctx](#) \*ctx, const uint8\_t \*key, const uint8\_t key\_len)
- Initialize context for performing CMAC in software.*
- ATCA\_STATUS [atcac\\_aes\\_cmac\\_update](#) (struct [atcac\\_aes\\_cmac\\_ctx](#) \*ctx, const uint8\_t \*data, const size\_t data\_size)
- Update CMAC context with input data.*
- ATCA\_STATUS [atcac\\_aes\\_cmac\\_finish](#) (struct [atcac\\_aes\\_cmac\\_ctx](#) \*ctx, uint8\_t \*cmac, size\_t \*cmac\_size)
- Finish CMAC calculation and clear the CMAC context.*
- ATCA\_STATUS [atcac\\_sha256\\_hmac\\_init](#) (struct [atcac\\_hmac\\_ctx](#) \*ctx, struct [atcac\\_sha2\\_256\\_ctx](#) \*sha256\_ctx, const uint8\_t \*key, const uint8\_t key\_len)
- Initialize context for performing HMAC (sha256) in software.*
- ATCA\_STATUS [atcac\\_sha256\\_hmac\\_update](#) (struct [atcac\\_hmac\\_ctx](#) \*ctx, const uint8\_t \*data, size\_t data\_size)
- Update HMAC context with input data.*
- ATCA\_STATUS [atcac\\_sha256\\_hmac\\_finish](#) (struct [atcac\\_hmac\\_ctx](#) \*ctx, uint8\_t \*digest, size\_t \*digest\_len)
- Finish CMAC calculation and clear the HMAC context.*
- ATCA\_STATUS [atcac\\_pk\\_init](#) (struct [atcac\\_pk\\_ctx](#) \*ctx, const uint8\_t \*buf, size\_t buflen, uint8\_t key\_type, bool pubkey)
- Set up a public/private key structure for use in asymmetric cryptographic functions.*
- ATCA\_STATUS [atcac\\_pk\\_init\\_pem](#) (struct [atcac\\_pk\\_ctx](#) \*ctx, const uint8\_t \*buf, size\_t buflen, bool pubkey)
- Set up a public/private key structure for use in asymmetric cryptographic functions.*
- ATCA\_STATUS [atcac\\_pk\\_free](#) (struct [atcac\\_pk\\_ctx](#) \*ctx)
- Free a public/private key structure.*
- ATCA\_STATUS [atcac\\_pk\\_public](#) (struct [atcac\\_pk\\_ctx](#) \*ctx, uint8\_t \*buf, size\_t \*buflen)
- Get the public key from the context.*
- ATCA\_STATUS [atcac\\_pk\\_sign](#) (struct [atcac\\_pk\\_ctx](#) \*ctx, const uint8\_t \*digest, size\_t dig\_len, uint8\_t \*signature, size\_t \*sig\_len)
- Perform a signature with the private key in the context.*
- ATCA\_STATUS [atcac\\_pk\\_verify](#) (struct [atcac\\_pk\\_ctx](#) \*ctx, const uint8\_t \*digest, size\_t dig\_len, const uint8\_t \*signature, size\_t sig\_len)
- Perform a verify using the public key in the provided context.*
- ATCA\_STATUS [atcac\\_pk\\_derive](#) (struct [atcac\\_pk\\_ctx](#) \*private\_ctx, struct [atcac\\_pk\\_ctx](#) \*public\_ctx, uint8\_t \*buf, size\_t \*buflen)

*Execute the key agreement protocol for the provided keys (if they can)*

- ATCA\_STATUS **atcac\_parse\_der** (struct [atcac\\_x509\\_ctx](#) \*\*cert, [cal\\_buffer](#) \*der)
- ATCA\_STATUS **atcac\_get\_subject** (const struct [atcac\\_x509\\_ctx](#) \*cert, [cal\\_buffer](#) \*cert\_subject)
- ATCA\_STATUS **atcac\_get\_subj\_public\_key** (const struct [atcac\\_x509\\_ctx](#) \*cert, [cal\\_buffer](#) \*subj\_public\_key)
- ATCA\_STATUS **atcac\_get\_subj\_key\_id** (const struct [atcac\\_x509\\_ctx](#) \*cert, [cal\\_buffer](#) \*subj\_public\_key\_id)
- ATCA\_STATUS **atcac\_get\_issuer** (const struct [atcac\\_x509\\_ctx](#) \*cert, [cal\\_buffer](#) \*issuer\_buf)
- ATCA\_STATUS **atcac\_get\_auth\_key\_id** (const struct [atcac\\_x509\\_ctx](#) \*cert, [cal\\_buffer](#) \*auth\_key\_id)
- ATCA\_STATUS **atcac\_get\_issue\_date** (const struct [atcac\\_x509\\_ctx](#) \*cert, [cal\\_buffer](#) \*not\_before, uint8\_t \*fmt)
- ATCA\_STATUS **atcac\_get\_expire\_date** (const struct [atcac\\_x509\\_ctx](#) \*cert, [cal\\_buffer](#) \*not\_after, uint8\_t \*fmt)
- ATCA\_STATUS **atcac\_get\_cert\_sn** (const struct [atcac\\_x509\\_ctx](#) \*cert, [cal\\_buffer](#) \*cert\_sn)
- void **atcac\_x509\_free** (void \*cert)

## 22.170.1 Detailed Description

Crypto abstraction functions for external host side cryptography.

### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.170.2 Function Documentation

### 22.170.2.1 atcac\_aes\_cmac\_finish()

```
ATCA_STATUS atcac_aes_cmac_finish (  
    struct atcac\_aes\_cmac\_ctx * ctx,  
    uint8_t * cmac,  
    size_t * cmac_size )
```

Finish CMAC calculation and clear the CMAC context.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### Parameters

in	<a href="#">ctx</a>	pointer to a aes-cmac context
out	<a href="#">cmac</a>	cmac value
in, out	<a href="#">cmac_size</a>	length of cmac

### 22.170.2.2 atcac\_aes\_cmac\_init()

```
ATCA_STATUS atcac_aes_cmac_init (
    struct atcac_aes_cmac_ctx * ctx,
    const uint8_t * key,
    const uint8_t key_len )
```

Initialize context for performing CMAC in software.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>ctx</i>	pointer to a aes-cmac context
in	<i>key</i>	key value to use
in	<i>key_len</i>	length of the key

### 22.170.2.3 atcac\_aes\_cmac\_update()

```
ATCA_STATUS atcac_aes_cmac_update (
    struct atcac_aes_cmac_ctx * ctx,
    const uint8_t * data,
    const size_t data_size )
```

Update CMAC context with input data.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>ctx</i>	pointer to a aes-cmac context
in	<i>data</i>	input data
in	<i>data_size</i>	length of input data

### 22.170.2.4 atcac\_aes\_gcm\_aad\_update()

```
ATCA_STATUS atcac_aes_gcm_aad_update (
    struct atcac_aes_gcm_ctx * ctx,
    const uint8_t * aad,
    const size_t aad_len )
```

Update the GCM context with additional authentication data (AAD)

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### Parameters

in	<i>ctx</i>	AES-GCM Context
in	<i>aad</i>	Additional Authentication Data
in	<i>aad_len</i>	Length of AAD

### 22.170.2.5 atcac\_aes\_gcm\_decrypt\_finish()

```
ATCA_STATUS atcac_aes_gcm_decrypt_finish (
    struct atcac_aes_gcm_ctx * ctx,
    const uint8_t * tag,
    size_t tag_len,
    bool * is_verified )
```

Compare the AES-GCM tag and free the context.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### Parameters

in	<i>ctx</i>	AES-GCM Context
in	<i>tag</i>	GCM Tag to Verify
in	<i>tag_len</i>	Length of the GCM tag
out	<i>is_verified</i>	Tag verified as matching

### 22.170.2.6 atcac\_aes\_gcm\_decrypt\_start()

```
ATCA_STATUS atcac_aes_gcm_decrypt_start (
    struct atcac_aes_gcm_ctx * ctx,
    const uint8_t * key,
    const uint8_t key_len,
    const uint8_t * iv,
    const uint8_t iv_len )
```

Initialize an AES-GCM context for decryption.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.



## Parameters

in	<i>ctx</i>	AES-GCM Context
in	<i>key</i>	AES Key
in	<i>key_len</i>	Length of the AES key - should be 16 or 32
in	<i>iv</i>	Initialization vector input
in	<i>iv_len</i>	Length of the initialization vector

**22.170.2.7 atcac\_aes\_gcm\_decrypt\_update()**

```
ATCA_STATUS atcac_aes_gcm_decrypt_update (
    struct atcac_aes_gcm_ctx * ctx,
    const uint8_t * ciphertext,
    const size_t ct_len,
    uint8_t * plaintext,
    size_t * pt_len )
```

Decrypt ciphertext using the initialized context.

## Returns

ATCA\_SUCCESS on success, otherwise an error code.

## Parameters

in	<i>ctx</i>	AES-GCM Context
in	<i>ciphertext</i>	Ciphertext to decrypt
in	<i>ct_len</i>	Length of the ciphertext
out	<i>plaintext</i>	Resulting decrypted plaintext
in, out	<i>pt_len</i>	Length of the plaintext buffer

**22.170.2.8 atcac\_aes\_gcm\_encrypt\_finish()**

```
ATCA_STATUS atcac_aes_gcm_encrypt_finish (
    struct atcac_aes_gcm_ctx * ctx,
    uint8_t * tag,
    size_t tag_len )
```

Get the AES-GCM tag and free the context.

## Returns

ATCA\_SUCCESS on success, otherwise an error code.

## Parameters

in	<i>ctx</i>	AES-GCM Context
out	<i>tag</i>	GCM Tag Result
in	<i>tag_len</i>	Length of the GCM tag

**22.170.2.9 atcac\_aes\_gcm\_encrypt\_start()**

```
ATCA_STATUS atcac_aes_gcm_encrypt_start (
    struct atcac_aes_gcm_ctx * ctx,
    const uint8_t * key,
    const uint8_t key_len,
    const uint8_t * iv,
    const uint8_t iv_len )
```

Initialize an AES-GCM context.

## Returns

ATCA\_SUCCESS on success, otherwise an error code.

## Parameters

in	<i>ctx</i>	AES-GCM Context
in	<i>key</i>	AES Key
in	<i>key_len</i>	Length of the AES key - should be 16 or 32
in	<i>iv</i>	Initialization vector input
in	<i>iv_len</i>	Length of the initialization vector

**22.170.2.10 atcac\_aes\_gcm\_encrypt\_update()**

```
ATCA_STATUS atcac_aes_gcm_encrypt_update (
    struct atcac_aes_gcm_ctx * ctx,
    const uint8_t * plaintext,
    const size_t pt_len,
    uint8_t * ciphertext,
    size_t * ct_len )
```

Encrypt a data using the initialized context.

## Returns

ATCA\_SUCCESS on success, otherwise an error code.

## Parameters

in	<i>ctx</i>	AES-GCM Context
in	<i>plaintext</i>	Input buffer to encrypt
in	<i>pt_len</i>	Length of the input
out	<i>ciphertext</i>	Output buffer
in, out	<i>ct_len</i>	Length of the ciphertext buffer

**22.170.2.11 atcac\_pk\_derive()**

```
ATCA_STATUS atcac_pk_derive (
    struct atcac_pk_ctx * private_ctx,
    struct atcac_pk_ctx * public_ctx,
    uint8_t * buf,
    size_t * buflen )
```

Execute the key agreement protocol for the provided keys (if they can)

## Returns

ATCA\_SUCCESS on success, otherwise an error code.

**22.170.2.12 atcac\_pk\_free()**

```
ATCA_STATUS atcac_pk_free (
    struct atcac_pk_ctx * ctx )
```

Free a public/private key structure.

## Returns

ATCA\_SUCCESS on success, otherwise an error code.

## Parameters

in	<i>ctx</i>	pointer to a pk context
----	------------	-------------------------

**22.170.2.13 atcac\_pk\_init()**

```
ATCA_STATUS atcac_pk_init (
    struct atcac_pk_ctx * ctx,
```

```
const uint8_t * buf,  
size_t buflen,  
uint8_t key_type,  
bool pubkey )
```

Set up a public/private key structure for use in asymmetric cryptographic functions.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>ctx</i>	pointer to a pk context
in	<i>buf</i>	buffer containing a pem encoded key
in	<i>buflen</i>	length of the input buffer
in	<i>pubkey</i>	buffer is a public key

22.170.2.14 atcac\_pk\_init\_pem()

```
ATCA_STATUS atcac_pk_init_pem (  
    struct atcac_pk_ctx * ctx,  
    const uint8_t * buf,  
    size_t buflen,  
    bool pubkey )
```

Set up a public/private key structure for use in asymmetric cryptographic functions.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>ctx</i>	pointer to a pk context
in	<i>buf</i>	buffer containing a pem encoded key
in	<i>buflen</i>	length of the input buffer
in	<i>pubkey</i>	buffer is a public key

22.170.2.15 atcac\_pk\_public()

```
ATCA_STATUS atcac_pk_public (  
    struct atcac_pk_ctx * ctx,  
    uint8_t * buf,  
    size_t * buflen )
```

Get the public key from the context.

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

**22.170.2.16 atcac\_pk\_sign()**

```
ATCA_STATUS atcac_pk_sign (
    struct atcac_pk_ctx * ctx,
    const uint8_t * digest,
    size_t dig_len,
    uint8_t * signature,
    size_t * sig_len )
```

Perform a signature with the private key in the context.

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

**22.170.2.17 atcac\_pk\_verify()**

```
ATCA_STATUS atcac_pk_verify (
    struct atcac_pk_ctx * ctx,
    const uint8_t * digest,
    size_t dig_len,
    const uint8_t * signature,
    size_t sig_len )
```

Perform a verify using the public key in the provided context.

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

**22.170.2.18 atcac\_sha256\_hmac\_finish()**

```
ATCA_STATUS atcac_sha256_hmac_finish (
    struct atcac_hmac_ctx * ctx,
    uint8_t * digest,
    size_t * digest_len )
```

Finish CMAC calculation and clear the HMAC context.

**Returns**

ATCA\_SUCCESS on success, otherwise an error code.

## Parameters

in	<i>ctx</i>	pointer to a sha256-hmac context
out	<i>digest</i>	hmac value
in, out	<i>digest_len</i>	length of hmac

**22.170.2.19 atcac\_sha256\_hmac\_init()**

```
ATCA_STATUS atcac_sha256_hmac_init (
    struct atcac_hmac_ctx * ctx,
    struct atcac_sha2_256_ctx * sha256_ctx,
    const uint8_t * key,
    const uint8_t key_len )
```

Initialize context for performing HMAC (sha256) in software.

## Returns

ATCA\_SUCCESS on success, otherwise an error code.

## Parameters

in	<i>ctx</i>	pointer to a sha256-hmac context
in	<i>sha256_ctx</i>	pointer to a sha256 context
in	<i>key</i>	key value to use
in	<i>key_len</i>	length of the key

**22.170.2.20 atcac\_sha256\_hmac\_update()**

```
ATCA_STATUS atcac_sha256_hmac_update (
    struct atcac_hmac_ctx * ctx,
    const uint8_t * data,
    size_t data_size )
```

Update HMAC context with input data.

## Returns

ATCA\_SUCCESS on success, otherwise an error code.

## Parameters

in	<i>ctx</i>	pointer to a sha256-hmac context
in	<i>data</i>	input data
in	<i>data_size</i>	length of input data

22.170.2.21   **atcac\_sw\_random()**

```
ATCA_STATUS atcac_sw_random (
    uint8_t * data,
    size_t data_size )
```

Return Random Bytes.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

22.170.2.22   **atcac\_sw\_sha1\_finish()**

```
ATCA_STATUS atcac_sw_sha1_finish (
    struct atcac_sha1_ctx * ctx,
    uint8_t digest[ATCA_SHA1_DIGEST_SIZE] )
```

Complete the SHA1 hash in software and return the digest.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	<i>ctx</i>	pointer to a hash context
out	<i>digest</i>	output buffer (20 bytes)

22.170.2.23   **atcac\_sw\_sha1\_init()**

```
ATCA_STATUS atcac_sw_sha1_init (
    struct atcac_sha1_ctx * ctx )
```

Initialize context for performing SHA1 hash in software.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

### Parameters

in	<i>ctx</i>	pointer to a hash context
----	------------	---------------------------

### 22.170.2.24 atcac\_sw\_sha1\_update()

```
ATCA_STATUS atcac_sw_sha1_update (
    struct atcac_sha1_ctx * ctx,
    const uint8_t * data,
    size_t data_size )
```

Add data to a SHA1 hash.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### Parameters

in	<i>ctx</i>	pointer to a hash context
in	<i>data</i>	input data buffer
in	<i>data_size</i>	input data length

### 22.170.2.25 atcac\_sw\_sha2\_256\_finish()

```
ATCA_STATUS atcac_sw_sha2_256_finish (
    struct atcac_sha2_256_ctx * ctx,
    uint8_t digest[ATCA_SHA2_256_DIGEST_SIZE] )
```

Complete the SHA256 hash in software and return the digest.

### Returns

ATCA\_SUCCESS on success, otherwise an error code.

### Parameters

in	<i>ctx</i>	pointer to a hash context
out	<i>digest</i>	output buffer (32 bytes)



22.170.2.26 atcac\_sw\_sha2\_256\_init()

```
ATCA_STATUS atcac_sw_sha2_256_init (
    struct atcac_sha2_256_ctx * ctx )
```

Initialize context for performing SHA256 hash in software.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	ctx	pointer to a hash context
----	-----	---------------------------

22.170.2.27 atcac\_sw\_sha2\_256\_update()

```
ATCA_STATUS atcac_sw_sha2_256_update (
    struct atcac_sha2_256_ctx * ctx,
    const uint8_t * data,
    size_t data_size )
```

Add data to a SHA256 hash.

Returns

ATCA\_SUCCESS on success, otherwise an error code.

Parameters

in	ctx	pointer to a hash context
in	data	input data buffer
in	data_size	input data length

22.171 atca\_openssl\_interface.h File Reference

OpenSSL Integration Support.

```
#include "atca_config_check.h"
```

Data Structures

- struct [atcac\\_sha1\\_ctx](#)

- struct [atcac\\_sha2\\_256\\_ctx](#)
- struct [atcac\\_aes\\_cmac\\_ctx](#)
- struct [atcac\\_hmac\\_ctx](#)
- struct [atcac\\_pk\\_ctx](#)
- struct [atcac\\_x509\\_ctx](#)

### Macros

- #define [ATCAC\\_SHA1\\_EN](#) (DEFAULT\_ENABLED)
- #define [ATCAC\\_SHA256\\_EN](#) (DEFAULT\_ENABLED)
- #define [ATCAC\\_AES\\_CMAC\\_EN](#) (DEFAULT\_ENABLED)
- #define [ATCAC\\_AES\\_GCM\\_EN](#) (DEFAULT\_ENABLED)
- #define [ATCAC\\_PKEY\\_EN](#) (DEFAULT\_ENABLED)
- #define [HOSTLIB\\_CERT\\_EN](#) (DEFAULT\_ENABLED)

### Typedefs

- typedef struct [atcac\\_sha1\\_ctx](#) [atcac\\_sha1\\_ctx\\_t](#)
- typedef struct [atcac\\_sha2\\_256\\_ctx](#) [atcac\\_sha2\\_256\\_ctx\\_t](#)
- typedef struct [atcac\\_aes\\_cmac\\_ctx](#) [atcac\\_aes\\_cmac\\_ctx\\_t](#)
- typedef struct [atcac\\_hmac\\_ctx](#) [atcac\\_hmac\\_ctx\\_t](#)
- typedef struct [atcac\\_pk\\_ctx](#) [atcac\\_pk\\_ctx\\_t](#)
- typedef struct [atcac\\_x509\\_ctx](#) [atcac\\_x509\\_ctx\\_t](#)

### 22.171.1 Detailed Description

OpenSSL Integration Support.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.171.2 Macro Definition Documentation

#### 22.171.2.1 ATCAC\_AES\_CMAC\_EN

```
#define ATCAC_AES_CMAC_EN (DEFAULT_ENABLED)
```

Indicates if this module is a provider of an AES-CMAC implementation

#### 22.171.2.2 ATCAC\_AES\_GCM\_EN

```
#define ATCAC_AES_GCM_EN (DEFAULT_ENABLED)
```

Indicates if this module is a provider of an AES-GCM implementation

### 22.171.2.3 ATCAC\_PKEY\_EN

```
#define ATCAC_PKEY_EN (DEFAULT_ENABLED)
```

Indicates if this module is a provider of a generic asymmetric cryptography implementation

### 22.171.2.4 ATCAC\_SHA1\_EN

```
#define ATCAC_SHA1_EN (DEFAULT_ENABLED)
```

Indicates if this module is a provider of a SHA1 implementation

### 22.171.2.5 ATCAC\_SHA256\_EN

```
#define ATCAC_SHA256_EN (DEFAULT_ENABLED)
```

Indicates if this module is a provider of a SHA256 implementation

### 22.171.2.6 HOSTLIB\_CERT\_EN

```
#define HOSTLIB_CERT_EN (DEFAULT_ENABLED)
```

Indicates if this module is a provider of x509 certificate handling

## 22.172 pkcs11\_attrib.c File Reference

PKCS11 Library Object Attributes Handling.

```
#include "pkcs11_config.h"
#include "pkcs11_attrib.h"
#include "cryptoauthlib.h"
#include "pkcs11_session.h"
```

### Functions

- CK\_RV [pkcs11\\_attrib\\_fill](#) (CK\_ATTRIBUTE\_PTR pAttribute, const void \*pData, const CK\_ULONG ulSize)  
*Perform the nessasary checks and copy data into an attribute structure.*
- CK\_RV [pkcs11\\_attrib\\_value](#) (CK\_ATTRIBUTE\_PTR pAttribute, const CK\_ULONG ulValue, const CK\_ULONG ulSize)  
*Helper function to write a numerical value to an attribute buffer.*
- CK\_RV [pkcs11\\_attrib\\_false](#) (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV [pkcs11\\_attrib\\_true](#) (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV [pkcs11\\_attrib\\_empty](#) (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)

### 22.172.1 Detailed Description

PKCS11 Library Object Attributes Handling.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.173 pkcs11\_attrib.h File Reference

PKCS11 Library Object Attribute Handling.

```
#include "cryptoauthlib.h"
#include "cryptoki.h"
#include "pkcs11_session.h"
```

### Data Structures

- struct [pkcs11\\_attrib\\_model\\_s](#)

### Typedefs

- typedef CK\_RV(\* [attrib\\_f](#)) (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- typedef struct [pkcs11\\_attrib\\_model\\_s](#) **pkcs11\_attrib\_model**
- typedef struct [pkcs11\\_attrib\\_model\\_s](#) \* **pkcs11\_attrib\_model\_ptr**

### Functions

- CK\_RV [pkcs11\\_attrib\\_fill](#) (CK\_ATTRIBUTE\_PTR pAttribute, const void \*pData, const CK\_ULONG ulSize)  
*Perform the nessasary checks and copy data into an attribute structure.*
- CK\_RV **pkcs11\_attrib\_value** (CK\_ATTRIBUTE\_PTR pAttribute, const CK\_ULONG ulValue, const CK\_↔  
ULONG ulSize)  
*Helper function to write a numerical value to an attribute buffer.*
- CK\_RV **pkcs11\_attrib\_false** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV **pkcs11\_attrib\_true** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV **pkcs11\_attrib\_empty** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)

### 22.173.1 Detailed Description

PKCS11 Library Object Attribute Handling.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.173.2 Typedef Documentation

### 22.173.2.1 attrib\_f

```
typedef CK_RV(* attrib_f) (CK_VOID_PTR pObject, CK_ATTRIBUTE_PTR pAttribute, pkcs11\_session\_ctx\_ptr
pSession)
```

Populate an attribute based on the "object"

## 22.174 pkcs11\_cert.c File Reference

PKCS11 Library Certificate Handling.

```
#include "cryptoauthlib.h"
#include "atcacert/atcacert_def.h"
#include "atcacert/atcacert_client.h"
#include "pkcs11_config.h"
#include "pkcs11_debug.h"
#include "pkcs11_token.h"
#include "pkcs11_cert.h"
#include "pkcs11_os.h"
#include "pkcs11_util.h"
#include "pkcs11_slot.h"
```

### Functions

- CK\_RV **pkcs11\_cert\_load** ([pkcs11\\_object\\_ptr](#) pObject, CK\_ATTRIBUTE\_PTR pAttribute, [ATCADevice](#) device)
- CK\_RV **pkcs11\_cert\_x509\_write** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV **pkcs11\_cert\_clear\_session\_cache** ([pkcs11\\_session\\_ctx\\_ptr](#) session\_ctx)
- CK\_RV **pkcs11\_cert\_clear\_object\_cache** ([pkcs11\\_object\\_ptr](#) pObject)

### Variables

- const [pkcs11\\_attr\\_model](#) [pkcs11\\_cert\\_x509public\\_attributes](#) []
- const CK\_ULONG **pkcs11\_cert\_x509public\_attributes\_count** = (CK\_ULONG)(sizeof([pkcs11\\_cert\\_x509public\\_attributes](#)) / sizeof([pkcs11\\_cert\\_x509public\\_attributes](#) [0]))
- const [pkcs11\\_attr\\_model](#) [pkcs11\\_cert\\_wtlspublic\\_attributes](#) []
- const CK\_ULONG **pkcs11\_cert\_wtlspublic\_attributes\_count** = (CK\_ULONG)(sizeof([pkcs11\\_cert\\_wtlspublic\\_attributes](#)) / sizeof([pkcs11\\_cert\\_wtlspublic\\_attributes](#) [0]))
- const [pkcs11\\_attr\\_model](#) [pkcs11\\_cert\\_x509\\_attributes](#) []
- const CK\_ULONG **pkcs11\_cert\_x509\_attributes\_count** = (CK\_ULONG)(sizeof([pkcs11\\_cert\\_x509\\_attributes](#)) / sizeof([pkcs11\\_cert\\_x509\\_attributes](#) [0]))

### 22.174.1 Detailed Description

PKCS11 Library Certificate Handling.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.175 pkcs11\_cert.h File Reference

PKCS11 Library Certificate Handling.

```
#include "pkcs11_object.h"
```

### Functions

- CK\_RV **pkcs11\_cert\_x509\_write** (CK\_VOID\_PTR pObj, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV **pkcs11\_cert\_load** (pkcs11\_object\_ptr pObj, CK\_ATTRIBUTE\_PTR pAttribute, [ATCADevice](#) device)
- CK\_RV **pkcs11\_cert\_clear\_session\_cache** ([pkcs11\\_session\\_ctx\\_ptr](#) session\_ctx)
- CK\_RV **pkcs11\_cert\_clear\_object\_cache** (pkcs11\_object\_ptr pObj)

### Variables

- const [pkcs11\\_attr\\_model](#) [pkcs11\\_cert\\_x509public\\_attributes](#) []
- const CK\_ULONG **pkcs11\_cert\_x509public\_attributes\_count**
- const [pkcs11\\_attr\\_model](#) [pkcs11\\_cert\\_wtlspublic\\_attributes](#) []
- const CK\_ULONG **pkcs11\_cert\_wtlspublic\_attributes\_count**
- const [pkcs11\\_attr\\_model](#) [pkcs11\\_cert\\_x509\\_attributes](#) []
- const CK\_ULONG **pkcs11\_cert\_x509\_attributes\_count**

### 22.175.1 Detailed Description

PKCS11 Library Certificate Handling.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.176 pkcs11\_config.c File Reference

PKCS11 Library Configuration.

```
#include <stdbool.h>
#include "cryptoauthlib.h"
#include "pkcs11_config.h"
#include "pkcs11_debug.h"
#include "pkcs11_slot.h"
#include "pkcs11_object.h"
#include "pkcs11_key.h"
#include "pkcs11_cert.h"
#include "pkcs11_os.h"
#include "pkcs11_util.h"
#include <limits.h>
#include <stdio.h>
#include <ctype.h>
#include <stdlib.h>
#include <errno.h>
#include <fcntl.h>
#include <dirent.h>
```

### Data Structures

- struct [pkcs11\\_conf\\_filedata\\_s](#)

### Macros

- #define **PKCS11\_CONFIG\_U8\_MAX** 0xFFL
- #define **PKCS11\_CONFIG\_U16\_MAX** 0xFFFFL
- #define **PKCS11\_CONFIG\_U32\_MAX** 0xFFFFFFFFL

### Typedefs

- typedef struct [pkcs11\\_conf\\_filedata\\_s](#) **pkcs11\_conf\_filedata**
- typedef struct [pkcs11\\_conf\\_filedata\\_s](#) \* **pkcs11\_conf\_filedata\_ptr**

### Functions

- void **pkcs11\_config\_init\_private** (pkcs11\_object\_ptr pObject, const char \*label, size\_t len)
- void **pkcs11\_config\_init\_public** (pkcs11\_object\_ptr pObject, const char \*label, size\_t len)
- void **pkcs11\_config\_init\_secret** (pkcs11\_object\_ptr pObject, const char \*label, size\_t len, size\_t keylen)
- void **pkcs11\_config\_init\_cert** (pkcs11\_object\_ptr pObject, const char \*label, size\_t len)
- void **pkcs11\_config\_split\_string** (char \*s, char splitter, int \*argc, char \*argv[])
- CK\_RV **pkcs11\_config\_cert** (pkcs11\_lib\_ctx\_ptr pLibCtx, pkcs11\_slot\_ctx\_ptr pSlot, pkcs11\_object\_ptr pObject, CK\_ATTRIBUTE\_PTR pLabel)
- CK\_RV **pkcs11\_config\_key** (pkcs11\_lib\_ctx\_ptr pLibCtx, pkcs11\_slot\_ctx\_ptr pSlot, pkcs11\_object\_ptr pObject, CK\_ATTRIBUTE\_PTR pLabel)
- CK\_RV **pkcs11\_config\_remove\_object** (pkcs11\_lib\_ctx\_ptr pLibCtx, pkcs11\_slot\_ctx\_ptr pSlot, pkcs11\_object\_ptr pObject)
- CK\_RV **pkcs11\_config\_load\_objects** (pkcs11\_slot\_ctx\_ptr slot\_ctx)
- CK\_RV **pkcs11\_config\_load** (pkcs11\_slot\_ctx\_ptr slot\_ctx)

### 22.176.1 Detailed Description

PKCS11 Library Configuration.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.177 pkcs11\_debug.c File Reference

PKCS11 Library Debugging.

```
#include "pkcs11_config.h"
#include "pkcs11_debug.h"
#include "pkcs11_os.h"
#include "atca_helpers.h"
```

### 22.177.1 Detailed Description

PKCS11 Library Debugging.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.178 pkcs11\_debug.h File Reference

PKCS11 Library Debugging.

```
#include "pkcs11_config.h"
```

#### Macros

- `#define PKCS11_DEBUG_NOFILE(...)`
- `#define PKCS11_DEBUG(...)`
- `#define PKCS11_DEBUG_RETURN(x) { return x; }`
- `#define pkcs11_debug_attributes(x, y)`

### 22.178.1 Detailed Description

PKCS11 Library Debugging.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.



## 22.179 pkcs11\_digest.h File Reference

PKCS11 Library Digest (SHA256) Handling.

```
#include "cryptoki.h"
```

### Functions

- CK\_RV **pkcs11\_digest\_init** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism)  
*Initializes a message-digesting operation using the specified mechanism in the specified session.*
- CK\_RV **pkcs11\_digest** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pDigest, CK\_ULONG\_PTR pulDigestLen)  
*Digest the specified data in a one-pass operation and return the resulting digest.*
- CK\_RV **pkcs11\_digest\_update** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ulPartLen)  
*Continues a multiple-part digesting operation.*
- CK\_RV **pkcs11\_digest\_final** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pDigest, CK\_ULONG\_PTR pulDigestLen)  
*Finishes a multiple-part digesting operation.*

### 22.179.1 Detailed Description

PKCS11 Library Digest (SHA256) Handling.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.180 pkcs11\_encrypt.c File Reference

PKCS11 Library Encrypt Support.

```
#include "cryptoauthlib.h"  
#include <limits.h>  
#include "pkcs11_config.h"  
#include "pkcs11_encrypt.h"  
#include "pkcs11_debug.h"  
#include "pkcs11_init.h"  
#include "pkcs11_object.h"  
#include "pkcs11_session.h"  
#include "pkcs11_util.h"  
#include "pkcs11_slot.h"
```

## Functions

- CK\_RV **pkcs11\_encrypt\_init** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hObject)
- CK\_RV **pkcs11\_encrypt** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pEncryptedData, CK\_ULONG\_PTR pulEncryptedDataLen)
- CK\_RV **pkcs11\_encrypt\_update** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pEncryptedData, CK\_ULONG\_PTR pulEncryptedDataLen)
- CK\_RV **pkcs11\_encrypt\_final** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pEncryptedData, CK\_ULONG\_PTR pulEncryptedDataLen)

*Finishes a multiple-part encryption operation.*

- CK\_RV **pkcs11\_decrypt\_init** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hObject)
- CK\_RV **pkcs11\_decrypt** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pEncryptedData, CK\_ULONG ulEncryptedDataLen, CK\_BYTE\_PTR pData, CK\_ULONG\_PTR pulDataLen)
- CK\_RV **pkcs11\_decrypt\_update** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pEncryptedData, CK\_ULONG ulEncryptedDataLen, CK\_BYTE\_PTR pData, CK\_ULONG\_PTR pulDataLen)
- CK\_RV **pkcs11\_decrypt\_final** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG\_PTR pulDataLen)

*Finishes a multiple-part decryption operation.*

### 22.180.1 Detailed Description

PKCS11 Library Encrypt Support.

Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.181 pkcs11\_encrypt.h File Reference

PKCS11 Library AES Support.

```
#include "cryptoki.h"
```

## Functions

- CK\_RV **pkcs11\_encrypt\_init** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hObject)
- CK\_RV **pkcs11\_encrypt** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pEncryptedData, CK\_ULONG\_PTR pulEncryptedDataLen)
- CK\_RV **pkcs11\_encrypt\_update** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pEncryptedData, CK\_ULONG\_PTR pulEncryptedDataLen)
- CK\_RV **pkcs11\_encrypt\_final** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pEncryptedData, CK\_ULONG\_PTR pulEncryptedDataLen)

*Finishes a multiple-part encryption operation.*

- CK\_RV **pkcs11\_decrypt\_init** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hObject)
- CK\_RV **pkcs11\_decrypt** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pEncryptedData, CK\_ULONG ulEncryptedDataLen, CK\_BYTE\_PTR pData, CK\_ULONG\_PTR pulDataLen)
- CK\_RV **pkcs11\_decrypt\_update** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pEncryptedData, CK\_ULONG ulEncryptedDataLen, CK\_BYTE\_PTR pData, CK\_ULONG\_PTR pulDataLen)
- CK\_RV **pkcs11\_decrypt\_final** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG\_PTR pulDataLen)

*Finishes a multiple-part decryption operation.*

### 22.181.1 Detailed Description

PKCS11 Library AES Support.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.182 pkcs11\_find.c File Reference

PKCS11 Library Object Find/Searching.

```
#include "cryptoauthlib.h"
#include "atcacert/atcacert_def.h"
#include "pkcs11_config.h"
#include "pkcs11_debug.h"
#include "pkcs11_init.h"
#include "pkcs11_os.h"
#include "pkcs11_slot.h"
#include "pkcs11_session.h"
#include "pkcs11_find.h"
#include "pkcs11_util.h"
#include "pkcs11_cert.h"
```

### Functions

- CK\_RV **pkcs11\_find\_init** (CK\_SESSION\_HANDLE hSession, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount)
- CK\_RV **pkcs11\_find\_continue** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE\_PTR phObject, CK\_ULONG ulMaxObjectCount, CK\_ULONG\_PTR pulObjectCount)
- CK\_RV **pkcs11\_find\_finish** (CK\_SESSION\_HANDLE hSession)
- CK\_RV **pkcs11\_find\_get\_attribute** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hObject, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount)

### 22.182.1 Detailed Description

PKCS11 Library Object Find/Searching.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.183 pkcs11\_find.h File Reference

PKCS11 Library Object Find/Searching.

```
#include "cryptoki.h"
#include "pkcs11_object.h"
```

## Functions

- CK\_RV **pkcs11\_find\_init** (CK\_SESSION\_HANDLE hSession, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount)
- CK\_RV **pkcs11\_find\_continue** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE\_PTR phObject, CK\_ULONG ulMaxObjectCount, CK\_ULONG\_PTR pulObjectCount)
- CK\_RV **pkcs11\_find\_finish** (CK\_SESSION\_HANDLE hSession)
- CK\_RV **pkcs11\_find\_get\_attribute** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hObject, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount)

### 22.183.1 Detailed Description

PKCS11 Library Object Find/Searching.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.184 pkcs11\_info.c File Reference

PKCS11 Library Information Functions.

```
#include "cryptoauthlib.h"
#include "pkcs11_config.h"
#include "pkcs11_init.h"
#include "pkcs11_slot.h"
#include "pkcs11_session.h"
#include "pkcs11_util.h"
#include "pkcs11_info.h"
#include <stdio.h>
```

## Functions

- CK\_RV **pkcs11\_get\_lib\_info** (CK\_INFO\_PTR pInfo)  
*Obtains general information about Cryptoki.*

## Variables

- const char **pkcs11\_lib\_manufacturer\_id** [] = "Microchip Technology Inc"
- const char **pkcs11\_lib\_description** [] = "Cryptoauthlib PKCS11 Interface"

### 22.184.1 Detailed Description

PKCS11 Library Information Functions.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.185 pkcs11\_info.h File Reference

PKCS11 Library Information Functions.

```
#include "cryptoki.h"
```

### Functions

- CK\_RV **pkcs11\_get\_lib\_info** (CK\_INFO\_PTR pInfo)  
*Obtains general information about Cryptoki.*

### Variables

- const char **pkcs11\_lib\_manufacturer\_id** []
- const char **pkcs11\_lib\_description** []

### 22.185.1 Detailed Description

PKCS11 Library Information Functions.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.186 pkcs11\_init.c File Reference

PKCS11 Library Init/Deinit.

```
#include "atca_device.h"  
#include "hal/atca_hal.h"  
#include "pkcs11_config.h"  
#include "pkcs11_debug.h"  
#include "pkcs11_init.h"  
#include "pkcs11_os.h"  
#include "pkcs11_slot.h"  
#include "pkcs11_object.h"  
#include "pkcs11_session.h"  
#include "cryptoauthlib.h"
```

## Functions

- `pkcs11_lib_ctx_ptr` **pkcs11\_get\_context** (void)  
*Retrieve the current library context.*
- CK\_RV **pkcs11\_lock\_context** (pkcs11\_lib\_ctx\_ptr pContext)
- CK\_RV **pkcs11\_unlock\_context** (pkcs11\_lib\_ctx\_ptr pContext)
- CK\_RV **pkcs11\_lock\_device** (pkcs11\_lib\_ctx\_ptr pContext)
- CK\_RV **pkcs11\_unlock\_device** (pkcs11\_lib\_ctx\_ptr pContext)
- CK\_RV **pkcs11\_lock\_both** (pkcs11\_lib\_ctx\_ptr pContext)
- CK\_RV **pkcs11\_unlock\_both** (pkcs11\_lib\_ctx\_ptr pContext)
- CK\_RV **pkcs11\_init\_check** (pkcs11\_lib\_ctx\_ptr \*ppContext, CK\_BBOOL lock)  
*Check if the library is initialized properly.*
- CK\_RV **pkcs11\_init** ([CK\\_C\\_INITIALIZE\\_ARGS](#) const \*pInitArgs)  
*Initializes the PKCS11 API Library for Cryptoauthlib.*
- CK\_RV **pkcs11\_deinit** (CK\_VOID\_PTR pReserved)

### 22.186.1 Detailed Description

PKCS11 Library Init/Deinit.

Copyright (c) 2017 Microchip Technology Inc. All rights reserved.

Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.187 pkcs11\_init.h File Reference

PKCS11 Library Initialization & Context.

```
#include "atca_compiler.h"
#include "pkcs11_config.h"
#include "pkcs11_os.h"
#include "cryptoauthlib.h"
```

## Data Structures

- struct [pkcs11\\_dev\\_ctx](#)
- struct [pkcs11\\_dev\\_res](#)
- struct [pkcs11\\_dev\\_state](#)
- struct [pkcs11\\_lib\\_ctx\\_s](#)

## Macros

- `#define` **PKCS11\_AES\_OP** (0x0u)
- `#define` **PKCS11\_DIGEST\_OP\_0** (0x1u)
- `#define` **PKCS11\_DIGEST\_OP\_1** (0x2u)
- `#define` **PKCS11\_AUTH\_OP\_0** (0x3u)
- `#define` **PKCS11\_AUTH\_OP\_1** (0x4u)
- `#define` **PKCS11\_MAX\_DEV\_CTX** (5u)
- `#define` **MAX\_DIGEST\_SESSIONS** (2u)
- `#define` **MAX\_AUTH\_SESSIONS** (2u)

## Typedefs

- typedef struct `pkcs11_lib_ctx_s` `pkcs11_lib_ctx`

## Functions

- CK\_RV `pkcs11_init` (`CK_C_INITIALIZE_ARGS` const \*pInitArgs)  
*Initializes the PKCS11 API Library for Cryptoauthlib.*
- CK\_RV `pkcs11_deinit` (`CK_VOID_PTR` pReserved)
- CK\_RV `pkcs11_init_check` (`pkcs11_lib_ctx_ptr` \*ppContext, `CK_BBOOL` lock)  
*Check if the library is initialized properly.*
- `pkcs11_lib_ctx_ptr` `pkcs11_get_context` (void)  
*Retrieve the current library context.*
- CK\_RV `pkcs11_lock_context` (`pkcs11_lib_ctx_ptr` pContext)
- CK\_RV `pkcs11_unlock_context` (`pkcs11_lib_ctx_ptr` pContext)
- CK\_RV `pkcs11_lock_device` (`pkcs11_lib_ctx_ptr` pContext)
- CK\_RV `pkcs11_unlock_device` (`pkcs11_lib_ctx_ptr` pContext)
- CK\_RV `pkcs11_lock_both` (`pkcs11_lib_ctx_ptr` pContext)
- CK\_RV `pkcs11_unlock_both` (`pkcs11_lib_ctx_ptr` pContext)

### 22.187.1 Detailed Description

PKCS11 Library Initialization & Context.

Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.187.2 Typedef Documentation

#### 22.187.2.1 `pkcs11_lib_ctx`

```
typedef struct pkcs11_lib_ctx_s pkcs11_lib_ctx
```

Library Context

## 22.188 `pkcs11_key.c` File Reference

PKCS11 Library Key Object Handling.

```
#include "cryptoauthlib.h"
#include "crypto/atca_crypto_sw_sha1.h"
#include "pkcs11_config.h"
#include "pkcs11_debug.h"
#include "pkcs11_token.h"
#include "pkcs11_attrib.h"
#include "pkcs11_key.h"
#include "pkcs11_session.h"
#include "pkcs11_slot.h"
#include "pkcs11_util.h"
#include "pkcs11_os.h"
```

## Functions

- const [pkcs11\\_ecc\\_key\\_info\\_t](#) \* **pkcs11\_get\_object\_key\_type** ([ATCADevice](#) device\_ctx, [pkcs11\\_object\\_ptr](#) obj\_ptr)
- CK\_RV **pkcs11\_ta\_get\_pubkey** (CK\_VOID\_PTR pObject, [cal\\_buffer](#) \*key\_buffer, [pkcs11\\_session\\_ctx\\_ptr](#) session\_ctx)
- CK\_RV **pkcs11\_key\_write** (CK\_VOID\_PTR pSession, CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, const [pkcs11\\_ecc\\_key\\_info\\_t](#) \*ec\_key\_info)
- CK\_RV **pkcs11\_key\_generate** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount, CK\_OBJECT\_HANDLE\_PTR phKey)
- CK\_RV **pkcs11\_key\_generate\_pair** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_ATTRIBUTE\_PTR pPublicKeyTemplate, CK\_ULONG ulPublicKeyAttributeCount, CK\_ATTRIBUTE\_PTR pPrivateKeyTemplate, CK\_ULONG ulPrivateKeyAttributeCount, CK\_OBJECT\_HANDLE\_PTR phPublicKey, CK\_OBJECT\_HANDLE\_PTR phPrivateKey)
- CK\_RV **pkcs11\_key\_derive** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hBaseKey, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount, CK\_OBJECT\_HANDLE\_PTR phKey)
- CK\_RV **pkcs11\_key\_clear\_session\_cache** ([pkcs11\\_session\\_ctx\\_ptr](#) session\_ctx)
- CK\_RV **pkcs11\_key\_clear\_object\_cache** ([pkcs11\\_object\\_ptr](#) pObject)

## Variables

- CK\_BYTE [pkcs11\\_ec\\_pbkey\\_asn1\\_hdr\\_p256](#) []
- CK\_BYTE [pkcs11\\_x962\\_asn1\\_hdr\\_ec256](#) []
- CK\_BYTE **pkcs11\_key\_ec\_params\_p256** [] = { 0x06, 0x08, 0x2a, 0x86, 0x48, 0xce, 0x3d, 0x03, 0x01, 0x07 }
- CK\_BYTE [pkcs11\\_ec\\_pbkey\\_asn1\\_hdr\\_p224](#) []
- CK\_BYTE [pkcs11\\_x962\\_asn1\\_hdr\\_ec224](#) []
- CK\_BYTE **pkcs11\_key\_ec\_params\_p224** [] = { 0x06, 0x05, 0x2B, 0x81, 0x04, 0x00, 0x21 }
- CK\_BYTE [pkcs11\\_ec\\_pbkey\\_asn1\\_hdr\\_p384](#) []
- CK\_BYTE **pkcs11\_key\_ec\_params\_p384** [] = { 0x06, 0x05, 0x2B, 0x81, 0x04, 0x00, 0x22 }
- CK\_BYTE [pkcs11\\_x962\\_asn1\\_hdr\\_ec384](#) []
- CK\_BYTE [pkcs11\\_ec\\_pbkey\\_asn1\\_hdr\\_p521](#) []
- CK\_BYTE [pkcs11\\_x962\\_asn1\\_hdr\\_ec521](#) []
- CK\_BYTE **pkcs11\_key\_ec\_params\_p521** [] = { 0x06, 0x05, 0x2B, 0x81, 0x04, 0x00, 0x23 }
- const [pkcs11\\_ecc\\_key\\_info\\_t](#) [ec\\_key\\_data\\_table](#) [4]
- const [pkcs11\\_attr\\_model](#) [pkcs11\\_key\\_public\\_attributes](#) []
- const CK\_ULONG **pkcs11\_key\_public\_attributes\_count** = (CK\_ULONG)(sizeof([pkcs11\\_key\\_public\\_attributes](#)) / sizeof([pkcs11\\_key\\_public\\_attributes](#) [0]))
- const [pkcs11\\_attr\\_model](#) [pkcs11\\_key\\_private\\_attributes](#) []
- const CK\_ULONG **pkcs11\_key\_private\_attributes\_count** = (CK\_ULONG)(sizeof([pkcs11\\_key\\_private\\_attributes](#)) / sizeof([pkcs11\\_key\\_private\\_attributes](#) [0]))
- const [pkcs11\\_attr\\_model](#) [pkcs11\\_key\\_secret\\_attributes](#) []
- const CK\_ULONG **pkcs11\_key\_secret\_attributes\_count** = (CK\_ULONG)(sizeof([pkcs11\\_key\\_secret\\_attributes](#)) / sizeof([pkcs11\\_key\\_secret\\_attributes](#) [0]))

### 22.188.1 Detailed Description

PKCS11 Library Key Object Handling.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.



## 22.189 pkcs11\_key.h File Reference

PKCS11 Library Object Handling.

```
#include "pkcs11_object.h"
```

### Data Structures

- struct [pkcs11\\_ecc\\_key\\_info\\_s](#)

### Macros

- #define **PKCS11\_X962\_ASN1\_HEADER\_SZ** 3u
- #define **PKCS11\_MAX\_ECC\_ASN1\_HDR\_SIZE** ATCA\_ECCP256\_ASN1\_HDR\_SIZE
- #define **PKCS11\_MAX\_ECC\_PB\_KEY\_SIZE** TA\_ECC521\_PUB\_KEY\_SIZE

### Typedefs

- typedef struct [pkcs11\\_ecc\\_key\\_info\\_s](#) **pkcs11\_ecc\_key\_info\_t**

### Functions

- CK\_RV **pkcs11\_key\_write** (CK\_VOID\_PTR pSession, CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, const [pkcs11\\_ecc\\_key\\_info\\_t](#) \*ec\_key\_info)
- CK\_RV **pkcs11\_key\_generate** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount, CK\_OBJECT\_HANDLE\_PTR phKey)
- CK\_RV **pkcs11\_key\_generate\_pair** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_ATTRIBUTE\_PTR pPublicKeyTemplate, CK\_ULONG ulPublicKeyAttributeCount, CK\_ATTRIBUTE\_PTR pPrivateKeyTemplate, CK\_ULONG ulPrivateKeyAttributeCount, CK\_OBJECT\_HANDLE\_PTR phPublicKey, CK\_OBJECT\_HANDLE\_PTR phPrivateKey)
- CK\_RV **pkcs11\_key\_derive** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hBaseKey, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount, CK\_OBJECT\_HANDLE\_PTR phKey)
- CK\_RV **pkcs11\_key\_clear\_session\_cache** ([pkcs11\\_session\\_ctx\\_ptr](#) session\_ctx)
- CK\_RV **pkcs11\_key\_clear\_object\_cache** ([pkcs11\\_object\\_ptr](#) pObject)
- const [pkcs11\\_ecc\\_key\\_info\\_t](#) \* **pkcs11\_get\_object\_key\_type** ([ATCADevice](#) device\_ctx, [pkcs11\\_object\\_ptr](#) obj\_ptr)
- CK\_RV **pkcs11\_ta\_get\_pubkey** (CK\_VOID\_PTR pObject, [cal\\_buffer](#) \*key\_buffer, [pkcs11\\_session\\_ctx\\_ptr](#) session\_ctx)

## Variables

- const [pkcs11\\_ecc\\_key\\_info\\_t](#) **ec\_key\_data\_table** [4]
- const [pkcs11\\_attr\\_model](#) **pkcs11\_key\_public\_attributes** []
- const CK\_ULONG **pkcs11\_key\_public\_attributes\_count**
- const [pkcs11\\_attr\\_model](#) **pkcs11\_key\_private\_attributes** []
- const CK\_ULONG **pkcs11\_key\_private\_attributes\_count**
- const [pkcs11\\_attr\\_model](#) **pkcs11\_key\_secret\_attributes** []
- const CK\_ULONG **pkcs11\_key\_secret\_attributes\_count**
- CK\_BYTE [pkcs11\\_ec\\_pbkey\\_asn1\\_hdr\\_p256](#) []
- CK\_BYTE [pkcs11\\_x962\\_asn1\\_hdr\\_ec256](#) []
- CK\_BYTE **pkcs11\_key\_ec\_params\_p256** []
- CK\_BYTE [pkcs11\\_ec\\_pbkey\\_asn1\\_hdr\\_p224](#) []
- CK\_BYTE [pkcs11\\_x962\\_asn1\\_hdr\\_ec224](#) []
- CK\_BYTE **pkcs11\_key\_ec\_params\_p224** []
- CK\_BYTE [pkcs11\\_ec\\_pbkey\\_asn1\\_hdr\\_p384](#) []
- CK\_BYTE [pkcs11\\_x962\\_asn1\\_hdr\\_ec384](#) []
- CK\_BYTE **pkcs11\_key\_ec\_params\_p384** []
- CK\_BYTE [pkcs11\\_ec\\_pbkey\\_asn1\\_hdr\\_p521](#) []
- CK\_BYTE [pkcs11\\_x962\\_asn1\\_hdr\\_ec521](#) []
- CK\_BYTE **pkcs11\_key\_ec\_params\_p521** []

### 22.189.1 Detailed Description

PKCS11 Library Object Handling.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.190 pkcs11\_main.c File Reference

PKCS11 Basic library redirects based on the 2.40 specification [docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/os/pkcs11-base-v2.40-os.html](https://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/os/pkcs11-base-v2.40-os.html).

```
#include "cryptoki.h"
#include "pkcs11_config.h"
#include "pkcs11_debug.h"
#include "pkcs11_encrypt.h"
#include "pkcs11_init.h"
#include "pkcs11_info.h"
#include "pkcs11_slot.h"
#include "pkcs11_mech.h"
#include "pkcs11_session.h"
#include "pkcs11_token.h"
#include "pkcs11_find.h"
#include "pkcs11_object.h"
#include "pkcs11_signature.h"
#include "pkcs11_digest.h"
#include "pkcs11_key.h"
```

## Functions

- **CK\_RV C\_Initialize** (CK\_VOID\_PTR pInitArgs)  
*Initializes Cryptoki library NOTES: If pInitArgs is a non-NULL\_PTR is must dereference to a [CK\\_C\\_INITIALIZE\\_ARGS](#) structure.*
- **CK\_RV C\_Finalize** (CK\_VOID\_PTR pReserved)  
*Clean up miscellaneous Cryptoki-associated resources.*
- **CK\_RV C\_GetInfo** (CK\_INFO\_PTR pInfo)  
*Obtains general information about Cryptoki.*
- **CK\_RV C\_GetFunctionList** (CK\_FUNCTION\_LIST\_PTR\_PTR ppFunctionList)  
*Obtains entry points of Cryptoki library functions.*
- **CK\_RV C\_GetSlotList** (CK\_BBOOL tokenPresent, CK\_SLOT\_ID\_PTR pSlotList, CK\_ULONG\_PTR pulCount)  
*Obtains a list of slots in the system.*
- **CK\_RV C\_GetSlotInfo** (CK\_SLOT\_ID slotID, CK\_SLOT\_INFO\_PTR pInfo)  
*Obtains information about a particular slot.*
- **CK\_RV C\_GetTokenInfo** (CK\_SLOT\_ID slotID, CK\_TOKEN\_INFO\_PTR pInfo)  
*Obtains information about a particular token.*
- **CK\_RV C\_GetMechanismList** (CK\_SLOT\_ID slotID, CK\_MECHANISM\_TYPE\_PTR pMechanismList, CK\_ULONG\_PTR pulCount)  
*Obtains a list of mechanisms supported by a token (in a slot)*
- **CK\_RV C\_GetMechanismInfo** (CK\_SLOT\_ID slotID, CK\_MECHANISM\_TYPE type, CK\_MECHANISM\_INFO\_PTR pInfo)  
*Obtains information about a particular mechanism of a token (in a slot)*
- **CK\_RV C\_InitToken** (CK\_SLOT\_ID slotID, CK\_UTF8CHAR\_PTR pPin, CK\_ULONG ulPinLen, CK\_UTF8CHAR\_PTR pLabel)  
*Initializes a token (in a slot)*
- **CK\_RV C\_InitPIN** (CK\_SESSION\_HANDLE hSession, CK\_UTF8CHAR\_PTR pPin, CK\_ULONG ulPinLen)  
*Initializes the normal user's PIN.*
- **CK\_RV C\_SetPIN** (CK\_SESSION\_HANDLE hSession, CK\_UTF8CHAR\_PTR pOldPin, CK\_ULONG ulOldLen, CK\_UTF8CHAR\_PTR pNewPin, CK\_ULONG ulNewLen)  
*Modifies the PIN of the current user.*
- **CK\_RV C\_OpenSession** (CK\_SLOT\_ID slotID, CK\_FLAGS flags, CK\_VOID\_PTR pApplication, CK\_NOTIFY Notify, CK\_SESSION\_HANDLE\_PTR phSession)  
*Opens a connection between an application and a particular token or sets up an application callback for token insertion.*
- **CK\_RV C\_CloseSession** (CK\_SESSION\_HANDLE hSession)  
*Close the given session.*
- **CK\_RV C\_CloseAllSessions** (CK\_SLOT\_ID slotID)  
*Close all open sessions.*
- **CK\_RV C\_GetSessionInfo** (CK\_SESSION\_HANDLE hSession, CK\_SESSION\_INFO\_PTR pInfo)  
*Retrieve information about the specified session.*
- **CK\_RV C\_GetOperationState** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pOperationState, CK\_ULONG\_PTR pulOperationStateLen)  
*Obtains the cryptographic operations state of a session.*
- **CK\_RV C\_SetOperationState** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pOperationState, CK\_ULONG ulOperationStateLen, CK\_OBJECT\_HANDLE hEncryptionKey, CK\_OBJECT\_HANDLE hAuthenticationKey)  
*Sets the cryptographic operations state of a session.*
- **CK\_RV C\_Login** (CK\_SESSION\_HANDLE hSession, CK\_USER\_TYPE userType, CK\_UTF8CHAR\_PTR pPin, CK\_ULONG ulPinLen)  
*Login on the token in the specified session.*
- **CK\_RV C\_Logout** (CK\_SESSION\_HANDLE hSession)

*Log out of the token in the specified session.*

- CK\_RV **C\_CreateObject** (CK\_SESSION\_HANDLE hSession, CK\_ATTRIBUTE\_PTR pTemplate, CK\_↔  
ULONG ulCount, CK\_OBJECT\_HANDLE\_PTR phObject)

*Create a new object on the token in the specified session using the given attribute template.*

- CK\_RV **C\_CopyObject** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hObject, CK\_↔  
ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount, CK\_OBJECT\_HANDLE\_PTR phNewObject)

*Create a copy of the object with the specified handle.*

- CK\_RV **C\_DestroyObject** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hObject)

*Destroy the specified object.*

- CK\_RV **C\_GetObjectSize** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hObject, CK\_↔  
ULONG\_PTR pulSize)

*Obtains the size of an object in bytes.*

- CK\_RV **C\_GetAttributeValue** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hObject, CK\_↔  
ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount)

*Obtains an attribute value of an object.*

- CK\_RV **C\_SetAttributeValue** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hObject, CK\_↔  
ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount)

*Change or set the value of the specified attributes on the specified object.*

- CK\_RV **C\_FindObjectsInit** (CK\_SESSION\_HANDLE hSession, CK\_ATTRIBUTE\_PTR pTemplate, CK\_↔  
ULONG ulCount)

*Initializes an object search in the specified session using the specified attribute template as search parameters.*

- CK\_RV **C\_FindObjects** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE\_PTR phObject, CK\_↔  
\_ULONG ulMaxObjectCount, CK\_ULONG\_PTR pulObjectCount)

*Continue the search for objects in the specified session.*

- CK\_RV **C\_FindObjectsFinal** (CK\_SESSION\_HANDLE hSession)

*Finishes an object search operation (and cleans up)*

- CK\_RV **C\_EncryptInit** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_↔  
OBJECT\_HANDLE hKey)

*Initializes an encryption operation using the specified mechanism and session.*

- CK\_RV **C\_Encrypt** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen,  
CK\_BYTE\_PTR pEncryptedData, CK\_ULONG\_PTR pulEncryptedDataLen)

*Perform a single operation encryption operation in the specified session.*

- CK\_RV **C\_EncryptUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ul↔  
PartLen, CK\_BYTE\_PTR pEncryptedPart, CK\_ULONG\_PTR pulEncryptedPartLen)

*Continues a multiple-part encryption operation.*

- CK\_RV **C\_EncryptFinal** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pLastEncryptedPart, CK\_↔  
ULONG\_PTR pulLastEncryptedPartLen)

*Finishes a multiple-part encryption operation.*

- CK\_RV **C\_DecryptInit** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_↔  
OBJECT\_HANDLE hKey)

*Initialize decryption using the specified object.*

- CK\_RV **C\_Decrypt** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pEncryptedData, CK\_ULONG ul↔  
EncryptedDataLen, CK\_BYTE\_PTR pData, CK\_ULONG\_PTR pulDataLen)

*Perform a single operation decryption in the given session.*

- CK\_RV **C\_DecryptUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pEncryptedPart, CK\_↔  
ULONG ulEncryptedPartLen, CK\_BYTE\_PTR pPart, CK\_ULONG\_PTR pulPartLen)

*Continues a multiple-part decryption operation.*

- CK\_RV **C\_DecryptFinal** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pLastPart, CK\_ULONG\_PTR  
pulLastPartLen)

*Finishes a multiple-part decryption operation.*

- CK\_RV **C\_DigestInit** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism)

*Initializes a message-digesting operation using the specified mechanism in the specified session.*

- **CK\_RV C\_Digest** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pDigest, CK\_ULONG\_PTR pulDigestLen)  
*Digest the specified data in a one-pass operation and return the resulting digest.*
- **CK\_RV C\_DigestUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ulPartLen)  
*Continues a multiple-part digesting operation.*
- **CK\_RV C\_DigestKey** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hKey)  
*Update a running digest operation by digesting a secret key with the specified handle.*
- **CK\_RV C\_DigestFinal** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pDigest, CK\_ULONG\_PTR pulDigestLen)  
*Finishes a multiple-part digesting operation.*
- **CK\_RV C\_SignInit** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hKey)  
*Initialize a signing operation using the specified key and mechanism.*
- **CK\_RV C\_Sign** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pSignature, CK\_ULONG\_PTR pulSignatureLen)  
*Sign the data in a single pass operation.*
- **CK\_RV C\_SignUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ulPartLen)  
*Continues a multiple-part signature operation.*
- **CK\_RV C\_SignFinal** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pSignature, CK\_ULONG\_PTR pulSignatureLen)  
*Finishes a multiple-part signature operation.*
- **CK\_RV C\_SignRecoverInit** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hKey)  
*Initializes a signature operation, where the data can be recovered from the signature.*
- **CK\_RV C\_SignRecover** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pSignature, CK\_ULONG\_PTR pulSignatureLen)  
*Signs single-part data, where the data can be recovered from the signature.*
- **CK\_RV C\_VerifyInit** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hKey)  
*Initializes a verification operation using the specified key and mechanism.*
- **CK\_RV C\_Verify** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pSignature, CK\_ULONG\_PTR pulSignatureLen)  
*Verifies a signature on single-part data.*
- **CK\_RV C\_VerifyUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ulPartLen)  
*Continues a multiple-part verification operation.*
- **CK\_RV C\_VerifyFinal** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pSignature, CK\_ULONG\_PTR pulSignatureLen)  
*Finishes a multiple-part verification operation.*
- **CK\_RV C\_VerifyRecoverInit** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hKey)  
*Initializes a verification operation where the data is recovered from the signature.*
- **CK\_RV C\_VerifyRecover** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pSignature, CK\_ULONG\_PTR pulSignatureLen, CK\_BYTE\_PTR pData, CK\_ULONG\_PTR pulDataLen)  
*Verifies a signature on single-part data, where the data is recovered from the signature.*
- **CK\_RV C\_DigestEncryptUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG\_PTR pulPartLen, CK\_BYTE\_PTR pEncryptedPart, CK\_ULONG\_PTR pulEncryptedPartLen)  
*Continues simultaneous multiple-part digesting and encryption operations.*
- **CK\_RV C\_DecryptDigestUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pEncryptedPart, CK\_ULONG\_PTR pulEncryptedPartLen, CK\_BYTE\_PTR pPart, CK\_ULONG\_PTR pulPartLen)  
*Continues simultaneous multiple-part decryption and digesting operations.*

- CK\_RV **C\_SignEncryptUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ulPartLen, CK\_BYTE\_PTR pEncryptedPart, CK\_ULONG\_PTR pulEncryptedPartLen)  
*Continues simultaneous multiple-part signature and encryption operations.*
- CK\_RV **C\_DecryptVerifyUpdate** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pEncryptedPart, CK\_ULONG ulEncryptedPartLen, CK\_BYTE\_PTR pPart, CK\_ULONG\_PTR pulPartLen)  
*Continues simultaneous multiple-part decryption and verification operations.*
- CK\_RV **C\_GenerateKey** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_↔ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount, CK\_OBJECT\_HANDLE\_PTR phKey)  
*Generates a secret key using the specified mechanism.*
- CK\_RV **C\_GenerateKeyPair** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_ATTRIBUTE\_PTR pPublicKeyTemplate, CK\_ULONG ulPublicKeyAttributeCount, CK\_ATTRIBUTE\_PTR pPrivateKeyTemplate, CK\_ULONG ulPrivateKeyAttributeCount, CK\_OBJECT\_HANDLE\_PTR phPublicKey, CK\_OBJECT\_HANDLE\_PTR phPrivateKey)  
*Generates a public-key/private-key pair using the specified mechanism.*
- CK\_RV **C\_WrapKey** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_↔OBJECT\_HANDLE hWrappingKey, CK\_OBJECT\_HANDLE hKey, CK\_BYTE\_PTR pWrappedKey, CK\_↔ULONG\_PTR pulWrappedKeyLen)  
*Wraps (encrypts) the specified key using the specified wrapping key and mechanism.*
- CK\_RV **C\_UnwrapKey** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_↔OBJECT\_HANDLE hUnwrappingKey, CK\_BYTE\_PTR pWrappedKey, CK\_ULONG ulWrappedKeyLen, CK\_↔ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulAttributeCount, CK\_OBJECT\_HANDLE\_PTR phKey)  
*Unwraps (decrypts) the specified key using the specified unwrapping key.*
- CK\_RV **C\_DeriveKey** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_↔OBJECT\_HANDLE hBaseKey, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulAttributeCount, CK\_↔OBJECT\_HANDLE\_PTR phKey)  
*Derive a key from the specified base key.*
- CK\_RV **C\_SeedRandom** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pSeed, CK\_ULONG ul↔SeedLen)  
*Mixes in additional seed material to the random number generator.*
- CK\_RV **C\_GenerateRandom** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR RandomData, CK\_↔ULONG ulRandomLen)  
*Generate the specified amount of random data.*
- CK\_RV **C\_GetFunctionStatus** (CK\_SESSION\_HANDLE hSession)  
*Legacy function - see PKCS#11 v2.40.*
- CK\_RV **C\_CancelFunction** (CK\_SESSION\_HANDLE hSession)  
*Legacy function.*
- CK\_RV **C\_WaitForSlotEvent** (CK\_FLAGS flags, CK\_SLOT\_ID\_PTR pSlot, CK\_VOID\_PTR pRserve)  
*Wait for a slot event (token insertion, removal, etc) on the specified slot to occur.*

## 22.190.1 Detailed Description

PKCS11 Basic library redirects based on the 2.40 specification [docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/os/pkcs11-base-v2.40-os.html](https://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/os/pkcs11-base-v2.40-os.html).

### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.191 pkcs11\_mech.c File Reference

PKCS11 Library Mechanism Handling.

```
#include "pkcs11_config.h"
#include "pkcs11_debug.h"
#include "pkcs11_init.h"
#include "pkcs11_mech.h"
#include "pkcs11_slot.h"
#include "cryptoauthlib.h"
```

### Data Structures

- struct [pkcs11\\_mech\\_table\\_e](#)

### Macros

- #define **PKCS11\_MECH\_ECC508\_EC\_CAPABILITY** (CKF\_EC\_F\_P | CKF\_EC\_NAMEDCURVE | CKF\_↔  
EC\_UNCOMPRESS)
- #define **TABLE\_SIZE**(x) sizeof(x) / sizeof(x[0])

### Typedefs

- typedef struct [pkcs11\\_mech\\_table\\_e](#) **pkcs11\_mech\_table\_e**
- typedef struct [pkcs11\\_mech\\_table\\_e](#) \* **pkcs11\_mech\_table\_ptr**

### Functions

- CK\_RV **pkcs11\_mech\_get\_list** (CK\_SLOT\_ID slotID, CK\_MECHANISM\_TYPE\_PTR pMechanismList, CK\_ULONG\_PTR pulCount)
- CK\_RV **pkcs\_mech\_get\_info** (CK\_SLOT\_ID slotID, CK\_MECHANISM\_TYPE type, CK\_MECHANISM\_↔  
INFO\_PTR pInfo)

#### 22.191.1 Detailed Description

PKCS11 Library Mechanism Handling.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.192 pkcs11\_mech.h File Reference

PKCS11 Library Mechanism Handling.

```
#include "cryptoki.h"
```

### Functions

- CK\_RV **pkcs11\_mech\_get\_list** (CK\_SLOT\_ID slotID, CK\_MECHANISM\_TYPE\_PTR pMechanismList, CK\_ULONG\_PTR pulCount)
- CK\_RV **pkcs\_mech\_get\_info** (CK\_SLOT\_ID slotID, CK\_MECHANISM\_TYPE type, CK\_MECHANISM\_↵INFO\_PTR pInfo)

### 22.192.1 Detailed Description

PKCS11 Library Mechanism Handling.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.193 pkcs11\_object.c File Reference

PKCS11 Library Object Handling Base.

```
#include "cryptoauthlib.h"
#include "atcacert/atcacert_def.h"
#include "cryptoki.h"
#include "pkcs11_config.h"
#include "pkcs11_debug.h"
#include "pkcs11_init.h"
#include "pkcs11_slot.h"
#include "pkcs11_session.h"
#include "pkcs11_util.h"
#include "pkcs11_object.h"
#include "pkcs11_os.h"
#include "pkcs11_find.h"
#include "pkcs11_key.h"
#include "pkcs11_cert.h"
```

### Functions

- CK\_RV **pkcs11\_object\_alloc** (CK\_SLOT\_ID slotId, pkcs11\_object\_ptr \*ppObject)
- CK\_RV **pkcs11\_object\_free** (pkcs11\_object\_ptr pObject)
- CK\_RV **pkcs11\_object\_check** (pkcs11\_object\_ptr \*ppObject, CK\_OBJECT\_HANDLE hObject)
- CK\_RV **pkcs11\_object\_get\_handle** (pkcs11\_object\_ptr pObject, CK\_OBJECT\_HANDLE\_PTR phObject)
- CK\_RV **pkcs11\_object\_get\_owner** (pkcs11\_object\_ptr pObject, CK\_SLOT\_ID\_PTR pSlotId)
- CK\_RV **pkcs11\_object\_get\_name** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV **pkcs11\_object\_get\_class** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV **pkcs11\_object\_get\_type** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV **pkcs11\_object\_get\_destroyable** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV **pkcs11\_object\_get\_size** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hObject, CK\_ULONG\_PTR pulSize)



- CK\_RV **pkcs11\_object\_find** (CK\_SLOT\_ID slotId, pkcs11\_object\_ptr \*ppObject, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount)
- CK\_RV **pkcs11\_object\_create** (CK\_SESSION\_HANDLE hSession, CK\_ATTRIBUTE\_PTR pTemplate, CK\_ULONG ulCount, CK\_OBJECT\_HANDLE\_PTR phObject)  
*Create a new object on the token in the specified session using the given attribute template.*
- CK\_RV **pkcs11\_object\_destroy** (CK\_SESSION\_HANDLE hSession, CK\_OBJECT\_HANDLE hObject)  
*Destroy the specified object.*
- CK\_RV **pkcs11\_object\_deinit** (pkcs11\_lib\_ctx\_ptr pContext)
- ATCA\_STATUS **pkcs11\_object\_load\_handle\_info** (ATCADevice device, pkcs11\_lib\_ctx\_ptr pContext)
- CK\_RV **pkcs11\_object\_is\_private** (pkcs11\_object\_ptr pObject, CK\_BBOOL \*is\_private, pkcs11\_session\_ctx\_ptr pSession)  
*Checks the attributes of the underlying cryptographic asset to determine if it is a private key - this changes the way the associated public key is referenced.*

## Variables

- [pkcs11\\_object\\_cache\\_t](#) **pkcs11\_object\_cache** [PKCS11\_MAX\_OBJECTS\_ALLOWED]
- const [pkcs11\\_attrib\\_model](#) **pkcs11\_object\_monotonic\_attributes** []
- const CK\_ULONG **pkcs11\_object\_monotonic\_attributes\_count** = (CK\_ULONG)(sizeof([pkcs11\\_object\\_monotonic\\_attributes](#)) / sizeof([pkcs11\\_object\\_monotonic\\_attributes](#) [0]))

### 22.193.1 Detailed Description

PKCS11 Library Object Handling Base.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.194 pkcs11\_object.h File Reference

PKCS11 Library Object Handling.

```
#include "cryptoauthlib.h"
#include "cryptoki.h"
#include "pkcs11_config.h"
#include "pkcs11_attr.h"
```

## Data Structures

- struct [pkcs11\\_object\\_s](#)
- struct [pkcs11\\_object\\_cache\\_s](#)

## Macros

- `#define PKCS11_OBJECT_FLAG_DESTROYABLE (0x01U)`
- `#define PKCS11_OBJECT_FLAG_MODIFIABLE (0x02U)`
- `#define PKCS11_OBJECT_FLAG_DYNAMIC (0x04U)`
- `#define PKCS11_OBJECT_FLAG_SENSITIVE (0x08U)`
- `#define PKCS11_OBJECT_FLAG_TA_TYPE (0x10U)`
- `#define PKCS11_OBJECT_FLAG_TRUST_TYPE (0x20U)`
- `#define PKCS11_OBJECT_FLAG_CERT_CACHE (0x40U)`
- `#define PKCS11_OBJECT_FLAG_KEY_CACHE (0x80U)`
- `#define PKCS11_OBJECT_FLAG_KEY_CACHE_COMPLEMENT ~(PKCS11_OBJECT_FLAG_KEY_CACHE & 0xffu)`
- `#define PKCS11_OBJECT_FLAG_CERT_CACHE_COMPLEMENT ~(PKCS11_OBJECT_FLAG_CERT_CACHE & 0xffu)`

## Typedefs

- `typedef struct pkcs11\_object\_s pkcs11_object`
- `typedef struct pkcs11\_object\_cache\_s pkcs11_object_cache_t`

## Functions

- `CK_RV pkcs11_object_alloc (CK_SLOT_ID slotId, pkcs11\_object\_ptr *ppObject)`
- `CK_RV pkcs11_object_free (pkcs11\_object\_ptr pObject)`
- `CK_RV pkcs11_object_check (pkcs11\_object\_ptr *ppObject, CK_OBJECT_HANDLE hObject)`
- `CK_RV pkcs11_object_find (CK_SLOT_ID slotId, pkcs11\_object\_ptr *ppObject, CK_ATTRIBUTE_PTR pTemplate, CK_ULONG ulCount)`
- `CK_RV pkcs11_object_is_private (pkcs11\_object\_ptr pObject, CK_BBOOL *is_private, pkcs11\_session\_ctx\_ptr pSession)`

*Checks the attributes of the underlying cryptographic asset to determine if it is a private key - this changes the way the associated public key is referenced.*
- `CK_RV pkcs11_object_deinit (pkcs11\_lib\_ctx\_ptr pContext)`
- `CK_RV pkcs11_object_get_owner (pkcs11\_object\_ptr pObject, CK_SLOT_ID_PTR pSlotId)`
- `ATCA_STATUS pkcs11_object_load_handle_info (ATCADevice device, pkcs11\_lib\_ctx\_ptr pContext)`
- `CK_RV pkcs11_object_get_class (CK_VOID_PTR pObject, CK_ATTRIBUTE_PTR pAttribute, pkcs11\_session\_ctx\_ptr pSession)`
- `CK_RV pkcs11_object_get_name (CK_VOID_PTR pObject, CK_ATTRIBUTE_PTR pAttribute, pkcs11\_session\_ctx\_ptr pSession)`
- `CK_RV pkcs11_object_get_type (CK_VOID_PTR pObject, CK_ATTRIBUTE_PTR pAttribute, pkcs11\_session\_ctx\_ptr pSession)`
- `CK_RV pkcs11_object_get_destroyable (CK_VOID_PTR pObject, CK_ATTRIBUTE_PTR pAttribute, pkcs11\_session\_ctx\_ptr pSession)`
- `CK_RV pkcs11_object_get_size (CK_SESSION_HANDLE hSession, CK_OBJECT_HANDLE hObject, CK_ULONG_PTR pulSize)`
- `CK_RV pkcs11_object_get_handle (pkcs11\_object\_ptr pObject, CK_OBJECT_HANDLE_PTR phObject)`
- `CK_RV pkcs11_object_create (CK_SESSION_HANDLE hSession, CK_ATTRIBUTE_PTR pTemplate, CK_ULONG ulCount, CK_OBJECT_HANDLE_PTR phObject)`

*Create a new object on the token in the specified session using the given attribute template.*
- `CK_RV pkcs11_object_destroy (CK_SESSION_HANDLE hSession, CK_OBJECT_HANDLE hObject)`

*Destroy the specified object.*

## Variables

- `pkcs11_object_cache_t pkcs11_object_cache []`
- `const pkcs11_attr_model pkcs11_object_monotonic_attributes []`
- `const CK_ULONG pkcs11_object_monotonic_attributes_count`

### 22.194.1 Detailed Description

PKCS11 Library Object Handling.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.195 pkcs11\_os.c File Reference

PKCS11 Library Operating System Abstraction Functions.

```
#include "pkcs11_os.h"
#include "pkcs11_util.h"
#include "pkcs11_init.h"
```

## Functions

- `CK_RV pkcs11_os_create_mutex (CK_VOID_PTR_PTR ppMutex)`  
*Application callback for creating a mutex object.*
- `CK_RV pkcs11_os_destroy_mutex (CK_VOID_PTR pMutex)`
- `CK_RV pkcs11_os_lock_mutex (CK_VOID_PTR pMutex)`
- `CK_RV pkcs11_os_unlock_mutex (CK_VOID_PTR pMutex)`
- `CK_RV pkcs11_os_alloc_shared_ctx (void **ppShared, size_t size)`
- `CK_RV pkcs11_os_free_shared_ctx (void *pShared, size_t size)`

### 22.195.1 Detailed Description

PKCS11 Library Operating System Abstraction Functions.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.196 pkcs11\_os.h File Reference

PKCS11 Library Operating System Abstraction.

```
#include "cryptoki.h"
#include "cryptoauthlib.h"
```

### Macros

- `#define pkcs11_os_malloc` `hal_malloc`
- `#define pkcs11_os_free` `hal_free`

### Functions

- CK\_RV `pkcs11_os_create_mutex` (CK\_VOID\_PTR\_PTR ppMutex)  
*Application callback for creating a mutex object.*
- CK\_RV `pkcs11_os_destroy_mutex` (CK\_VOID\_PTR pMutex)
- CK\_RV `pkcs11_os_lock_mutex` (CK\_VOID\_PTR pMutex)
- CK\_RV `pkcs11_os_unlock_mutex` (CK\_VOID\_PTR pMutex)
- CK\_RV `pkcs11_os_alloc_shared_ctx` (void \*\*ppShared, size\_t size)
- CK\_RV `pkcs11_os_free_shared_ctx` (void \*pShared, size\_t size)

### 22.196.1 Detailed Description

PKCS11 Library Operating System Abstraction.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.197 pkcs11\_session.c File Reference

PKCS11 Library Session Handling.

```
#include "cryptoauthlib.h"
#include "host/atca_host.h"
#include "pkcs11_config.h"
#include "pkcs11_debug.h"
#include "pkcs11_session.h"
#include "pkcs11_token.h"
#include "pkcs11_init.h"
#include "pkcs11_slot.h"
#include "pkcs11_object.h"
#include "pkcs11_os.h"
#include "pkcs11_util.h"
#include "pkcs11_key.h"
#include "pkcs11_cert.h"
```

## Functions

- [pkcs11\\_session\\_ctx\\_ptr](#) **pkcs11\_get\_session\_context** (CK\_SESSION\_HANDLE hSession)
- CK\_RV **pkcs11\_session\_check** ([pkcs11\\_session\\_ctx\\_ptr](#) \*pSession, CK\_SESSION\_HANDLE hSession)  
*Check if the session is initialized properly.*
- CK\_RV **pkcs11\_reserve\_resource** (pkcs11\_lib\_ctx\_ptr pContext, [pkcs11\\_session\\_ctx\\_ptr](#) pSession, uint8\_t resource)
- CK\_RV **pkcs11\_release\_resource** (pkcs11\_lib\_ctx\_ptr pContext, [pkcs11\\_session\\_ctx\\_ptr](#) pSession, uint8\_t resource)
- CK\_RV **pkcs11\_session\_open** (CK\_SLOT\_ID slotID, CK\_FLAGS flags, CK\_VOID\_PTR pApplication, CK\_NOTIFY notify, CK\_SESSION\_HANDLE\_PTR phSession)
- CK\_RV **pkcs11\_session\_close** (CK\_SESSION\_HANDLE hSession)
- CK\_RV **pkcs11\_session\_closeall** (CK\_SLOT\_ID slotID)  
*Close all sessions for a given slot - not actually all open sessions.*
- CK\_RV **pkcs11\_session\_get\_info** (CK\_SESSION\_HANDLE hSession, CK\_SESSION\_INFO\_PTR pInfo)  
*Obtains information about a particular session.*
- CK\_RV **pkcs11\_session\_login** (CK\_SESSION\_HANDLE hSession, CK\_USER\_TYPE userType, CK\_UTF8CHAR\_PTR pPin, CK\_ULONG ulPinLen)
- CK\_RV **pkcs11\_session\_logout** (CK\_SESSION\_HANDLE hSession)

### 22.197.1 Detailed Description

PKCS11 Library Session Handling.

Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.198 pkcs11\_session.h File Reference

PKCS11 Library Session Management & Context.

```
#include "cryptoki.h"
#include "pkcs11_config.h"
#include "cal_internal.h"
```

## Data Structures

- struct [pkcs11\\_session\\_mech\\_ctx\\_s](#)
- struct [pkcs11\\_session\\_ctx\\_s](#)

## Typedefs

- typedef struct [pkcs11\\_session\\_mech\\_ctx\\_s](#) **pkcs11\_session\_mech\_ctx**
- typedef struct [pkcs11\\_session\\_mech\\_ctx\\_s](#) \* **pkcs11\_session\_mech\_ctx\_ptr**
- typedef struct [pkcs11\\_session\\_ctx\\_s](#) **pkcs11\_session\_ctx**
- typedef struct [pkcs11\\_session\\_ctx\\_s](#) \* **pkcs11\_session\_ctx\_ptr**

## Functions

- [pkcs11\\_session\\_ctx\\_ptr](#) **pkcs11\_get\_session\_context** (CK\_SESSION\_HANDLE hSession)
- CK\_RV **pkcs11\_session\_check** ([pkcs11\\_session\\_ctx\\_ptr](#) \*pSession, CK\_SESSION\_HANDLE hSession)  
*Check if the session is initialized properly.*
- CK\_RV **pkcs11\_session\_get\_info** (CK\_SESSION\_HANDLE hSession, CK\_SESSION\_INFO\_PTR pInfo)  
*Obtains information about a particular session.*
- CK\_RV **pkcs11\_session\_open** (CK\_SLOT\_ID slotID, CK\_FLAGS flags, CK\_VOID\_PTR pApplication, CK\_NOTIFY notify, CK\_SESSION\_HANDLE\_PTR phSession)
- CK\_RV **pkcs11\_session\_close** (CK\_SESSION\_HANDLE hSession)
- CK\_RV [pkcs11\\_session\\_closeall](#) (CK\_SLOT\_ID slotID)  
*Close all sessions for a given slot - not actually all open sessions.*
- CK\_RV [pkcs11\\_session\\_login](#) (CK\_SESSION\_HANDLE hSession, CK\_USER\_TYPE userType, CK\_UTF8CHAR\_PTR pPin, CK\_ULONG ulPinLen)
- CK\_RV **pkcs11\_session\_logout** (CK\_SESSION\_HANDLE hSession)
- CK\_RV **pkcs11\_reserve\_resource** ([pkcs11\\_lib\\_ctx\\_ptr](#) pContext, [pkcs11\\_session\\_ctx\\_ptr](#) pSession, uint8\_t resource)
- CK\_RV **pkcs11\_release\_resource** ([pkcs11\\_lib\\_ctx\\_ptr](#) pContext, [pkcs11\\_session\\_ctx\\_ptr](#) pSession, uint8\_t resource)

### 22.198.1 Detailed Description

PKCS11 Library Session Management & Context.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.198.2 Typedef Documentation

#### 22.198.2.1 [pkcs11\\_session\\_ctx](#)

```
typedef struct pkcs11\_session\_ctx\_s pkcs11\_session\_ctx
```

Session Context

## 22.199 pkcs11\_signature.c File Reference

PKCS11 Library Sign/Verify Handling.

```
#include "pkcs11_config.h"
#include "pkcs11_debug.h"
#include "pkcs11_init.h"
#include "pkcs11_signature.h"
#include "pkcs11_object.h"
#include "pkcs11_session.h"
#include "pkcs11_util.h"
#include "cryptoauthlib.h"
#include "pkcs11_slot.h"
#include "pkcs11_key.h"
#include "atcacert/atcacert_der.h"
```

## Functions

- CK\_RV **pkcs11\_signature\_sign\_init** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hKey)  
*Initialize a signing operation using the specified key and mechanism.*
- CK\_RV **pkcs11\_signature\_sign** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pSignature, CK\_ULONG\_PTR pulSignatureLen)  
*Sign the data in a single pass operation.*
- CK\_RV **pkcs11\_signature\_sign\_continue** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ulPartLen)  
*Continues a multiple-part signature operation.*
- CK\_RV **pkcs11\_signature\_sign\_finish** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pSignature, CK\_ULONG\_PTR pulSignatureLen)  
*Finishes a multiple-part signature operation.*
- CK\_RV **pkcs11\_signature\_verify\_init** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hKey)  
*Initializes a verification operation using the specified key and mechanism.*
- CK\_RV **pkcs11\_signature\_verify** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pSignature, CK\_ULONG ulSignatureLen)  
*Verifies a signature on single-part data.*
- CK\_RV **pkcs11\_signature\_verify\_continue** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ulPartLen)  
*Continues a multiple-part verification operation.*
- CK\_RV **pkcs11\_signature\_verify\_finish** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pSignature, CK\_ULONG ulSignatureLen)  
*Finishes a multiple-part verification operation.*

### 22.199.1 Detailed Description

PKCS11 Library Sign/Verify Handling.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.200 pkcs11\_signature.h File Reference

PKCS11 Library Sign/Verify Handling.

```
#include "cryptoki.h"
```

## Functions

- CK\_RV **pkcs11\_signature\_sign\_init** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hKey)  
*Initialize a signing operation using the specified key and mechanism.*
- CK\_RV **pkcs11\_signature\_sign** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pSignature, CK\_ULONG\_PTR pulSignatureLen)  
*Sign the data in a single pass operation.*
- CK\_RV **pkcs11\_signature\_sign\_continue** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ulPartLen)  
*Continues a multiple-part signature operation.*
- CK\_RV **pkcs11\_signature\_sign\_finish** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pSignature, CK\_ULONG\_PTR pulSignatureLen)  
*Finishes a multiple-part signature operation.*
- CK\_RV **pkcs11\_signature\_verify\_init** (CK\_SESSION\_HANDLE hSession, CK\_MECHANISM\_PTR pMechanism, CK\_OBJECT\_HANDLE hKey)  
*Initializes a verification operation using the specified key and mechanism.*
- CK\_RV **pkcs11\_signature\_verify** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pData, CK\_ULONG ulDataLen, CK\_BYTE\_PTR pSignature, CK\_ULONG ulSignatureLen)  
*Verifies a signature on single-part data.*
- CK\_RV **pkcs11\_signature\_verify\_continue** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pPart, CK\_ULONG ulPartLen)  
*Continues a multiple-part verification operation.*
- CK\_RV **pkcs11\_signature\_verify\_finish** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pSignature, CK\_ULONG ulSignatureLen)  
*Finishes a multiple-part verification operation.*

### 22.200.1 Detailed Description

PKCS11 Library Sign/Verify Handling.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.201 pkcs11\_slot.c File Reference

PKCS11 Library Slot Handling.

```
#include "cryptoauthlib.h"
#include "pkcs11_config.h"
#include "pkcs11_debug.h"
#include "pkcs11_init.h"
#include "pkcs11_slot.h"
#include "pkcs11_info.h"
#include "pkcs11_util.h"
#include "pkcs11_object.h"
#include "pkcs11_os.h"
#include <stdio.h>
```



## Functions

- pkcs11\_slot\_ctx\_ptr **pkcs11\_slot\_get\_context** (pkcs11\_lib\_ctx\_ptr lib\_ctx, CK\_SLOT\_ID slotID)  
*Retrieve the current slot context.*
- pkcs11\_slot\_ctx\_ptr **pkcs11\_slot\_get\_new\_context** (pkcs11\_lib\_ctx\_ptr lib\_ctx)
- CK\_VOID\_PTR **pkcs11\_slot\_initslots** (CK\_ULONG pulCount)
- CK\_RV **pkcs11\_slot\_deinitslots** (pkcs11\_lib\_ctx\_ptr lib\_ctx)
- CK\_RV **pkcs11\_slot\_config** (CK\_SLOT\_ID slotID)
- CK\_RV **pkcs11\_slot\_init** (CK\_SLOT\_ID slotID)  
*This is an internal function that initializes a pkcs11 slot - it must already have the locks in place before being called.*
- CK\_RV **pkcs11\_slot\_get\_list** (CK\_BBOOL tokenPresent, CK\_SLOT\_ID\_PTR pSlotList, CK\_ULONG\_PTR pulCount)
- CK\_RV **pkcs11\_slot\_get\_info** (CK\_SLOT\_ID slotID, CK\_SLOT\_INFO\_PTR pInfo)  
*Obtains information about a particular slot.*

### 22.201.1 Detailed Description

PKCS11 Library Slot Handling.

The nomenclature here can lead to some confusion - the pkcs11 slot is not the same as a device slot. So for example each slot defined here is a specific device (most systems would have only one). The "slots" as defined by the device specification would be enumerated separately as related to specific supported mechanisms as cryptographic "objects".

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.202 pkcs11\_slot.h File Reference

PKCS11 Library Slot Handling & Context.

```
#include "pkcs11_init.h"
#include "cryptoauthlib.h"
```

## Data Structures

- struct [pkcs11\\_slot\\_ctx\\_s](#)

## Macros

- #define **SLOT\_STATE\_UNINITIALIZED** (0U)
- #define **SLOT\_STATE\_CONFIGURED** (1U)
- #define **SLOT\_STATE\_READY** (2U)

## Typedefs

- typedef struct [pkcs11\\_slot\\_ctx\\_s](#) [pkcs11\\_slot\\_ctx](#)

## Functions

- CK\_RV **pkcs11\_slot\_init** (CK\_SLOT\_ID slotID)  
*This is an internal function that initializes a pkcs11 slot - it must already have the locks in place before being called.*
- CK\_RV **pkcs11\_slot\_config** (CK\_SLOT\_ID slotID)
- CK\_VOID\_PTR **pkcs11\_slot\_initslots** (CK\_ULONG pulCount)
- CK\_RV **pkcs11\_slot\_deinitslots** (pkcs11\_lib\_ctx\_ptr lib\_ctx)
- pkcs11\_slot\_ctx\_ptr **pkcs11\_slot\_get\_context** (pkcs11\_lib\_ctx\_ptr lib\_ctx, CK\_SLOT\_ID slotID)  
*Retrieve the current slot context.*
- pkcs11\_slot\_ctx\_ptr **pkcs11\_slot\_get\_new\_context** (pkcs11\_lib\_ctx\_ptr lib\_ctx)
- CK\_RV **pkcs11\_slot\_get\_list** (CK\_BBOOL tokenPresent, CK\_SLOT\_ID\_PTR pSlotList, CK\_ULONG\_PTR pulCount)
- CK\_RV **pkcs11\_slot\_get\_info** (CK\_SLOT\_ID slotID, CK\_SLOT\_INFO\_PTR pInfo)  
*Obtains information about a particular slot.*

### 22.202.1 Detailed Description

PKCS11 Library Slot Handling & Context.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

### 22.202.2 Typedef Documentation

#### 22.202.2.1 pkcs11\_slot\_ctx

```
typedef struct pkcs11_slot_ctx_s pkcs11_slot_ctx
```

Slot Context

## 22.203 pkcs11\_token.c File Reference

PKCS11 Library Token Handling.

```
#include "cryptoauthlib.h"  
#include "pkcs11_config.h"  
#include "pkcs11_debug.h"  
#include "pkcs11_token.h"  
#include "pkcs11_slot.h"  
#include "pkcs11_info.h"  
#include "pkcs11_util.h"  
#include "pkcs11_object.h"  
#include "pkcs11_key.h"  
#include "pkcs11_cert.h"  
#include "pkcs11_session.h"
```

## Functions

- CK\_RV **pkcs11\_token\_init** (CK\_SLOT\_ID slotID, CK\_UTF8CHAR\_PTR pPin, CK\_ULONG ulPinLen, CK\_UTF8CHAR\_PTR pLabel)
- CK\_RV **pkcs11\_token\_get\_access\_type** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV **pkcs11\_token\_get\_writable** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV **pkcs11\_token\_get\_storage** (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV **pkcs11\_token\_get\_info** (CK\_SLOT\_ID slotID, CK\_TOKEN\_INFO\_PTR pInfo)  
*Obtains information about a particular token.*
- CK\_RV **pkcs11\_token\_random** (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pRandomData, CK\_ULONG ulRandomLen)  
*Generate the specified amount of random data.*
- CK\_RV **pkcs11\_token\_convert\_pin\_to\_key** (const CK\_UTF8CHAR\_PTR pPin, const CK\_ULONG ulPinLen, const CK\_UTF8CHAR\_PTR pSalt, const CK\_ULONG ulSaltLen, CK\_BYTE\_PTR pKey, CK\_ULONG ulKeyLen, [pkcs11\\_slot\\_ctx\\_ptr](#) slot\_ctx)
- CK\_RV **pkcs11\_token\_set\_pin** (CK\_SESSION\_HANDLE hSession, CK\_UTF8CHAR\_PTR pOldPin, CK\_ULONG ulOldLen, CK\_UTF8CHAR\_PTR pNewPin, CK\_ULONG ulNewLen)

### 22.203.1 Detailed Description

PKCS11 Library Token Handling.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.204 pkcs11\_token.h File Reference

PKCS11 Library Token Management & Context.

```
#include "pkcs11_init.h"
#include "pkcs11_session.h"
```

## Macros

- **#define ATCA\_SERIAL\_NUM\_SIZE** (9)

## Functions

- CK\_RV [pkcs11\\_token\\_init](#) (CK\_SLOT\_ID slotID, CK\_UTF8CHAR\_PTR pPin, CK\_ULONG ulPinLen, CK\_UTF8CHAR\_PTR pLabel)
- CK\_RV [pkcs11\\_token\\_get\\_access\\_type](#) (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV [pkcs11\\_token\\_get\\_writable](#) (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV [pkcs11\\_token\\_get\\_storage](#) (CK\_VOID\_PTR pObject, CK\_ATTRIBUTE\_PTR pAttribute, [pkcs11\\_session\\_ctx\\_ptr](#) pSession)
- CK\_RV [pkcs11\\_token\\_get\\_info](#) (CK\_SLOT\_ID slotID, CK\_TOKEN\_INFO\_PTR pInfo)  
*Obtains information about a particular token.*
- CK\_RV [pkcs11\\_token\\_convert\\_pin\\_to\\_key](#) (const CK\_UTF8CHAR\_PTR pPin, const CK\_ULONG ulPinLen, const CK\_UTF8CHAR\_PTR pSalt, const CK\_ULONG ulSaltLen, CK\_BYTE\_PTR pKey, CK\_ULONG ulKeyLen, [pkcs11\\_slot\\_ctx\\_ptr](#) slot\_ctx)
- CK\_RV [pkcs11\\_token\\_random](#) (CK\_SESSION\_HANDLE hSession, CK\_BYTE\_PTR pRandomData, CK\_ULONG ulRandomLen)  
*Generate the specified amount of random data.*
- CK\_RV [pkcs11\\_token\\_set\\_pin](#) (CK\_SESSION\_HANDLE hSession, CK\_UTF8CHAR\_PTR pOldPin, CK\_ULONG ulOldLen, CK\_UTF8CHAR\_PTR pNewPin, CK\_ULONG ulNewLen)

### 22.204.1 Detailed Description

PKCS11 Library Token Management & Context.

Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.205 pkcs11\_util.c File Reference

PKCS11 Library Utility Functions.

```
#include "pkcs11_util.h"
```

## Functions

- void [pkcs11\\_util\\_escape\\_string](#) (CK\_UTF8CHAR\_PTR buf, CK\_ULONG buf\_len)
- CK\_RV [pkcs11\\_util\\_convert\\_rv](#) (ATCA\_STATUS status)
- int [pkcs11\\_util\\_memset](#) (void \*dest, size\_t destsz, int ch, size\_t count)

### 22.205.1 Detailed Description

PKCS11 Library Utility Functions.

Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.206 pkcs11\_util.h File Reference

PKCS11 Library Utilities.

```
#include "pkcs11_config.h"
#include "cryptoki.h"
#include "cryptoauthlib.h"
```

### Macros

- `#define PKCS11_UTIL_ARRAY_SIZE(x) sizeof(x) / sizeof(x[0])`

### Functions

- void **pkcs11\_util\_escape\_string** (CK\_UTF8CHAR\_PTR buf, CK\_ULONG buf\_len)
- CK\_RV **pkcs11\_util\_convert\_rv** (ATCA\_STATUS status)
- int **pkcs11\_util\_memset** (void \*dest, size\_t destsz, int ch, size\_t count)

### 22.206.1 Detailed Description

PKCS11 Library Utilities.

Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.207 atca\_wolfssl\_interface.c File Reference

Crypto abstraction functions for external host side cryptography.

```
#include "cryptoauthlib.h"
```

### 22.207.1 Detailed Description

Crypto abstraction functions for external host side cryptography.

Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.208 atca\_wolfssl\_interface.h File Reference

Configuration Check for WolfSSL Integration Support.

```
#include "atca_config_check.h"
```

### 22.208.1 Detailed Description

Configuration Check for WolfSSL Integration Support.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.

## 22.209 atca\_wolfssl\_internal.h File Reference

WolfSSL Integration Support.

### 22.209.1 Detailed Description

WolfSSL Integration Support.

#### Copyright

(c) 2015-2020 Microchip Technology Inc. and its subsidiaries.



# Index

- `_array_to_code`
    - `cryptoauthlib.library`, 338
  - `_ascii_kit_host_context`, 357
  - `_atcacert_convert_bytes`
    - `cryptoauthlib.atcacert`, 328
  - `_atcacert_convert_enum`
    - `cryptoauthlib.atcacert`, 328
  - `_check_type_rationality`
    - `cryptoauthlib.library`, 338
  - `_convert_pointer_to_list`
    - `cryptoauthlib.library`, 338
  - `_ctype_from_definition`
    - `cryptoauthlib.library`, 338
  - `_def_`
    - `cryptoauthlib.atcacert.atcacert_cert_element_t`, 399
    - `cryptoauthlib.atcacert.atcacert_device_loc_t`, 406
    - `cryptoauthlib.iface._ATCAHID`, 359
    - `cryptoauthlib.iface._ATCAKIT`, 362
    - `cryptoauthlib.iface._ATCAUART`, 365
    - `cryptoauthlib.iface.ATCAIfaceCfg`, 415
  - `_def_to_field`
    - `cryptoauthlib.library`, 339
  - `_fields_`
    - `cryptoauthlib.atcab.atca_aes_cbc_ctx`, 369
    - `cryptoauthlib.atcab.atca_aes_cbcmac_ctx`, 370
    - `cryptoauthlib.atcab.atca_aes_ccm_ctx`, 370
    - `cryptoauthlib.atcab.atca_aes_cmac_ctx`, 371
    - `cryptoauthlib.atcab.atca_aes_ctr_ctx`, 372
    - `cryptoauthlib.atcab.atca_aes_gcm_ctx`, 373
    - `cryptoauthlib.atcab.atca_sha256_ctx`, 388
    - `cryptoauthlib.atcacert.atcacert_comp_data_t`, 403
    - `cryptoauthlib.atcacert.atcacert_tm_utc_t`, 409
    - `cryptoauthlib.device.AesEnable`, 368
    - `cryptoauthlib.device.Atecc508aConfig`, 422
    - `cryptoauthlib.device.Atecc608Config`, 424
    - `cryptoauthlib.device.Atsha204aConfig`, 426
    - `cryptoauthlib.device.ChipMode508`, 430
    - `cryptoauthlib.device.ChipMode608`, 431
    - `cryptoauthlib.device.ChipOptions`, 432
    - `cryptoauthlib.device.Counter204`, 448
    - `cryptoauthlib.device.CountMatch`, 448
    - `cryptoauthlib.device.I2cEnable`, 456
    - `cryptoauthlib.device.KeyConfig`, 457
    - `cryptoauthlib.device.SecureBoot`, 470
    - `cryptoauthlib.device.SlotConfig`, 471
    - `cryptoauthlib.device.UseLock`, 476
    - `cryptoauthlib.device.VolatileKeyPermission`, 476
    - `cryptoauthlib.device.X509Format`, 477
    - `cryptoauthlib.iface._ATCACUSTOM`, 358
    - `cryptoauthlib.iface._ATCAI2C`, 360
    - `cryptoauthlib.iface._ATCAIfaceParams`, 361
    - `cryptoauthlib.iface._ATCASPI`, 363
    - `cryptoauthlib.iface._ATCASWI`, 364
    - `cryptoauthlib.iface._U_Address`, 367
  - `_force_local_library`
    - `cryptoauthlib.library`, 339
  - `_get_attribute_from_ctypes`
    - `cryptoauthlib.library`, 339
  - `_get_field_definition`
    - `cryptoauthlib.library`, 339
  - `_iface_load_default_config`
    - `cryptoauthlib.iface`, 335
  - `_is_pointer`
    - `cryptoauthlib.library`, 340
  - `_kit_host_map_entry`, 366
  - `_map_`
    - `cryptoauthlib.iface._ATCAI2C`, 360
    - `cryptoauthlib.iface.ATCAIfaceCfg`, 415
  - `_obj_to_code`
    - `cryptoauthlib.library`, 340
  - `_object_definition_code`
    - `cryptoauthlib.library`, 340
  - `_pointer_to_code`
    - `cryptoauthlib.library`, 340
  - `_structure_to_code`
    - `cryptoauthlib.library`, 341
  - `_structure_to_string`
    - `cryptoauthlib.library`, 341
  - `_to_code`
    - `cryptoauthlib.library`, 341
- `address`
  - `atca_iface.h`, 559
  - `ATCAIfaceCfg`, 414
- `api_206a.c`, 479
  - `sha206a_authenticate`, 480
  - `sha206a_check_dk_useflag_validity`, 480
  - `sha206a_check_pk_useflag_validity`, 481
  - `sha206a_diversify_parent_key`, 481
  - `sha206a_generate_challenge_response_pair`, 481
  - `sha206a_generate_derive_key`, 482
  - `sha206a_get_data_store_lock_status`, 482
  - `sha206a_get_dk_update_count`, 483
  - `sha206a_get_dk_useflag_count`, 483
  - `sha206a_get_pk_useflag_count`, 483
  - `sha206a_read_data_store`, 484
  - `sha206a_verify_device_consumption`, 484
  - `sha206a_write_data_store`, 485



api\_206a.h, 485  
     sha206a\_authenticate, 486  
     sha206a\_check\_dk\_useflag\_validity, 487  
     sha206a\_check\_pk\_useflag\_validity, 487  
     sha206a\_diversify\_parent\_key, 487  
     sha206a\_generate\_challenge\_response\_pair, 488  
     sha206a\_generate\_derive\_key, 488  
     sha206a\_get\_data\_store\_lock\_status, 489  
     sha206a\_get\_dk\_update\_count, 489  
     sha206a\_get\_dk\_useflag\_count, 489  
     sha206a\_get\_pk\_useflag\_count, 490  
     sha206a\_read\_data\_store, 490  
     sha206a\_verify\_device\_consumption, 491  
     sha206a\_write\_data\_store, 491  
 ascii\_kit\_host.c, 494  
     kit\_host\_init, 494  
     kit\_host\_init\_phy, 495  
 ascii\_kit\_host.h, 495  
     kit\_host\_init, 497  
     kit\_host\_init\_phy, 498  
     kit\_host\_map\_entry\_t, 497  
     KIT\_MESSAGE\_SIZE\_MAX, 496  
 ATCA\_ALLOC\_FAILURE  
     atca\_status.h, 562  
 ATCA\_ASSERT\_FAILURE  
     atca\_status.h, 562  
 ATCA\_BAD\_OPCODE  
     atca\_status.h, 562  
 ATCA\_BAD\_PARAM  
     atca\_status.h, 562  
 atca\_basic.c, 520  
 atca\_basic.h, 528  
 atca\_cfgs.c, 537  
 atca\_cfgs.h, 537  
 ATCA\_CHECK\_INVALID\_MSG  
     atca\_config\_check.h, 540  
 atca\_check\_mac\_in\_out, 373  
     slot\_key, 374  
     target\_key, 374  
 ATCA\_CHECKMAC\_VERIFY\_FAILED  
     atca\_status.h, 562  
 ATCA\_COMM\_FAIL  
     atca\_status.h, 562  
 atca\_compiler.h, 537  
     UNUSED\_VAR, 538  
 atca\_config\_check.h, 538  
     ATCA\_CHECK\_INVALID\_MSG, 540  
     ATCA\_SHA\_SUPPORT, 540  
     ATCA\_UNUSED\_VAR\_CHECK, 540  
     ATCA\_USE\_ATCAB\_FUNCTIONS, 540  
     ATCAB\_AES\_GFM\_EN, 540  
     ATCAB\_GENKEY\_MAC\_EN, 540  
     ATCAB\_INFO\_LATCH\_EN, 540  
     ATCAB\_VERIFY\_MAC\_EN, 541  
     ATCAC\_RANDOM\_EN, 541  
     ATCAC\_SHA1\_EN, 541  
     ATCAC\_SHA256\_EN, 541  
     ATCAC\_SIGN\_EN, 541  
     ATCAC\_VERIFY\_EN, 541  
     ATCACERT\_EN, 542  
     MULTIPART\_BUF\_EN, 542  
 atca\_crypto\_hw\_aes.h, 640  
 atca\_crypto\_hw\_aes\_cbc.c, 640  
 atca\_crypto\_hw\_aes\_cbcmac.c, 641  
 atca\_crypto\_hw\_aes\_ccm.c, 641  
 atca\_crypto\_hw\_aes\_cmac.c, 642  
 atca\_crypto\_hw\_aes\_ctr.c, 642  
 atca\_crypto\_pad.c, 643  
 atca\_crypto\_pbkdf2.c, 643  
 ATCA\_CRYPT\_SHA1\_EN  
     crypto\_sw\_config\_check.h, 649  
 ATCA\_CRYPT\_SHA2\_HMAC\_CTR\_EN  
     crypto\_sw\_config\_check.h, 649  
 ATCA\_CRYPT\_SHA2\_HMAC\_EN  
     crypto\_sw\_config\_check.h, 649  
 atca\_crypto\_sw.h, 644  
 atca\_crypto\_sw\_aes\_gcm.c, 644  
 atca\_crypto\_sw\_sha1.c, 644  
 atca\_crypto\_sw\_sha1.h, 645  
 atca\_crypto\_sw\_sha2.c, 645  
 atca\_crypto\_sw\_sha2.h, 646  
 ATCA\_CUSTOM\_IFACE  
     ATCAIface (atca\_), 168  
 atca\_debug.c, 542  
 atca\_decrypt\_in\_out, 374  
 atca\_delay\_10us  
     Hardware abstraction layer (hal\_), 224  
 atca\_delay\_ms  
     Hardware abstraction layer (hal\_), 224  
 atca\_delay\_us  
     Hardware abstraction layer (hal\_), 225  
 atca\_delete\_in\_out, 374  
 atca\_derive\_key\_in\_out, 375  
 atca\_derive\_key\_mac\_in\_out, 375  
 atca\_device, 376  
     device\_state, 376  
     mlface, 376  
 atca\_device.c, 542  
 atca\_device.h, 543  
 atca\_devtypes.h, 544  
 atca\_diversified\_key\_in\_out, 377  
 atca\_evp\_ctx, 377  
 ATCA\_EXECUTION\_ERROR  
     atca\_status.h, 562  
 ATCA\_FUNC\_FAIL  
     atca\_status.h, 562  
 atca\_gen\_dig\_in\_out, 377  
 ATCA\_GEN\_FAIL  
     atca\_status.h, 563  
 atca\_gen\_key\_in\_out, 378  
 atca\_hal.c, 656  
 atca\_hal.h, 657  
 atca\_hal\_kit\_phy\_t, 379  
     hal\_data, 379  
     packet\_alloc, 379  
     packet\_free, 379

- recv, [379](#)
- send, [379](#)
- atca\_hal\_list\_entry\_t, [380](#)
- phy, [380](#)
- atca\_hal\_shm\_t, [380](#)
- ATCA\_HEALTH\_TEST\_ERROR
  - atca\_status.h, [563](#)
- atca\_helpers.c, [545](#)
  - atcab\_base64decode, [546](#)
  - atcab\_base64decode\_, [547](#)
  - atcab\_base64encode, [547](#)
  - atcab\_base64encode\_, [548](#)
  - atcab\_bin2hex\_, [548](#)
  - atcab\_hex2bin, [549](#)
  - atcab\_reversal, [549](#)
  - isAlpha, [550](#)
  - isBase64, [550](#)
  - isBase64Digit, [551](#)
  - isBlankSpace, [551](#)
  - isDigit, [551](#)
  - isHex, [552](#)
  - isHexAlpha, [552](#)
  - isHexDigit, [552](#)
  - packHex, [553](#)
- atca\_helpers.h, [553](#)
- ATCA\_HID\_IFACE
  - ATCAIface (atca\_), [168](#)
- atca\_hmac\_in\_out, [380](#)
- atca\_host.c, [701](#)
- atca\_host.h, [701](#)
- atca\_host\_config\_check.h, [704](#)
  - ATCAH\_CHECK\_MAC, [705](#)
  - ATCAH\_CONFIG\_TO\_SIGN\_INTERNAL, [705](#)
  - ATCAH\_DECRYPT, [706](#)
  - ATCAH\_DELETE\_MAC, [706](#)
  - ATCAH\_DERIVE\_KEY, [706](#)
  - ATCAH\_DERIVE\_KEY\_MAC, [706](#)
  - ATCAH\_ENCODE\_COUNTER\_MATCH, [706](#)
  - ATCAH\_GEN\_KEY\_MSG, [707](#)
  - ATCAH\_GEN\_MAC, [707](#)
  - ATCAH\_GEN\_OUTPUT\_RESP\_MAC, [707](#)
  - ATCAH\_GEN\_SESSION\_KEY, [707](#)
  - ATCAH\_GENDIG, [707](#)
  - ATCAH\_GENDIVKEY, [708](#)
  - ATCAH\_HMAC, [708](#)
  - ATCAH\_INCLUDE\_DATA, [708](#)
  - ATCAH\_IO\_DECRYPT, [708](#)
  - ATCAH\_MAC, [708](#)
  - ATCAH\_NONCE, [709](#)
  - ATCAH\_PRIVWRITE\_AUTH\_MAC, [709](#)
  - ATCAH\_SECUREBOOT\_ENC, [709](#)
  - ATCAH\_SECUREBOOT\_MAC, [709](#)
  - ATCAH\_SHA256, [709](#)
  - ATCAH\_SIGN\_INTERNAL\_MSG, [710](#)
  - ATCAH\_VERIFY\_MAC, [710](#)
  - ATCAH\_WRITE\_AUTH\_MAC, [710](#)
- ATCA\_I2C\_GPIO\_IFACE
  - ATCAIface (atca\_), [168](#)
- atca\_i2c\_host\_s, [382](#)
- ATCA\_I2C\_IFACE
  - ATCAIface (atca\_), [168](#)
- atca\_iface, [382](#)
  - hal, [382](#)
  - hal\_data, [382](#)
  - mlfaceCFG, [382](#)
  - phy, [382](#)
- atca\_iface.c, [555](#)
- atca\_iface.h, [556](#)
  - address, [559](#)
- atca\_iface\_is\_kit
  - ATCAIface (atca\_), [168](#)
- atca\_iface\_is\_swi
  - ATCAIface (atca\_), [168](#)
- atca\_include\_data\_in\_out, [383](#)
- ATCA\_INVALID\_ID
  - atca\_status.h, [563](#)
- ATCA\_INVALID\_SIZE
  - atca\_status.h, [563](#)
- atca\_io\_decrypt\_in\_out, [383](#)
- atca\_jwt.c, [710](#)
- atca\_jwt.h, [711](#)
- ATCA\_KIT\_IFACE
  - ATCAIface (atca\_), [168](#)
- atca\_mac\_in\_out, [383](#)
- atca\_mbedtls\_ecdh\_ioprot\_cb
  - mbedtls Wrapper methods (atca\_mbedtls\_), [261](#)
- atca\_mbedtls\_ecdh\_slot\_cb
  - mbedtls Wrapper methods (atca\_mbedtls\_), [262](#)
- atca\_mbedtls\_eckey\_info
  - atca\_mbedtls\_wrap.c, [726](#)
- atca\_mbedtls\_eckey\_s, [384](#)
- atca\_mbedtls\_eckey\_t
  - mbedtls Wrapper methods (atca\_mbedtls\_), [261](#)
- atca\_mbedtls\_interface.h, [711](#)
  - ATCAC\_AES\_CMAC\_EN, [712](#)
  - ATCAC\_AES\_GCM\_EN, [712](#)
  - ATCAC\_PKEY\_EN, [712](#)
  - ATCAC\_SHA1\_EN, [712](#)
  - ATCAC\_SHA256\_EN, [712](#)
  - HOSTLIB\_CERT\_EN, [712](#)
- atca\_mbedtls\_pk\_init
  - mbedtls Wrapper methods (atca\_mbedtls\_), [262](#)
- atca\_mbedtls\_pk\_init\_ext
  - mbedtls Wrapper methods (atca\_mbedtls\_), [262](#)
- atca\_mbedtls\_wrap.c, [713](#)
  - atca\_mbedtls\_eckey\_info, [726](#)
  - atcac\_aes\_cmac\_finish, [715](#)
  - atcac\_aes\_cmac\_init, [716](#)
  - atcac\_aes\_cmac\_update, [716](#)
  - atcac\_aes\_gcm\_aad\_update, [716](#)
  - atcac\_aes\_gcm\_decrypt\_finish, [717](#)
  - atcac\_aes\_gcm\_decrypt\_start, [717](#)
  - atcac\_aes\_gcm\_decrypt\_update, [718](#)
  - atcac\_aes\_gcm\_encrypt\_finish, [718](#)
  - atcac\_aes\_gcm\_encrypt\_start, [719](#)
  - atcac\_aes\_gcm\_encrypt\_update, [719](#)

- atcac\_pk\_derive, 720
- atcac\_pk\_free, 720
- atcac\_pk\_init, 720
- atcac\_pk\_init\_pem, 721
- atcac\_pk\_public, 721
- atcac\_pk\_sign, 722
- atcac\_pk\_verify, 722
- atcac\_sha256\_hmac\_finish, 722
- atcac\_sha256\_hmac\_init, 723
- atcac\_sha256\_hmac\_update, 723
- atcac\_sw\_random, 724
- atcac\_sw\_sha1\_finish, 724
- atcac\_sw\_sha1\_init, 724
- atcac\_sw\_sha1\_update, 725
- atcac\_sw\_sha2\_256\_finish, 725
- atcac\_sw\_sha2\_256\_init, 725
- atcac\_sw\_sha2\_256\_update, 726
- ATCA\_NO\_DEVICES
  - atca\_status.h, 563
- atca\_nonce\_in\_out, 384
- ATCA\_NOT\_INITIALIZED
  - atca\_status.h, 563
- ATCA\_NOT\_LOCKED
  - atca\_status.h, 563
- atca\_openssl\_interface.c, 727
  - atcac\_aes\_cmac\_finish, 729
  - atcac\_aes\_cmac\_init, 729
  - atcac\_aes\_cmac\_update, 730
  - atcac\_aes\_gcm\_aad\_update, 730
  - atcac\_aes\_gcm\_decrypt\_finish, 731
  - atcac\_aes\_gcm\_decrypt\_start, 731
  - atcac\_aes\_gcm\_decrypt\_update, 732
  - atcac\_aes\_gcm\_encrypt\_finish, 732
  - atcac\_aes\_gcm\_encrypt\_start, 733
  - atcac\_aes\_gcm\_encrypt\_update, 733
  - atcac\_pk\_derive, 734
  - atcac\_pk\_free, 734
  - atcac\_pk\_init, 734
  - atcac\_pk\_init\_pem, 735
  - atcac\_pk\_public, 735
  - atcac\_pk\_sign, 736
  - atcac\_pk\_verify, 736
  - atcac\_sha256\_hmac\_finish, 736
  - atcac\_sha256\_hmac\_init, 737
  - atcac\_sha256\_hmac\_update, 737
  - atcac\_sw\_random, 738
  - atcac\_sw\_sha1\_finish, 738
  - atcac\_sw\_sha1\_init, 738
  - atcac\_sw\_sha1\_update, 739
  - atcac\_sw\_sha2\_256\_finish, 739
  - atcac\_sw\_sha2\_256\_init, 739
  - atcac\_sw\_sha2\_256\_update, 740
- atca\_openssl\_interface.h, 740
  - ATCAC\_AES\_CMACE\_EN, 741
  - ATCAC\_AES\_GCM\_EN, 741
  - ATCAC\_PKEY\_EN, 741
  - ATCAC\_SHA1\_EN, 742
  - ATCAC\_SHA256\_EN, 742
  - HOSTLIB\_CERT\_EN, 742
  - ATCA\_PARITY\_ERROR
    - atca\_status.h, 563
  - ATCA\_PARSE\_ERROR
    - atca\_status.h, 564
  - atca\_platform.h, 560
  - atca\_plib\_i2c\_api, 385
  - atca\_resp\_mac\_in\_out, 385
  - ATCA\_RESYNC\_WITH\_WAKEUP
    - atca\_status.h, 564
  - ATCA\_RX\_CRC\_ERROR
    - atca\_status.h, 564
  - ATCA\_RX\_FAIL
    - atca\_status.h, 564
  - ATCA\_RX\_NO\_RESPONSE
    - atca\_status.h, 564
  - ATCA\_RX\_TIMEOUT
    - atca\_status.h, 564
  - atca\_secureboot\_enc\_in\_out, 386
  - atca\_secureboot\_mac\_in\_out, 386
  - atca\_session\_key\_in\_out, 386
  - ATCA\_SHA256\_BLOCK\_SIZE
    - cryptoauthlib.h, 655
  - atca\_sha256\_ctx, 387
  - ATCA\_SHA\_SUPPORT
    - atca\_config\_check.h, 540
  - atca\_sign\_internal\_in\_out, 388
  - ATCA\_SMALL\_BUFFER
    - atca\_status.h, 564
  - ATCA\_SPI\_GPIO\_IFACE
    - ATCAIface (atca\_), 168
  - atca\_spi\_host\_s, 389
  - ATCA\_SPI\_IFACE
    - ATCAIface (atca\_), 168
  - atca\_status.h, 560
    - ATCA\_ALLOC\_FAILURE, 562
    - ATCA\_ASSERT\_FAILURE, 562
    - ATCA\_BAD\_OPCODE, 562
    - ATCA\_BAD\_PARAM, 562
    - ATCA\_CHECKMAC\_VERIFY\_FAILED, 562
    - ATCA\_COMM\_FAIL, 562
    - ATCA\_EXECUTION\_ERROR, 562
    - ATCA\_FUNC\_FAIL, 562
    - ATCA\_GEN\_FAIL, 563
    - ATCA\_HEALTH\_TEST\_ERROR, 563
    - ATCA\_INVALID\_ID, 563
    - ATCA\_INVALID\_SIZE, 563
    - ATCA\_NO\_DEVICES, 563
    - ATCA\_NOT\_INITIALIZED, 563
    - ATCA\_NOT\_LOCKED, 563
    - ATCA\_PARITY\_ERROR, 563
    - ATCA\_PARSE\_ERROR, 564
    - ATCA\_RESYNC\_WITH\_WAKEUP, 564
    - ATCA\_RX\_CRC\_ERROR, 564
    - ATCA\_RX\_FAIL, 564
    - ATCA\_RX\_NO\_RESPONSE, 564
    - ATCA\_RX\_TIMEOUT, 564
    - ATCA\_SMALL\_BUFFER, 564

- ATCA\_STATUS\_CRC, [564](#)
- ATCA\_STATUS\_ECC, [565](#)
- ATCA\_STATUS\_SELFTEST\_ERROR, [565](#)
- ATCA\_STATUS\_UNKNOWN, [565](#)
- ATCA\_SUCCESS, [565](#)
- ATCA\_TIMEOUT, [565](#)
- ATCA\_TOO\_MANY\_COMM\_RETRIES, [565](#)
- ATCA\_TX\_FAIL, [565](#)
- ATCA\_TX\_TIMEOUT, [565](#)
- ATCA\_UNIMPLEMENTED, [566](#)
- ATCA\_USE\_FLAGS\_CONSUMED, [566](#)
- ATCA\_WAKE\_FAILED, [566](#)
- ATCA\_WAKE\_SUCCESS, [566](#)
- ATCA\_STATUS\_CRC
  - [atca\\_status.h](#), [564](#)
- ATCA\_STATUS\_ECC
  - [atca\\_status.h](#), [565](#)
- ATCA\_STATUS\_SELFTEST\_ERROR
  - [atca\\_status.h](#), [565](#)
- ATCA\_STATUS\_UNKNOWN
  - [atca\\_status.h](#), [565](#)
- ATCA\_SUCCESS
  - [atca\\_status.h](#), [565](#)
- ATCA\_SWI\_GPIO\_IFACE
  - [ATCAIface](#) ([atca\\_](#)), [168](#)
- ATCA\_SWI\_IFACE
  - [ATCAIface](#) ([atca\\_](#)), [168](#)
- ATCA\_SWI\_WAKE\_WORD\_ADDR
  - [hal\\_swi\\_gpio.h](#), [682](#)
- [atca\\_temp\\_key](#), [389](#)
- ATCA\_TIMEOUT
  - [atca\\_status.h](#), [565](#)
- ATCA\_TOO\_MANY\_COMM\_RETRIES
  - [atca\\_status.h](#), [565](#)
- ATCA\_TX\_FAIL
  - [atca\\_status.h](#), [565](#)
- ATCA\_TX\_TIMEOUT
  - [atca\\_status.h](#), [565](#)
- [atca\\_uart\\_host\\_s](#), [390](#)
- ATCA\_UART\_IFACE
  - [ATCAIface](#) ([atca\\_](#)), [168](#)
- ATCA\_UNIMPLEMENTED
  - [atca\\_status.h](#), [566](#)
- ATCA\_UNUSED\_VAR\_CHECK
  - [atca\\_config\\_check.h](#), [540](#)
- ATCA\_USE\_ATCAB\_FUNCTIONS
  - [atca\\_config\\_check.h](#), [540](#)
- ATCA\_USE\_FLAGS\_CONSUMED
  - [atca\\_status.h](#), [566](#)
- [atca\\_utils\\_sizes.c](#), [566](#)
- [atca\\_verify\\_in\\_out](#), [390](#)
- [atca\\_verify\\_mac](#), [390](#)
- [atca\\_version.h](#), [568](#)
- ATCA\_WAKE\_FAILED
  - [atca\\_status.h](#), [566](#)
- ATCA\_WAKE\_SUCCESS
  - [atca\\_status.h](#), [566](#)
- [atca\\_wolfssl\\_interface.c](#), [776](#)
- [atca\\_wolfssl\\_interface.h](#), [776](#)
- [atca\\_wolfssl\\_internal.h](#), [777](#)
- [atca\\_write\\_mac\\_in\\_out](#), [391](#)
- atcab\_aes
  - Basic Crypto API methods ([atcab\\_](#)), [89](#)
  - [cryptoauthlib.atcab](#), [280](#)
- atcab\_aes\_cbc\_decrypt\_block
  - [cryptoauthlib.atcab](#), [280](#)
- ATCAB\_AES\_CBC\_DECRYPT\_EN
  - [crypto\\_hw\\_config\\_check.h](#), [647](#)
- atcab\_aes\_cbc\_encrypt\_block
  - [cryptoauthlib.atcab](#), [281](#)
- ATCAB\_AES\_CBC\_ENCRYPT\_EN
  - [crypto\\_hw\\_config\\_check.h](#), [647](#)
- atcab\_aes\_cbc\_init
  - [cryptoauthlib.atcab](#), [281](#)
- ATCAB\_AES\_CBCMAC\_EN
  - [crypto\\_hw\\_config\\_check.h](#), [647](#)
- atcab\_aes\_cbcmac\_finish
  - [cryptoauthlib.atcab](#), [282](#)
- atcab\_aes\_cbcmac\_init
  - [cryptoauthlib.atcab](#), [282](#)
- atcab\_aes\_cbcmac\_update
  - [cryptoauthlib.atcab](#), [282](#)
- atcab\_aes\_ccm\_aad\_finish
  - [cryptoauthlib.atcab](#), [283](#)
- atcab\_aes\_ccm\_aad\_update
  - [cryptoauthlib.atcab](#), [283](#)
- atcab\_aes\_ccm\_decrypt\_finish
  - [cryptoauthlib.atcab](#), [283](#)
- atcab\_aes\_ccm\_decrypt\_update
  - [cryptoauthlib.atcab](#), [284](#)
- ATCAB\_AES\_CCM\_EN
  - [crypto\\_hw\\_config\\_check.h](#), [647](#)
- atcab\_aes\_ccm\_encrypt\_finish
  - [cryptoauthlib.atcab](#), [284](#)
- atcab\_aes\_ccm\_encrypt\_update
  - [cryptoauthlib.atcab](#), [284](#)
- atcab\_aes\_ccm\_init
  - [cryptoauthlib.atcab](#), [285](#)
- atcab\_aes\_ccm\_init\_rand
  - [cryptoauthlib.atcab](#), [285](#)
- atcab\_aes\_cmac\_finish
  - [cryptoauthlib.atcab](#), [286](#)
- atcab\_aes\_cmac\_init
  - [cryptoauthlib.atcab](#), [286](#)
- atcab\_aes\_cmac\_update
  - [cryptoauthlib.atcab](#), [286](#)
- atcab\_aes\_ctr\_decrypt\_block
  - [cryptoauthlib.atcab](#), [287](#)
- ATCAB\_AES\_CTR\_EN
  - [crypto\\_hw\\_config\\_check.h](#), [648](#)
- atcab\_aes\_ctr\_encrypt\_block
  - [cryptoauthlib.atcab](#), [287](#)
- atcab\_aes\_ctr\_init
  - [cryptoauthlib.atcab](#), [287](#)
- atcab\_aes\_ctr\_init\_rand
  - [cryptoauthlib.atcab](#), [288](#)

- ATCAB\_AES\_CTR RAND\_IV\_EN
  - crypto\_hw\_config\_check.h, [648](#)
- atcab\_aes\_decrypt
  - Basic Crypto API methods (atcab\_), [89](#)
  - cryptoauthlib.atcab, [288](#)
- atcab\_aes\_decrypt\_ext
  - Basic Crypto API methods (atcab\_), [90](#)
- atcab\_aes\_encrypt
  - Basic Crypto API methods (atcab\_), [90](#)
  - cryptoauthlib.atcab, [289](#)
- atcab\_aes\_encrypt\_ext
  - Basic Crypto API methods (atcab\_), [91](#)
- ATCAB\_AES\_EXTRAS\_EN
  - crypto\_hw\_config\_check.h, [648](#)
- atcab\_aes\_gcm\_aad\_update
  - Basic Crypto API methods (atcab\_), [91](#)
  - cryptoauthlib.atcab, [289](#)
- atcab\_aes\_gcm\_aad\_update\_ext
  - Basic Crypto API methods (atcab\_), [92](#)
- atcab\_aes\_gcm\_decrypt\_finish
  - Basic Crypto API methods (atcab\_), [92](#)
  - cryptoauthlib.atcab, [290](#)
- atcab\_aes\_gcm\_decrypt\_finish\_ext
  - Basic Crypto API methods (atcab\_), [93](#)
- atcab\_aes\_gcm\_decrypt\_update
  - Basic Crypto API methods (atcab\_), [93](#)
  - cryptoauthlib.atcab, [290](#)
- atcab\_aes\_gcm\_decrypt\_update\_ext
  - Basic Crypto API methods (atcab\_), [94](#)
- atcab\_aes\_gcm\_encrypt\_finish
  - Basic Crypto API methods (atcab\_), [94](#)
  - cryptoauthlib.atcab, [290](#)
- atcab\_aes\_gcm\_encrypt\_finish\_ext
  - Basic Crypto API methods (atcab\_), [95](#)
- atcab\_aes\_gcm\_encrypt\_update
  - Basic Crypto API methods (atcab\_), [95](#)
  - cryptoauthlib.atcab, [291](#)
- atcab\_aes\_gcm\_encrypt\_update\_ext
  - Basic Crypto API methods (atcab\_), [96](#)
- atcab\_aes\_gcm\_init
  - Basic Crypto API methods (atcab\_), [96](#)
  - cryptoauthlib.atcab, [291](#)
- atcab\_aes\_gcm\_init\_ext
  - Basic Crypto API methods (atcab\_), [97](#)
- atcab\_aes\_gcm\_init\_rand
  - Basic Crypto API methods (atcab\_), [97](#)
  - cryptoauthlib.atcab, [291](#)
- atcab\_aes\_gfm
  - Basic Crypto API methods (atcab\_), [98](#)
  - cryptoauthlib.atcab, [292](#)
- ATCAB\_AES\_GFM\_EN
  - atca\_config\_check.h, [540](#)
- ATCAB\_AES\_UPDATE\_EN
  - crypto\_hw\_config\_check.h, [648](#)
- atcab\_base64decode
  - atca\_helpers.c, [546](#)
  - Basic Crypto API methods (atcab\_), [98](#)
- atcab\_base64decode\_
  - atca\_helpers.c, [547](#)
  - Basic Crypto API methods (atcab\_), [99](#)
- atcab\_base64encode
  - atca\_helpers.c, [547](#)
  - Basic Crypto API methods (atcab\_), [99](#)
- atcab\_base64encode\_
  - atca\_helpers.c, [548](#)
  - Basic Crypto API methods (atcab\_), [100](#)
- atcab\_bin2hex
  - Basic Crypto API methods (atcab\_), [100](#)
- atcab\_bin2hex\_
  - atca\_helpers.c, [548](#)
  - Basic Crypto API methods (atcab\_), [101](#)
- atcab\_challenge
  - Basic Crypto API methods (atcab\_), [101](#)
  - cryptoauthlib.atcab, [292](#)
- atcab\_challenge\_seed\_update
  - Basic Crypto API methods (atcab\_), [102](#)
  - cryptoauthlib.atcab, [293](#)
- atcab\_checkmac
  - Basic Crypto API methods (atcab\_), [102](#)
  - cryptoauthlib.atcab, [293](#)
- atcab\_checkmac\_with\_response\_mac
  - Basic Crypto API methods (atcab\_), [103](#)
- atcab\_cmp\_config\_zone
  - Basic Crypto API methods (atcab\_), [103](#)
  - cryptoauthlib.atcab, [293](#)
- atcab\_counter
  - Basic Crypto API methods (atcab\_), [104](#)
  - cryptoauthlib.atcab, [294](#)
- atcab\_counter\_increment
  - Basic Crypto API methods (atcab\_), [104](#)
  - cryptoauthlib.atcab, [294](#)
- atcab\_counter\_read
  - Basic Crypto API methods (atcab\_), [104](#)
  - cryptoauthlib.atcab, [294](#)
- atcab\_derivekey
  - Basic Crypto API methods (atcab\_), [105](#)
  - cryptoauthlib.atcab, [295](#)
- atcab\_derivekey\_ext
  - Basic Crypto API methods (atcab\_), [105](#)
- atcab\_ecdh
  - Basic Crypto API methods (atcab\_), [106](#)
  - cryptoauthlib.atcab, [295](#)
- atcab\_ecdh\_base
  - Basic Crypto API methods (atcab\_), [106](#)
  - cryptoauthlib.atcab, [295](#)
- atcab\_ecdh\_enc
  - Basic Crypto API methods (atcab\_), [107](#)
  - cryptoauthlib.atcab, [296](#)
- atcab\_ecdh\_ioenc
  - Basic Crypto API methods (atcab\_), [107](#)
  - cryptoauthlib.atcab, [296](#)
- atcab\_ecdh\_tempkey
  - Basic Crypto API methods (atcab\_), [108](#)
  - cryptoauthlib.atcab, [297](#)
- atcab\_ecdh\_tempkey\_ioenc
  - Basic Crypto API methods (atcab\_), [108](#)

- cryptoauthlib.atcab, [297](#)
- atcab\_gendig
  - Basic Crypto API methods (atcab\_), [108](#)
  - cryptoauthlib.atcab, [298](#)
- atcab\_gendivkey
  - Basic Crypto API methods (atcab\_), [109](#)
- atcab\_genkey
  - Basic Crypto API methods (atcab\_), [109](#)
  - cryptoauthlib.atcab, [298](#)
- atcab\_genkey\_base
  - Basic Crypto API methods (atcab\_), [110](#)
  - cryptoauthlib.atcab, [298](#)
- atcab\_genkey\_ext
  - Basic Crypto API methods (atcab\_), [110](#)
- ATCAB\_GENKEY\_MAC\_EN
  - atca\_config\_check.h, [540](#)
- atcab\_get\_device
  - Basic Crypto API methods (atcab\_), [111](#)
  - cryptoauthlib.atcab, [299](#)
- atcab\_get\_device\_address
  - Basic Crypto API methods (atcab\_), [111](#)
- atcab\_get\_device\_type
  - Basic Crypto API methods (atcab\_), [111](#)
  - cryptoauthlib.atcab, [299](#)
- atcab\_get\_device\_type\_ext
  - Basic Crypto API methods (atcab\_), [111](#)
- atcab\_get\_pubkey
  - Basic Crypto API methods (atcab\_), [112](#)
  - cryptoauthlib.atcab, [299](#)
- atcab\_get\_pubkey\_ext
  - Basic Crypto API methods (atcab\_), [112](#)
- atcab\_get\_zone\_size
  - Basic Crypto API methods (atcab\_), [113](#)
- atcab\_get\_zone\_size\_ext
  - Basic Crypto API methods (atcab\_), [113](#)
- atcab\_hex2bin
  - atca\_helpers.c, [549](#)
  - Basic Crypto API methods (atcab\_), [113](#)
- atcab\_hmac
  - Basic Crypto API methods (atcab\_), [114](#)
  - cryptoauthlib.atcab, [300](#)
- atcab\_hw\_sha2\_256
  - Basic Crypto API methods (atcab\_), [114](#)
  - cryptoauthlib.atcab, [300](#)
- atcab\_hw\_sha2\_256\_finish
  - Basic Crypto API methods (atcab\_), [115](#)
  - cryptoauthlib.atcab, [300](#)
- atcab\_hw\_sha2\_256\_init
  - Basic Crypto API methods (atcab\_), [115](#)
  - cryptoauthlib.atcab, [301](#)
- atcab\_hw\_sha2\_256\_update
  - Basic Crypto API methods (atcab\_), [115](#)
  - cryptoauthlib.atcab, [301](#)
- atcab\_idle
  - Basic Crypto API methods (atcab\_), [116](#)
- atcab\_info
  - Basic Crypto API methods (atcab\_), [116](#)
  - cryptoauthlib.atcab, [301](#)
- atcab\_info\_base
  - Basic Crypto API methods (atcab\_), [116](#)
  - cryptoauthlib.atcab, [302](#)
- atcab\_info\_chip\_status
  - Basic Crypto API methods (atcab\_), [117](#)
- atcab\_info\_ext
  - Basic Crypto API methods (atcab\_), [117](#)
- atcab\_info\_get\_latch
  - Basic Crypto API methods (atcab\_), [118](#)
  - cryptoauthlib.atcab, [302](#)
- ATCAB\_INFO\_LATCH\_EN
  - atca\_config\_check.h, [540](#)
- atcab\_info\_lock\_status
  - Basic Crypto API methods (atcab\_), [118](#)
- atcab\_info\_set\_latch
  - Basic Crypto API methods (atcab\_), [118](#)
  - cryptoauthlib.atcab, [302](#)
- atcab\_init
  - Basic Crypto API methods (atcab\_), [119](#)
  - cryptoauthlib.atcab, [303](#)
- atcab\_init\_device
  - Basic Crypto API methods (atcab\_), [119](#)
- atcab\_init\_ext
  - Basic Crypto API methods (atcab\_), [119](#)
- atcab\_is\_ca2\_device
  - Basic Crypto API methods (atcab\_), [120](#)
- atcab\_is\_ca\_device
  - Basic Crypto API methods (atcab\_), [120](#)
- atcab\_is\_config\_locked
  - Basic Crypto API methods (atcab\_), [120](#)
- atcab\_is\_config\_locked\_ext
  - Basic Crypto API methods (atcab\_), [121](#)
- atcab\_is\_data\_locked
  - Basic Crypto API methods (atcab\_), [121](#)
- atcab\_is\_data\_locked\_ext
  - Basic Crypto API methods (atcab\_), [121](#)
- atcab\_is\_locked
  - Basic Crypto API methods (atcab\_), [122](#)
  - cryptoauthlib.atcab, [303](#)
- atcab\_is\_private\_ext
  - Basic Crypto API methods (atcab\_), [122](#)
- atcab\_is\_slot\_locked
  - Basic Crypto API methods (atcab\_), [123](#)
  - cryptoauthlib.atcab, [303](#)
- atcab\_is\_slot\_locked\_ext
  - Basic Crypto API methods (atcab\_), [123](#)
- atcab\_is\_ta\_device
  - Basic Crypto API methods (atcab\_), [124](#)
- atcab\_kdf
  - Basic Crypto API methods (atcab\_), [124](#)
  - cryptoauthlib.atcab, [304](#)
- atcab\_lock
  - Basic Crypto API methods (atcab\_), [124](#)
  - cryptoauthlib.atcab, [304](#)
- atcab\_lock\_config\_zone
  - Basic Crypto API methods (atcab\_), [125](#)
  - cryptoauthlib.atcab, [305](#)
- atcab\_lock\_config\_zone\_crc



- Basic Crypto API methods (atcab\_), 125
- cryptoauthlib.atcab, 305
- atcab\_lock\_config\_zone\_ext
  - Basic Crypto API methods (atcab\_), 126
- atcab\_lock\_data\_slot
  - Basic Crypto API methods (atcab\_), 126
  - cryptoauthlib.atcab, 305
- atcab\_lock\_data\_slot\_ext
  - Basic Crypto API methods (atcab\_), 126
- atcab\_lock\_data\_zone
  - Basic Crypto API methods (atcab\_), 127
  - cryptoauthlib.atcab, 306
- atcab\_lock\_data\_zone\_crc
  - Basic Crypto API methods (atcab\_), 127
  - cryptoauthlib.atcab, 306
- atcab\_lock\_data\_zone\_ext
  - Basic Crypto API methods (atcab\_), 127
- atcab\_mac
  - Basic Crypto API methods (atcab\_), 128
  - cryptoauthlib.atcab, 306
- atcab\_nonce
  - Basic Crypto API methods (atcab\_), 128
  - cryptoauthlib.atcab, 307
- atcab\_nonce\_base
  - Basic Crypto API methods (atcab\_), 129
  - cryptoauthlib.atcab, 307
- atcab\_nonce\_load
  - Basic Crypto API methods (atcab\_), 129
  - cryptoauthlib.atcab, 308
- atcab\_nonce\_rand
  - Basic Crypto API methods (atcab\_), 130
  - cryptoauthlib.atcab, 308
- atcab\_nonce\_rand\_ext
  - Basic Crypto API methods (atcab\_), 130
- ATCAB\_PBKDF2\_SHA256\_EN
  - crypto\_sw\_config\_check.h, 650
- atcab\_priv\_write
  - Basic Crypto API methods (atcab\_), 131
  - cryptoauthlib.atcab, 309
- atcab\_random
  - Basic Crypto API methods (atcab\_), 131
  - cryptoauthlib.atcab, 309
- atcab\_random\_ext
  - Basic Crypto API methods (atcab\_), 131
- atcab\_read\_bytes\_zone
  - Basic Crypto API methods (atcab\_), 132
  - cryptoauthlib.atcab, 309
- atcab\_read\_config\_zone
  - Basic Crypto API methods (atcab\_), 132
  - cryptoauthlib.atcab, 310
- atcab\_read\_config\_zone\_ext
  - Basic Crypto API methods (atcab\_), 133
- atcab\_read\_enc
  - Basic Crypto API methods (atcab\_), 133
  - cryptoauthlib.atcab, 310
- atcab\_read\_pubkey
  - Basic Crypto API methods (atcab\_), 134
  - cryptoauthlib.atcab, 311
- atcab\_read\_pubkey\_ext
  - Basic Crypto API methods (atcab\_), 134
- atcab\_read\_serial\_number
  - Basic Crypto API methods (atcab\_), 135
  - cryptoauthlib.atcab, 311
- atcab\_read\_serial\_number\_ext
  - Basic Crypto API methods (atcab\_), 135
- atcab\_read\_sig
  - Basic Crypto API methods (atcab\_), 135
  - cryptoauthlib.atcab, 311
- atcab\_read\_zone
  - Basic Crypto API methods (atcab\_), 136
  - cryptoauthlib.atcab, 312
- atcab\_read\_zone\_ext
  - Basic Crypto API methods (atcab\_), 136
- atcab\_release
  - Basic Crypto API methods (atcab\_), 137
  - cryptoauthlib.atcab, 312
- atcab\_release\_ext
  - Basic Crypto API methods (atcab\_), 137
- atcab\_reversal
  - atca\_helpers.c, 549
  - Basic Crypto API methods (atcab\_), 137
- atcab\_secureboot
  - Basic Crypto API methods (atcab\_), 138
  - cryptoauthlib.atcab, 312
- atcab\_secureboot\_mac
  - Basic Crypto API methods (atcab\_), 138
  - cryptoauthlib.atcab, 313
- atcab\_selftest
  - Basic Crypto API methods (atcab\_), 139
  - cryptoauthlib.atcab, 313
- atcab\_sha
  - Basic Crypto API methods (atcab\_), 139
  - cryptoauthlib.atcab, 314
- atcab\_sha\_base
  - Basic Crypto API methods (atcab\_), 140
  - cryptoauthlib.atcab, 314
- atcab\_sha\_end
  - Basic Crypto API methods (atcab\_), 141
  - cryptoauthlib.atcab, 315
- atcab\_sha\_hmac
  - Basic Crypto API methods (atcab\_), 141
  - cryptoauthlib.atcab, 315
- atcab\_sha\_hmac\_ext
  - Basic Crypto API methods (atcab\_), 141
- atcab\_sha\_hmac\_finish
  - Basic Crypto API methods (atcab\_), 142
  - cryptoauthlib.atcab, 316
- atcab\_sha\_hmac\_init
  - Basic Crypto API methods (atcab\_), 143
  - cryptoauthlib.atcab, 316
- atcab\_sha\_hmac\_update
  - Basic Crypto API methods (atcab\_), 143
  - cryptoauthlib.atcab, 316
- atcab\_sha\_read\_context
  - Basic Crypto API methods (atcab\_), 143
  - cryptoauthlib.atcab, 317

- atcab\_sha\_start
  - Basic Crypto API methods (atcab\_), 144
  - cryptoauthlib.atcab, 317
- atcab\_sha\_update
  - Basic Crypto API methods (atcab\_), 144
  - cryptoauthlib.atcab, 317
- atcab\_sha\_write\_context
  - Basic Crypto API methods (atcab\_), 144
  - cryptoauthlib.atcab, 318
- atcab\_sign
  - Basic Crypto API methods (atcab\_), 145
  - cryptoauthlib.atcab, 318
- atcab\_sign\_base
  - Basic Crypto API methods (atcab\_), 145
  - cryptoauthlib.atcab, 318
- atcab\_sign\_ext
  - Basic Crypto API methods (atcab\_), 146
- atcab\_sign\_internal
  - Basic Crypto API methods (atcab\_), 146
  - cryptoauthlib.atcab, 319
- atcab\_sleep
  - Basic Crypto API methods (atcab\_), 147
- atcab\_updateextra
  - Basic Crypto API methods (atcab\_), 147
  - cryptoauthlib.atcab, 319
- atcab\_verify
  - Basic Crypto API methods (atcab\_), 147
  - cryptoauthlib.atcab, 319
- atcab\_verify\_extern
  - Basic Crypto API methods (atcab\_), 148
  - cryptoauthlib.atcab, 320
- atcab\_verify\_extern\_ext
  - Basic Crypto API methods (atcab\_), 149
- atcab\_verify\_extern\_mac
  - Basic Crypto API methods (atcab\_), 149
  - cryptoauthlib.atcab, 321
- atcab\_verify\_extern\_stored\_mac
  - cryptoauthlib.atcab, 321
- atcab\_verify\_invalidate
  - Basic Crypto API methods (atcab\_), 150
  - cryptoauthlib.atcab, 322
- ATCAB\_VERIFY\_MAC\_EN
  - atca\_config\_check.h, 541
- atcab\_verify\_stored
  - Basic Crypto API methods (atcab\_), 150
  - cryptoauthlib.atcab, 322
- atcab\_verify\_stored\_ext
  - Basic Crypto API methods (atcab\_), 151
- atcab\_verify\_stored\_mac
  - Basic Crypto API methods (atcab\_), 151
  - cryptoauthlib.atcab, 323
- atcab\_verify\_stored\_with\_tempkey
  - Basic Crypto API methods (atcab\_), 152
- atcab\_verify\_validate
  - Basic Crypto API methods (atcab\_), 152
  - cryptoauthlib.atcab, 323
- atcab\_version
  - Basic Crypto API methods (atcab\_), 153
- atcab\_wakeup
  - Basic Crypto API methods (atcab\_), 153
- atcab\_write
  - Basic Crypto API methods (atcab\_), 153
  - cryptoauthlib.atcab, 324
- atcab\_write\_bytes\_zone
  - Basic Crypto API methods (atcab\_), 154
  - cryptoauthlib.atcab, 324
- atcab\_write\_config\_counter
  - Basic Crypto API methods (atcab\_), 155
  - cryptoauthlib.atcab, 325
- atcab\_write\_config\_zone
  - Basic Crypto API methods (atcab\_), 155
  - cryptoauthlib.atcab, 325
- atcab\_write\_config\_zone\_ext
  - Basic Crypto API methods (atcab\_), 155
- atcab\_write\_enc
  - Basic Crypto API methods (atcab\_), 156
  - cryptoauthlib.atcab, 325
- atcab\_write\_pubkey
  - Basic Crypto API methods (atcab\_), 156
  - cryptoauthlib.atcab, 326
- atcab\_write\_pubkey\_ext
  - Basic Crypto API methods (atcab\_), 157
- atcab\_write\_zone
  - Basic Crypto API methods (atcab\_), 157
  - cryptoauthlib.atcab, 326
- atcab\_write\_zone\_ext
  - Basic Crypto API methods (atcab\_), 159
- atcac\_aes\_cmac\_ctx, 396
- ATCAC\_AES\_CMAC\_EN
  - atca\_mbedtls\_interface.h, 712
  - atca\_openssl\_interface.h, 741
- atcac\_aes\_cmac\_finish
  - atca\_mbedtls\_wrap.c, 715
  - atca\_openssl\_interface.c, 729
- atcac\_aes\_cmac\_init
  - atca\_mbedtls\_wrap.c, 716
  - atca\_openssl\_interface.c, 729
- atcac\_aes\_cmac\_update
  - atca\_mbedtls\_wrap.c, 716
  - atca\_openssl\_interface.c, 730
- atcac\_aes\_gcm\_aad\_update
  - atca\_mbedtls\_wrap.c, 716
  - atca\_openssl\_interface.c, 730
- atcac\_aes\_gcm\_ctx, 396
- atcac\_aes\_gcm\_decrypt\_finish
  - atca\_mbedtls\_wrap.c, 717
  - atca\_openssl\_interface.c, 731
- atcac\_aes\_gcm\_decrypt\_start
  - atca\_mbedtls\_wrap.c, 717
  - atca\_openssl\_interface.c, 731
- atcac\_aes\_gcm\_decrypt\_update
  - atca\_mbedtls\_wrap.c, 718
  - atca\_openssl\_interface.c, 732
- ATCAC\_AES\_GCM\_EN
  - atca\_mbedtls\_interface.h, 712
  - atca\_openssl\_interface.h, 741



- crypto\_sw\_config\_check.h, 650
- atcac\_aes\_gcm\_encrypt\_finish
  - atca\_mbedtls\_wrap.c, 718
  - atca\_openssl\_interface.c, 732
- atcac\_aes\_gcm\_encrypt\_start
  - atca\_mbedtls\_wrap.c, 719
  - atca\_openssl\_interface.c, 733
- atcac\_aes\_gcm\_encrypt\_update
  - atca\_mbedtls\_wrap.c, 719
  - atca\_openssl\_interface.c, 733
- atcac\_hmac\_ctx, 396
- ATCAC\_PBKDF2\_SHA256\_EN
  - crypto\_sw\_config\_check.h, 650
- atcac\_pk\_ctx, 396
- atcac\_pk\_derive
  - atca\_mbedtls\_wrap.c, 720
  - atca\_openssl\_interface.c, 734
- atcac\_pk\_free
  - atca\_mbedtls\_wrap.c, 720
  - atca\_openssl\_interface.c, 734
- atcac\_pk\_init
  - atca\_mbedtls\_wrap.c, 720
  - atca\_openssl\_interface.c, 734
- atcac\_pk\_init\_pem
  - atca\_mbedtls\_wrap.c, 721
  - atca\_openssl\_interface.c, 735
- atcac\_pk\_public
  - atca\_mbedtls\_wrap.c, 721
  - atca\_openssl\_interface.c, 735
- atcac\_pk\_sign
  - atca\_mbedtls\_wrap.c, 722
  - atca\_openssl\_interface.c, 736
- atcac\_pk\_verify
  - atca\_mbedtls\_wrap.c, 722
  - atca\_openssl\_interface.c, 736
- ATCAC\_PKEY\_EN
  - atca\_mbedtls\_interface.h, 712
  - atca\_openssl\_interface.h, 741
- ATCAC\_RANDOM\_EN
  - atca\_config\_check.h, 541
  - crypto\_sw\_config\_check.h, 650
- atcac\_sha1\_ctx, 396
- ATCAC\_SHA1\_EN
  - atca\_config\_check.h, 541
  - atca\_mbedtls\_interface.h, 712
  - atca\_openssl\_interface.h, 742
  - crypto\_sw\_config\_check.h, 650
- ATCAC\_SHA256\_EN
  - atca\_config\_check.h, 541
  - atca\_mbedtls\_interface.h, 712
  - atca\_openssl\_interface.h, 742
  - crypto\_sw\_config\_check.h, 651
- atcac\_sha256\_hmac\_finish
  - atca\_mbedtls\_wrap.c, 722
  - atca\_openssl\_interface.c, 736
- atcac\_sha256\_hmac\_init
  - atca\_mbedtls\_wrap.c, 723
  - atca\_openssl\_interface.c, 737
- atcac\_sha256\_hmac\_update
  - atca\_mbedtls\_wrap.c, 723
  - atca\_openssl\_interface.c, 737
- atcac\_sha2\_256\_ctx, 396
- ATCAC\_SIGN\_EN
  - atca\_config\_check.h, 541
  - crypto\_sw\_config\_check.h, 651
- atcac\_sw\_random
  - atca\_mbedtls\_wrap.c, 724
  - atca\_openssl\_interface.c, 738
- atcac\_sw\_sha1\_finish
  - atca\_mbedtls\_wrap.c, 724
  - atca\_openssl\_interface.c, 738
- atcac\_sw\_sha1\_init
  - atca\_mbedtls\_wrap.c, 724
  - atca\_openssl\_interface.c, 738
- atcac\_sw\_sha1\_update
  - atca\_mbedtls\_wrap.c, 725
  - atca\_openssl\_interface.c, 739
- atcac\_sw\_sha2\_256\_finish
  - atca\_mbedtls\_wrap.c, 725
  - atca\_openssl\_interface.c, 739
- atcac\_sw\_sha2\_256\_init
  - atca\_mbedtls\_wrap.c, 725
  - atca\_openssl\_interface.c, 739
- atcac\_sw\_sha2\_256\_update
  - atca\_mbedtls\_wrap.c, 726
  - atca\_openssl\_interface.c, 740
- ATCAC\_VERIFY\_EN
  - atca\_config\_check.h, 541
  - crypto\_sw\_config\_check.h, 651
- atcac\_x509\_ctx, 397
- atcacert.h, 568
- atcacert\_build\_state\_s, 397
- atcacert\_build\_state\_t
  - Certificate manipulation methods (atcacert\_), 181
- atcacert\_calc\_expire\_years
  - Certificate manipulation methods (atcacert\_), 184
- atcacert\_cert\_element\_s, 397
- atcacert\_cert\_element\_t
  - Certificate manipulation methods (atcacert\_), 181
- atcacert\_cert\_loc\_s, 399
- atcacert\_cert\_loc\_t
  - Certificate manipulation methods (atcacert\_), 181
- atcacert\_cert\_sn\_src\_e
  - Certificate manipulation methods (atcacert\_), 182
- atcacert\_cert\_sn\_src\_t
  - Certificate manipulation methods (atcacert\_), 181
- atcacert\_cert\_type\_e
  - Certificate manipulation methods (atcacert\_), 183
- atcacert\_cert\_type\_t
  - Certificate manipulation methods (atcacert\_), 181
- atcacert\_check\_config.h, 569
- atcacert\_client.c, 569
- atcacert\_client.h, 570
- atcacert\_create\_csr
  - Certificate manipulation methods (atcacert\_), 185
- cryptoauthlib.atcacert, 328

- atcacert\_create\_csr\_pem
  - Certificate manipulation methods (atcacert\_), 185
  - cryptoauthlib.atcacert, 328
- atcacert\_date.c, 571
- atcacert\_date.h, 572
- atcacert\_date\_cmp
  - Certificate manipulation methods (atcacert\_), 186
- atcacert\_date\_dec
  - Certificate manipulation methods (atcacert\_), 186
  - cryptoauthlib.atcacert, 329
- atcacert\_date\_dec\_compcert
  - Certificate manipulation methods (atcacert\_), 187
  - cryptoauthlib.atcacert, 329
- atcacert\_date\_dec\_compcert\_ext
  - Certificate manipulation methods (atcacert\_), 187
- atcacert\_date\_enc
  - Certificate manipulation methods (atcacert\_), 188
  - cryptoauthlib.atcacert, 330
- atcacert\_date\_enc\_compcert
  - Certificate manipulation methods (atcacert\_), 188
  - cryptoauthlib.atcacert, 330
- atcacert\_date\_enc\_compcert\_ext
  - Certificate manipulation methods (atcacert\_), 188
- atcacert\_date\_from\_asn1\_tag
  - Certificate manipulation methods (atcacert\_), 189
- atcacert\_date\_get\_max\_date
  - Certificate manipulation methods (atcacert\_), 189
  - cryptoauthlib.atcacert, 330
- atcacert\_decode\_pem
  - atcacert\_pem.h, 582
- atcacert\_decode\_pem\_cert
  - atcacert\_pem.h, 582
- atcacert\_decode\_pem\_csr
  - atcacert\_pem.h, 583
- atcacert\_def.c, 574
- atcacert\_def.h, 575
- atcacert\_def\_s, 404
- atcacert\_def\_t
  - Certificate manipulation methods (atcacert\_), 182
- atcacert\_der.c, 577
- atcacert\_der.h, 578
- atcacert\_der\_dec\_ecdsa\_sig\_value
  - Certificate manipulation methods (atcacert\_), 190
- atcacert\_der\_dec\_integer
  - Certificate manipulation methods (atcacert\_), 190
- atcacert\_der\_dec\_length
  - Certificate manipulation methods (atcacert\_), 191
- atcacert\_der\_enc\_ecdsa\_sig\_value
  - Certificate manipulation methods (atcacert\_), 191
- atcacert\_der\_enc\_integer
  - Certificate manipulation methods (atcacert\_), 192
- atcacert\_der\_enc\_length
  - Certificate manipulation methods (atcacert\_), 192
- atcacert\_device\_loc\_s, 405
- atcacert\_device\_loc\_t
  - Certificate manipulation methods (atcacert\_), 182
- atcacert\_device\_zone\_e
  - Certificate manipulation methods (atcacert\_), 183
- atcacert\_device\_zone\_t
  - Certificate manipulation methods (atcacert\_), 182
- ATCACERT\_E\_BAD\_CERT
  - Certificate manipulation methods (atcacert\_), 179
- ATCACERT\_E\_BAD\_PARAMS
  - Certificate manipulation methods (atcacert\_), 179
- ATCACERT\_E\_BUFFER\_TOO\_SMALL
  - Certificate manipulation methods (atcacert\_), 179
- ATCACERT\_E\_DECODING\_ERROR
  - Certificate manipulation methods (atcacert\_), 179
- ATCACERT\_E\_ELEM\_MISSING
  - Certificate manipulation methods (atcacert\_), 180
- ATCACERT\_E\_ELEM\_OUT\_OF\_BOUNDS
  - Certificate manipulation methods (atcacert\_), 180
- ATCACERT\_E\_ERROR
  - Certificate manipulation methods (atcacert\_), 180
- ATCACERT\_E\_INVALID\_DATE
  - Certificate manipulation methods (atcacert\_), 180
- ATCACERT\_E\_INVALID\_TRANSFORM
  - Certificate manipulation methods (atcacert\_), 180
- ATCACERT\_E\_SUCCESS
  - Certificate manipulation methods (atcacert\_), 180
- ATCACERT\_E\_UNEXPECTED\_ELEM\_SIZE
  - Certificate manipulation methods (atcacert\_), 180
- ATCACERT\_E\_UNIMPLEMENTED
  - Certificate manipulation methods (atcacert\_), 180
- ATCACERT\_E\_VERIFY\_FAILED
  - Certificate manipulation methods (atcacert\_), 181
- ATCACERT\_EN
  - atca\_config\_check.h, 542
- atcacert\_encode\_pem
  - atcacert\_pem.h, 583
- atcacert\_encode\_pem\_cert
  - atcacert\_pem.h, 584
- atcacert\_encode\_pem\_csr
  - atcacert\_pem.h, 584
- atcacert\_gen\_challenge\_hw
  - Certificate manipulation methods (atcacert\_), 193
- atcacert\_gen\_challenge\_sw
  - Certificate manipulation methods (atcacert\_), 193
- atcacert\_get\_auth\_key\_id
  - Certificate manipulation methods (atcacert\_), 193
- atcacert\_get\_cert\_sn
  - Certificate manipulation methods (atcacert\_), 194
- atcacert\_get\_expire\_date
  - Certificate manipulation methods (atcacert\_), 194
- atcacert\_get\_issue\_date
  - Certificate manipulation methods (atcacert\_), 195
- atcacert\_get\_issuer
  - Certificate manipulation methods (atcacert\_), 195
- atcacert\_get\_response
  - Certificate manipulation methods (atcacert\_), 196
  - cryptoauthlib.atcacert, 331
- atcacert\_get\_subj\_key\_id
  - Certificate manipulation methods (atcacert\_), 196
- atcacert\_get\_subj\_public\_key
  - Certificate manipulation methods (atcacert\_), 197
- atcacert\_get\_subject

- Certificate manipulation methods (atcacert\_), 197
- atcacert\_host\_hw.c, 579
- atcacert\_host\_hw.h, 579
- atcacert\_host\_sw.c, 580
- atcacert\_host\_sw.h, 580
- atcacert\_max\_cert\_size
  - cryptoauthlib.atcacert, 331
- atcacert\_pem.c, 581
- atcacert\_pem.h, 581
  - atcacert\_decode\_pem, 582
  - atcacert\_decode\_pem\_cert, 582
  - atcacert\_decode\_pem\_csr, 583
  - atcacert\_encode\_pem, 583
  - atcacert\_encode\_pem\_cert, 584
  - atcacert\_encode\_pem\_csr, 584
- atcacert\_read\_cert
  - Certificate manipulation methods (atcacert\_), 198
  - cryptoauthlib.atcacert, 331
- atcacert\_read\_cert\_ext
  - Certificate manipulation methods (atcacert\_), 198
- atcacert\_read\_cert\_size
  - Certificate manipulation methods (atcacert\_), 199
- atcacert\_read\_cert\_size\_ext
  - Certificate manipulation methods (atcacert\_), 199
- atcacert\_read\_device\_loc
  - Certificate manipulation methods (atcacert\_), 200
- atcacert\_read\_device\_loc\_ext
  - Certificate manipulation methods (atcacert\_), 200
- atcacert\_read\_subj\_key\_id
  - Certificate manipulation methods (atcacert\_), 201
- atcacert\_read\_subj\_key\_id\_ext
  - Certificate manipulation methods (atcacert\_), 201
- atcacert\_std\_cert\_element\_e
  - Certificate manipulation methods (atcacert\_), 184
- atcacert\_std\_cert\_element\_t
  - Certificate manipulation methods (atcacert\_), 182
- atcacert\_tm\_utc\_s, 408
- atcacert\_tm\_utc\_t
  - Certificate manipulation methods (atcacert\_), 182
- atcacert\_transform\_e
  - Certificate manipulation methods (atcacert\_), 184
- atcacert\_verify\_cert\_hw
  - Certificate manipulation methods (atcacert\_), 202
- atcacert\_verify\_cert\_sw
  - Certificate manipulation methods (atcacert\_), 202
- atcacert\_verify\_response\_hw
  - Certificate manipulation methods (atcacert\_), 203
- atcacert\_verify\_response\_sw
  - Certificate manipulation methods (atcacert\_), 203
- atcacert\_write\_cert
  - Certificate manipulation methods (atcacert\_), 204
  - cryptoauthlib.atcacert, 332
- atcacert\_write\_cert\_ext
  - Certificate manipulation methods (atcacert\_), 204
- ATCADevice (atca\_), 163
  - atGetIFace, 164
  - deleteATCADevice, 165
  - initATCADevice, 165
  - newATCADevice, 165
  - releaseATCADevice, 166
- ATCAH\_CHECK\_MAC
  - atca\_host\_config\_check.h, 705
- ATCAH\_CONFIG\_TO\_SIGN\_INTERNAL
  - atca\_host\_config\_check.h, 705
- ATCAH\_DECRYPT
  - atca\_host\_config\_check.h, 706
- ATCAH\_DELETE\_MAC
  - atca\_host\_config\_check.h, 706
- ATCAH\_DERIVE\_KEY
  - atca\_host\_config\_check.h, 706
- ATCAH\_DERIVE\_KEY\_MAC
  - atca\_host\_config\_check.h, 706
- ATCAH\_ENCODE\_COUNTER\_MATCH
  - atca\_host\_config\_check.h, 706
- ATCAH\_GEN\_KEY\_MSG
  - atca\_host\_config\_check.h, 707
- ATCAH\_GEN\_MAC
  - atca\_host\_config\_check.h, 707
- ATCAH\_GEN\_OUTPUT\_RESP\_MAC
  - atca\_host\_config\_check.h, 707
- ATCAH\_GEN\_SESSION\_KEY
  - atca\_host\_config\_check.h, 707
- ATCAH\_GENDIG
  - atca\_host\_config\_check.h, 707
- ATCAH\_GENDIVKEY
  - atca\_host\_config\_check.h, 708
- ATCAH\_HMAC
  - atca\_host\_config\_check.h, 708
- ATCAH\_INCLUDE\_DATA
  - atca\_host\_config\_check.h, 708
- ATCAH\_IO\_DECRYPT
  - atca\_host\_config\_check.h, 708
- ATCAH\_MAC
  - atca\_host\_config\_check.h, 708
- ATCAH\_NONCE
  - atca\_host\_config\_check.h, 709
- ATCAH\_PRIVWRITE\_AUTH\_MAC
  - atca\_host\_config\_check.h, 709
- ATCAH\_SECUREBOOT\_ENC
  - atca\_host\_config\_check.h, 709
- ATCAH\_SECUREBOOT\_MAC
  - atca\_host\_config\_check.h, 709
- ATCAH\_SHA256
  - atca\_host\_config\_check.h, 709
- ATCAH\_SIGN\_INTERNAL\_MSG
  - atca\_host\_config\_check.h, 710
- ATCAH\_VERIFY\_MAC
  - atca\_host\_config\_check.h, 710
- ATCAH\_WRITE\_AUTH\_MAC
  - atca\_host\_config\_check.h, 710
- ATCAHAL\_t, 412
- atcal2Cmaster, 412
- ATCAIface (atca\_), 166
  - ATCA\_CUSTOM\_IFACE, 168
  - ATCA\_HID\_IFACE, 168
  - ATCA\_I2C\_GPIO\_IFACE, 168

- ATCA\_I2C\_IFACE, [168](#)
- atca\_iface\_is\_kit, [168](#)
- atca\_iface\_is\_swi, [168](#)
- ATCA\_KIT\_IFACE, [168](#)
- ATCA\_SPI\_GPIO\_IFACE, [168](#)
- ATCA\_SPI\_IFACE, [168](#)
- ATCA\_SWI\_GPIO\_IFACE, [168](#)
- ATCA\_SWI\_IFACE, [168](#)
- ATCA\_UART\_IFACE, [168](#)
- ATCAIfaceType, [168](#)
- atcontrol, [169](#)
- atgetifacecfg, [169](#)
- atgetifacehaldat, [170](#)
- atidle, [170](#)
- atinit, [170](#)
- atreceive, [171](#)
- atsend, [171](#)
- atsleep, [172](#)
- atwake, [172](#)
- deleteATCAIface, [172](#)
- ifacecfg\_set\_address, [173](#)
- ifacetype\_is\_kit, [173](#)
- initATCAIface, [173](#)
- releaseATCAIface, [174](#)
- ATCAIfaceCfg, [413](#)
  - address, [414](#)
- ATCAIfaceType
  - ATCAIface (atca\_), [168](#)
- atCalcCrc
  - calib\_command.c, [593](#)
  - calib\_command.h, [614](#)
- ATCAPacket, [417](#)
- atcaSWImaster, [419](#)
- atCheckCrc
  - calib\_command.c, [594](#)
  - calib\_command.h, [615](#)
- atcontrol
  - ATCAIface (atca\_), [169](#)
- atCRC
  - calib\_command.c, [594](#)
  - calib\_command.h, [615](#)
- atecc508a\_config\_s, [421](#)
- ATECC508A\_DEVICE\_CONFIG
  - test\_device, [354](#)
- ATECC508A\_DEVICE\_CONFIG\_VECTOR
  - test\_device, [354](#)
- atecc608\_config\_s, [423](#)
- ATECC608\_DEVICE\_CONFIG
  - test\_device, [355](#)
- ATECC608\_DEVICE\_CONFIG\_VECTOR
  - test\_device, [355](#)
- atGetIFace
  - ATCADevice (atca\_), [164](#)
- atgetifacecfg
  - ATCAIface (atca\_), [169](#)
- atgetifacehaldat
  - ATCAIface (atca\_), [170](#)
- atidle
  - ATCAIface (atca\_), [170](#)
- atInfo
  - calib\_command.c, [594](#)
  - calib\_command.h, [615](#)
- atinit
  - ATCAIface (atca\_), [170](#)
- atIsECCFamily
  - calib\_command.c, [595](#)
  - calib\_command.h, [616](#)
- atIsSHAFamily
  - calib\_command.c, [595](#)
  - calib\_command.h, [616](#)
- atPause
  - calib\_command.c, [595](#)
  - calib\_command.h, [616](#)
- atreceive
  - ATCAIface (atca\_), [171](#)
- atsend
  - ATCAIface (atca\_), [171](#)
- atsha204a\_config\_s, [425](#)
- ATSHA204A\_DEVICE\_CONFIG
  - test\_device, [355](#)
- ATSHA204A\_DEVICE\_CONFIG\_VECTOR
  - test\_device, [356](#)
- atsleep
  - ATCAIface (atca\_), [172](#)
- attrib\_f
  - pkcs11\_attrib.h, [744](#)
- attributes
  - pkcs11\_object\_s, [466](#)
- Attributes (pkcs11\_attrib\_), [263](#)
  - ec\_key\_data\_table, [273](#)
  - pkcs11\_attrib\_fill, [271](#)
  - pkcs11\_cert\_wtlspublic\_attributes, [273](#)
  - pkcs11\_cert\_x509\_attributes, [274](#)
  - pkcs11\_cert\_x509public\_attributes, [274](#)
  - pkcs11\_deinit, [272](#)
  - pkcs11\_ec\_pbkey\_asn1\_hdr\_p224, [274](#)
  - pkcs11\_ec\_pbkey\_asn1\_hdr\_p256, [274](#)
  - pkcs11\_ec\_pbkey\_asn1\_hdr\_p384, [274](#)
  - pkcs11\_ec\_pbkey\_asn1\_hdr\_p521, [275](#)
  - pkcs11\_init, [272](#)
  - pkcs11\_key\_private\_attributes, [275](#)
  - pkcs11\_key\_public\_attributes, [275](#)
  - pkcs11\_key\_secret\_attributes, [275](#)
  - pkcs11\_object\_monotonic\_attributes, [275](#)
  - pkcs11\_os\_create\_mutex, [272](#)
  - pkcs11\_session\_closeall, [272](#)
  - pkcs11\_session\_login, [273](#)
  - pkcs11\_token\_init, [273](#)
  - pkcs11\_x962\_asn1\_hdr\_ec224, [276](#)
  - pkcs11\_x962\_asn1\_hdr\_ec256, [276](#)
  - pkcs11\_x962\_asn1\_hdr\_ec384, [276](#)
  - pkcs11\_x962\_asn1\_hdr\_ec521, [276](#)
- atwake
  - ATCAIface (atca\_), [172](#)
- Basic Crypto API methods (atcab\_), [80](#)
  - atcab\_aes, [89](#)

atcab\_aes\_decrypt, 89  
atcab\_aes\_decrypt\_ext, 90  
atcab\_aes\_encrypt, 90  
atcab\_aes\_encrypt\_ext, 91  
atcab\_aes\_gcm\_aad\_update, 91  
atcab\_aes\_gcm\_aad\_update\_ext, 92  
atcab\_aes\_gcm\_decrypt\_finish, 92  
atcab\_aes\_gcm\_decrypt\_finish\_ext, 93  
atcab\_aes\_gcm\_decrypt\_update, 93  
atcab\_aes\_gcm\_decrypt\_update\_ext, 94  
atcab\_aes\_gcm\_encrypt\_finish, 94  
atcab\_aes\_gcm\_encrypt\_finish\_ext, 95  
atcab\_aes\_gcm\_encrypt\_update, 95  
atcab\_aes\_gcm\_encrypt\_update\_ext, 96  
atcab\_aes\_gcm\_init, 96  
atcab\_aes\_gcm\_init\_ext, 97  
atcab\_aes\_gcm\_init\_rand, 97  
atcab\_aes\_gfm, 98  
atcab\_base64decode, 98  
atcab\_base64decode\_, 99  
atcab\_base64encode, 99  
atcab\_base64encode\_, 100  
atcab\_bin2hex, 100  
atcab\_bin2hex\_, 101  
atcab\_challenge, 101  
atcab\_challenge\_seed\_update, 102  
atcab\_checkmac, 102  
atcab\_checkmac\_with\_response\_mac, 103  
atcab\_cmp\_config\_zone, 103  
atcab\_counter, 104  
atcab\_counter\_increment, 104  
atcab\_counter\_read, 104  
atcab\_derivekey, 105  
atcab\_derivekey\_ext, 105  
atcab\_ecdh, 106  
atcab\_ecdh\_base, 106  
atcab\_ecdh\_enc, 107  
atcab\_ecdh\_ioenc, 107  
atcab\_ecdh\_tempkey, 108  
atcab\_ecdh\_tempkey\_ioenc, 108  
atcab\_gendig, 108  
atcab\_gendivkey, 109  
atcab\_genkey, 109  
atcab\_genkey\_base, 110  
atcab\_genkey\_ext, 110  
atcab\_get\_device, 111  
atcab\_get\_device\_address, 111  
atcab\_get\_device\_type, 111  
atcab\_get\_device\_type\_ext, 111  
atcab\_get\_pubkey, 112  
atcab\_get\_pubkey\_ext, 112  
atcab\_get\_zone\_size, 113  
atcab\_get\_zone\_size\_ext, 113  
atcab\_hex2bin, 113  
atcab\_hmac, 114  
atcab\_hw\_sha2\_256, 114  
atcab\_hw\_sha2\_256\_finish, 115  
atcab\_hw\_sha2\_256\_init, 115  
atcab\_hw\_sha2\_256\_update, 115  
atcab\_idle, 116  
atcab\_info, 116  
atcab\_info\_base, 116  
atcab\_info\_chip\_status, 117  
atcab\_info\_ext, 117  
atcab\_info\_get\_latch, 118  
atcab\_info\_lock\_status, 118  
atcab\_info\_set\_latch, 118  
atcab\_init, 119  
atcab\_init\_device, 119  
atcab\_init\_ext, 119  
atcab\_is\_ca2\_device, 120  
atcab\_is\_ca\_device, 120  
atcab\_is\_config\_locked, 120  
atcab\_is\_config\_locked\_ext, 121  
atcab\_is\_data\_locked, 121  
atcab\_is\_data\_locked\_ext, 121  
atcab\_is\_locked, 122  
atcab\_is\_private\_ext, 122  
atcab\_is\_slot\_locked, 123  
atcab\_is\_slot\_locked\_ext, 123  
atcab\_is\_ta\_device, 124  
atcab\_kdf, 124  
atcab\_lock, 124  
atcab\_lock\_config\_zone, 125  
atcab\_lock\_config\_zone\_crc, 125  
atcab\_lock\_config\_zone\_ext, 126  
atcab\_lock\_data\_slot, 126  
atcab\_lock\_data\_slot\_ext, 126  
atcab\_lock\_data\_zone, 127  
atcab\_lock\_data\_zone\_crc, 127  
atcab\_lock\_data\_zone\_ext, 127  
atcab\_mac, 128  
atcab\_nonce, 128  
atcab\_nonce\_base, 129  
atcab\_nonce\_load, 129  
atcab\_nonce\_rand, 130  
atcab\_nonce\_rand\_ext, 130  
atcab\_priv\_write, 131  
atcab\_random, 131  
atcab\_random\_ext, 131  
atcab\_read\_bytes\_zone, 132  
atcab\_read\_config\_zone, 132  
atcab\_read\_config\_zone\_ext, 133  
atcab\_read\_enc, 133  
atcab\_read\_pubkey, 134  
atcab\_read\_pubkey\_ext, 134  
atcab\_read\_serial\_number, 135  
atcab\_read\_serial\_number\_ext, 135  
atcab\_read\_sig, 135  
atcab\_read\_zone, 136  
atcab\_read\_zone\_ext, 136  
atcab\_release, 137  
atcab\_release\_ext, 137  
atcab\_reversal, 137  
atcab\_secureboot, 138  
atcab\_secureboot\_mac, 138

- atcab\_selftest, 139
- atcab\_sha, 139
- atcab\_sha\_base, 140
- atcab\_sha\_end, 141
- atcab\_sha\_hmac, 141
- atcab\_sha\_hmac\_ext, 141
- atcab\_sha\_hmac\_finish, 142
- atcab\_sha\_hmac\_init, 143
- atcab\_sha\_hmac\_update, 143
- atcab\_sha\_read\_context, 143
- atcab\_sha\_start, 144
- atcab\_sha\_update, 144
- atcab\_sha\_write\_context, 144
- atcab\_sign, 145
- atcab\_sign\_base, 145
- atcab\_sign\_ext, 146
- atcab\_sign\_internal, 146
- atcab\_sleep, 147
- atcab\_updateextra, 147
- atcab\_verify, 147
- atcab\_verify\_extern, 148
- atcab\_verify\_extern\_ext, 149
- atcab\_verify\_extern\_mac, 149
- atcab\_verify\_invalidate, 150
- atcab\_verify\_stored, 150
- atcab\_verify\_stored\_ext, 151
- atcab\_verify\_stored\_mac, 151
- atcab\_verify\_stored\_with\_tempkey, 152
- atcab\_verify\_validate, 152
- atcab\_version, 153
- atcab\_wakeup, 153
- atcab\_write, 153
- atcab\_write\_bytes\_zone, 154
- atcab\_write\_config\_counter, 155
- atcab\_write\_config\_zone, 155
- atcab\_write\_config\_zone\_ext, 155
- atcab\_write\_enc, 156
- atcab\_write\_pubkey, 156
- atcab\_write\_pubkey\_ext, 157
- atcab\_write\_zone, 157
- atcab\_write\_zone\_ext, 159
- isAlpha, 159
- isBase64, 160
- isBase64Digit, 160
- isBlankSpace, 160
- isDigit, 161
- isHex, 161
- isHexAlpha, 162
- isHexDigit, 162
- packHex, 162
- Basic Crypto API methods for CryptoAuth Devices
  - (calib\_), 205
  - calib\_ca2\_get\_addr, 209
  - calib\_ca2\_is\_config\_locked, 209
  - calib\_ca2\_is\_data\_locked, 210
  - calib\_ca2\_is\_locked, 210
  - calib\_exit, 211
  - calib\_get\_addr, 211
  - calib\_get\_zone\_size, 212
  - calib\_idle, 212
  - calib\_info, 212
  - calib\_info\_base, 213
  - calib\_info\_chip\_status, 213
  - calib\_info\_lock\_status, 214
  - calib\_info\_privkey\_valid, 214
  - calib\_sleep, 214
  - calib\_wakeup, 215
  - calib\_wakeup\_i2c, 215
  - bind\_host\_and\_secure\_element\_with\_io\_protection
    - secure\_boot.c, 499
    - secure\_boot.h, 501
  - BIT\_DELAY\_1L
    - hal\_swi\_gpio.h, 682
  - BIT\_DELAY\_5
    - hal\_swi\_gpio.h, 682
  - BIT\_DELAY\_7
    - hal\_swi\_gpio.h, 682
  - buf
    - cal\_buffer\_s, 428
  - cal\_buf\_read\_bytes
    - cal\_buffer.c, 586
    - cal\_buffer.h, 588
  - cal\_buf\_read\_number
    - cal\_buffer.c, 586
    - cal\_buffer.h, 589
  - cal\_buf\_write\_bytes
    - cal\_buffer.c, 586
    - cal\_buffer.h, 589
  - cal\_buf\_write\_number
    - cal\_buffer.c, 587
    - cal\_buffer.h, 589
  - cal\_buffer.c, 585
    - cal\_buf\_read\_bytes, 586
    - cal\_buf\_read\_number, 586
    - cal\_buf\_write\_bytes, 586
    - cal\_buf\_write\_number, 587
  - cal\_buffer.h, 587
    - cal\_buf\_read\_bytes, 588
    - cal\_buf\_read\_number, 589
    - cal\_buf\_write\_bytes, 589
    - cal\_buf\_write\_number, 589
  - cal\_buffer\_s, 428
    - buf, 428
    - len, 428
  - cal\_internal.h, 590
  - calib\_aes.c, 590
  - calib\_aes\_gcm.c, 591
  - calib\_aes\_gcm.h, 591
  - calib\_basic.c, 591
  - calib\_ca2\_get\_addr
    - Basic Crypto API methods for CryptoAuth Devices
      - (calib\_), 209
  - calib\_ca2\_is\_config\_locked
    - Basic Crypto API methods for CryptoAuth Devices
      - (calib\_), 209
  - calib\_ca2\_is\_data\_locked



- Basic Crypto API methods for CryptoAuth Devices (calib\_), 210
- calib\_ca2\_is\_locked
  - Basic Crypto API methods for CryptoAuth Devices (calib\_), 210
- calib\_checkmac.c, 592
- calib\_command.c, 593
  - atCalcCrc, 593
  - atCheckCrc, 594
  - atCRC, 594
  - atInfo, 594
  - atIsECCFamily, 595
  - atIsSHAFamily, 595
  - atPause, 595
  - isATCAError, 596
- calib\_command.h, 596
  - atCalcCrc, 614
  - atCheckCrc, 615
  - atCRC, 615
  - atInfo, 615
  - atIsECCFamily, 616
  - atIsSHAFamily, 616
  - atPause, 616
  - isATCAError, 617
- calib\_config\_check.h, 617
  - CALIB\_INFO\_LATCH\_EN, 619
  - CALIB\_LOCK\_CA2\_EN, 619
  - CALIB\_LOCK\_EN, 619
  - CALIB\_READ\_EN, 619
  - CALIB\_SHA\_CONTEXT\_EN, 620
  - CALIB\_SHA\_EN, 620
  - CALIB\_SHA\_HMAC\_EN, 620
  - CALIB\_SIGN\_CA2\_EN, 620
  - CALIB\_SIGN\_EN, 620
  - CALIB\_UPDATEEXTRA\_EN, 620
  - CALIB\_VERIFY\_EN, 621
  - CALIB\_VERIFY\_MAC\_EN, 621
  - CALIB\_VERIFY\_STORED\_EN, 621
  - CALIB\_WRITE\_ENC\_EN, 621
- calib\_counter.c, 622
- calib\_delete.c, 622
- calib\_derivekey.c, 623
- calib\_device.h, 623
- calib\_ecdh.c, 626
- calib\_execute\_command
  - calib\_execution.c, 627
  - calib\_execution.h, 629
- calib\_execution.c, 627
  - calib\_execute\_command, 627
  - calib\_get\_execution\_time, 628
- calib\_execution.h, 628
  - calib\_execute\_command, 629
  - calib\_get\_execution\_time, 630
- calib\_exit
  - Basic Crypto API methods for CryptoAuth Devices (calib\_), 211
- calib\_gendig.c, 630
- calib\_genkey.c, 631
- calib\_get\_addr
  - Basic Crypto API methods for CryptoAuth Devices (calib\_), 211
- calib\_get\_execution\_time
  - calib\_execution.c, 628
  - calib\_execution.h, 630
- calib\_get\_zone\_size
  - Basic Crypto API methods for CryptoAuth Devices (calib\_), 212
- calib\_helpers.c, 631
- calib\_hmac.c, 632
- calib\_idle
  - Basic Crypto API methods for CryptoAuth Devices (calib\_), 212
- calib\_info
  - Basic Crypto API methods for CryptoAuth Devices (calib\_), 212
- calib\_info.c, 632
- calib\_info\_base
  - Basic Crypto API methods for CryptoAuth Devices (calib\_), 213
- calib\_info\_chip\_status
  - Basic Crypto API methods for CryptoAuth Devices (calib\_), 213
- CALIB\_INFO\_LATCH\_EN
  - calib\_config\_check.h, 619
- calib\_info\_lock\_status
  - Basic Crypto API methods for CryptoAuth Devices (calib\_), 214
- calib\_info\_privkey\_valid
  - Basic Crypto API methods for CryptoAuth Devices (calib\_), 214
- calib\_kdf.c, 633
- calib\_lock.c, 633
- CALIB\_LOCK\_CA2\_EN
  - calib\_config\_check.h, 619
- CALIB\_LOCK\_EN
  - calib\_config\_check.h, 619
- calib\_mac.c, 634
- calib\_nonce.c, 634
- calib\_privwrite.c, 635
- calib\_random.c, 635
- calib\_read.c, 636
- CALIB\_READ\_EN
  - calib\_config\_check.h, 619
- calib\_secureboot.c, 636
- calib\_selftest.c, 637
- calib\_sha.c, 637
- CALIB\_SHA\_CONTEXT\_EN
  - calib\_config\_check.h, 620
- CALIB\_SHA\_EN
  - calib\_config\_check.h, 620
- CALIB\_SHA\_HMAC\_EN
  - calib\_config\_check.h, 620
- calib\_sign.c, 638
- CALIB\_SIGN\_CA2\_EN
  - calib\_config\_check.h, 620
- CALIB\_SIGN\_EN

- calib\_config\_check.h, 620
- calib\_sleep
  - Basic Crypto API methods for CryptoAuth Devices (calib\_), 214
- calib\_updateextra.c, 638
- CALIB\_UPDATEEXTRA\_EN
  - calib\_config\_check.h, 620
- calib\_verify.c, 639
- CALIB\_VERIFY\_EN
  - calib\_config\_check.h, 621
- CALIB\_VERIFY\_MAC\_EN
  - calib\_config\_check.h, 621
- CALIB\_VERIFY\_STORED\_EN
  - calib\_config\_check.h, 621
- calib\_wakeup
  - Basic Crypto API methods for CryptoAuth Devices (calib\_), 215
- calib\_wakeup\_i2c
  - Basic Crypto API methods for CryptoAuth Devices (calib\_), 215
- calib\_write.c, 639
- CALIB\_WRITE\_ENC\_EN
  - calib\_config\_check.h, 621
- Certificate manipulation methods (atcacert\_), 174
  - atcacert\_build\_state\_t, 181
  - atcacert\_calc\_expire\_years, 184
  - atcacert\_cert\_element\_t, 181
  - atcacert\_cert\_loc\_t, 181
  - atcacert\_cert\_sn\_src\_e, 182
  - atcacert\_cert\_sn\_src\_t, 181
  - atcacert\_cert\_type\_e, 183
  - atcacert\_cert\_type\_t, 181
  - atcacert\_create\_csr, 185
  - atcacert\_create\_csr\_pem, 185
  - atcacert\_date\_cmp, 186
  - atcacert\_date\_dec, 186
  - atcacert\_date\_dec\_compcert, 187
  - atcacert\_date\_dec\_compcert\_ext, 187
  - atcacert\_date\_enc, 188
  - atcacert\_date\_enc\_compcert, 188
  - atcacert\_date\_enc\_compcert\_ext, 188
  - atcacert\_date\_from\_asn1\_tag, 189
  - atcacert\_date\_get\_max\_date, 189
  - atcacert\_def\_t, 182
  - atcacert\_der\_dec\_ecdsa\_sig\_value, 190
  - atcacert\_der\_dec\_integer, 190
  - atcacert\_der\_dec\_length, 191
  - atcacert\_der\_enc\_ecdsa\_sig\_value, 191
  - atcacert\_der\_enc\_integer, 192
  - atcacert\_der\_enc\_length, 192
  - atcacert\_device\_loc\_t, 182
  - atcacert\_device\_zone\_e, 183
  - atcacert\_device\_zone\_t, 182
  - ATCACERT\_E\_BAD\_CERT, 179
  - ATCACERT\_E\_BAD\_PARAMS, 179
  - ATCACERT\_E\_BUFFER\_TOO\_SMALL, 179
  - ATCACERT\_E\_DECODING\_ERROR, 179
  - ATCACERT\_E\_ELEM\_MISSING, 180
  - ATCACERT\_E\_ELEM\_OUT\_OF\_BOUNDS, 180
  - ATCACERT\_E\_ERROR, 180
  - ATCACERT\_E\_INVALID\_DATE, 180
  - ATCACERT\_E\_INVALID\_TRANSFORM, 180
  - ATCACERT\_E\_SUCCESS, 180
  - ATCACERT\_E\_UNEXPECTED\_ELEM\_SIZE, 180
  - ATCACERT\_E\_UNIMPLEMENTED, 180
  - ATCACERT\_E\_VERIFY\_FAILED, 181
  - atcacert\_gen\_challenge\_hw, 193
  - atcacert\_gen\_challenge\_sw, 193
  - atcacert\_get\_auth\_key\_id, 193
  - atcacert\_get\_cert\_sn, 194
  - atcacert\_get\_expire\_date, 194
  - atcacert\_get\_issue\_date, 195
  - atcacert\_get\_issuer, 195
  - atcacert\_get\_response, 196
  - atcacert\_get\_subj\_key\_id, 196
  - atcacert\_get\_subj\_public\_key, 197
  - atcacert\_get\_subject, 197
  - atcacert\_read\_cert, 198
  - atcacert\_read\_cert\_ext, 198
  - atcacert\_read\_cert\_size, 199
  - atcacert\_read\_cert\_size\_ext, 199
  - atcacert\_read\_device\_loc, 200
  - atcacert\_read\_device\_loc\_ext, 200
  - atcacert\_read\_subj\_key\_id, 201
  - atcacert\_read\_subj\_key\_id\_ext, 201
  - atcacert\_std\_cert\_element\_e, 184
  - atcacert\_std\_cert\_element\_t, 182
  - atcacert\_tm\_utc\_t, 182
  - atcacert\_transform\_e, 184
  - atcacert\_verify\_cert\_hw, 202
  - atcacert\_verify\_cert\_sw, 202
  - atcacert\_verify\_response\_hw, 203
  - atcacert\_verify\_response\_sw, 203
  - atcacert\_write\_cert, 204
  - atcacert\_write\_cert\_ext, 204
  - CERTTYPE\_CUSTOM, 183
  - CERTTYPE\_X509, 183
  - CERTTYPE\_X509\_FULL\_STORED, 183
  - DATEFMT\_ISO8601\_SEP, 181
  - DEVZONE\_CONFIG, 183
  - DEVZONE\_DATA, 183
  - DEVZONE\_GENKEY, 183
  - DEVZONE\_NONE, 183
  - DEVZONE\_OTP, 183
  - SNSRC\_DEVICE\_SN, 183
  - SNSRC\_DEVICE\_SN\_HASH, 183
  - SNSRC\_DEVICE\_SN\_HASH\_POS, 183
  - SNSRC\_DEVICE\_SN\_HASH\_RAW, 183
  - SNSRC\_PUB\_KEY\_HASH, 183
  - SNSRC\_PUB\_KEY\_HASH\_POS, 183
  - SNSRC\_PUB\_KEY\_HASH\_RAW, 183
  - SNSRC\_SIGNER\_ID, 183
  - SNSRC\_STORED, 183
  - SNSRC\_STORED\_DYNAMIC, 183
  - STDCERT\_NUM\_ELEMENTS, 184
  - TF\_BIN2HEX\_LC, 184



- TF\_BIN2HEX\_SPACE\_LC, [184](#)
- TF\_BIN2HEX\_SPACE\_UC, [184](#)
- TF\_BIN2HEX\_UC, [184](#)
- TF\_HEX2BIN\_LC, [184](#)
- TF\_HEX2BIN\_SPACE\_LC, [184](#)
- TF\_HEX2BIN\_SPACE\_UC, [184](#)
- TF\_HEX2BIN\_UC, [184](#)
- TF\_NONE, [184](#)
- TF\_REVERSE, [184](#)
- CERTTYPE\_CUSTOM
  - Certificate manipulation methods (atcacert\_), [183](#)
- CERTTYPE\_X509
  - Certificate manipulation methods (atcacert\_), [183](#)
- CERTTYPE\_X509\_FULL\_STORED
  - Certificate manipulation methods (atcacert\_), [183](#)
- cfg\_ateccx08a\_i2c\_default
  - cryptoauthlib.iface, [335](#)
- cfg\_ateccx08a\_kithid\_default
  - cryptoauthlib.iface, [336](#)
- cfg\_ateccx08a\_swi\_default
  - cryptoauthlib.iface, [336](#)
- cfg\_atsha20xa\_i2c\_default
  - cryptoauthlib.iface, [336](#)
- cfg\_atsha20xa\_kithid\_default
  - cryptoauthlib.iface, [336](#)
- cfg\_atsha20xa\_swi\_default
  - cryptoauthlib.iface, [336](#)
- change\_i2c\_speed
  - Hardware abstraction layer (hal\_), [225](#)
- check\_rationality
  - cryptoauthlib.library.AtcaStructure, [419](#)
  - cryptoauthlib.library.AtcaUnion, [420](#)
- check\_status
  - cryptoauthlib.status, [349](#)
- CK\_AES\_CBC\_ENCRYPT\_DATA\_PARAMS, [432](#)
- CK\_AES\_CCM\_PARAMS, [432](#)
- CK\_AES\_CTR\_PARAMS, [432](#)
- CK\_AES\_GCM\_PARAMS, [433](#)
- CK\_ARIA\_CBC\_ENCRYPT\_DATA\_PARAMS, [433](#)
- CK\_ATTRIBUTE, [433](#)
- CK\_C\_INITIALIZE\_ARGS, [433](#)
- CK\_CAMELLIA\_CBC\_ENCRYPT\_DATA\_PARAMS, [433](#)
- CK\_CAMELLIA\_CTR\_PARAMS, [434](#)
- CK\_CCM\_PARAMS, [434](#)
- CK\_CMS\_SIG\_PARAMS, [434](#)
- CK\_DATE, [434](#)
- CK\_DES\_CBC\_ENCRYPT\_DATA\_PARAMS, [434](#)
- CK\_DSA\_PARAMETER\_GEN\_PARAM, [435](#)
- CK\_ECDH1\_DERIVE\_PARAMS, [435](#)
- CK\_ECDH2\_DERIVE\_PARAMS, [435](#)
- CK\_ECDH\_AES\_KEY\_WRAP\_PARAMS, [435](#)
- CK\_ECMQV\_DERIVE\_PARAMS, [436](#)
- CK\_FUNCTION\_LIST, [436](#)
- CK\_GCM\_PARAMS, [436](#)
- CK\_GOSTR3410\_DERIVE\_PARAMS, [436](#)
- CK\_GOSTR3410\_KEY\_WRAP\_PARAMS, [437](#)
- CK\_INFO, [437](#)
- CK\_KEA\_DERIVE\_PARAMS, [437](#)
- CK\_KEY\_DERIVATION\_STRING\_DATA, [437](#)
- CK\_KEY\_WRAP\_SET\_OAEP\_PARAMS, [437](#)
- CK\_KIP\_PARAMS, [438](#)
- CK\_MECHANISM, [438](#)
- CK\_MECHANISM\_INFO, [438](#)
- CK\_OTP\_PARAM, [438](#)
- CK\_OTP\_PARAMS, [438](#)
- CK\_OTP\_SIGNATURE\_INFO, [439](#)
- CK\_PBE\_PARAMS, [439](#)
- CK\_PKCS5\_PBKD2\_PARAMS, [439](#)
- CK\_PKCS5\_PBKD2\_PARAMS2, [439](#)
- CK\_RC2\_CBC\_PARAMS, [440](#)
- CK\_RC2\_MAC\_GENERAL\_PARAMS, [440](#)
- CK\_RC5\_CBC\_PARAMS, [440](#)
- CK\_RC5\_MAC\_GENERAL\_PARAMS, [440](#)
- CK\_RC5\_PARAMS, [440](#)
- CK\_RSA\_AES\_KEY\_WRAP\_PARAMS, [440](#)
- CK\_RSA\_PKCS\_OAEP\_PARAMS, [441](#)
- CK\_RSA\_PKCS\_PSS\_PARAMS, [441](#)
- CK\_SEED\_CBC\_ENCRYPT\_DATA\_PARAMS, [441](#)
- CK\_SESSION\_INFO, [441](#)
- CK\_SKIPJACK\_PRIVATE\_WRAP\_PARAMS, [441](#)
- CK\_SKIPJACK\_RELAYX\_PARAMS, [442](#)
- CK\_SLOT\_INFO, [442](#)
- CK\_SSL3\_KEY\_MAT\_OUT, [442](#)
- CK\_SSL3\_KEY\_MAT\_PARAMS, [442](#)
- CK\_SSL3\_MASTER\_KEY\_DERIVE\_PARAMS, [443](#)
- CK\_SSL3\_RANDOM\_DATA, [443](#)
- CK\_TLS12\_KEY\_MAT\_PARAMS, [443](#)
- CK\_TLS12\_MASTER\_KEY\_DERIVE\_PARAMS, [443](#)
- CK\_TLS\_KDF\_PARAMS, [443](#)
- CK\_TLS\_MAC\_PARAMS, [444](#)
- CK\_TLS\_PRF\_PARAMS, [444](#)
- CK\_TOKEN\_INFO, [444](#)
- CK\_VERSION, [444](#)
- CK\_WTLS\_KEY\_MAT\_OUT, [445](#)
- CK\_WTLS\_KEY\_MAT\_PARAMS, [445](#)
- CK\_WTLS\_MASTER\_KEY\_DERIVE\_PARAMS, [445](#)
- CK\_WTLS\_PRF\_PARAMS, [445](#)
- CK\_WTLS\_RANDOM\_DATA, [445](#)
- CK\_X9\_42\_DH1\_DERIVE\_PARAMS, [446](#)
- CK\_X9\_42\_DH2\_DERIVE\_PARAMS, [446](#)
- CK\_X9\_42\_MQV\_DERIVE\_PARAMS, [446](#)
- CL\_HashContext, [446](#)
- class\_id
  - pkcs11\_object\_s, [466](#)
- class\_type
  - pkcs11\_object\_s, [466](#)
- config\_path
  - pkcs11\_lib\_ctx\_s, [464](#)
- Configuration (cfg\_), [163](#)
- count
  - pkcs11\_object\_s, [466](#)
- crypto\_hw\_config\_check.h, [646](#)
  - ATCAB\_AES\_CBC\_DECRYPT\_EN, [647](#)
  - ATCAB\_AES\_CBC\_ENCRYPT\_EN, [647](#)
  - ATCAB\_AES\_CBCMAC\_EN, [647](#)
  - ATCAB\_AES\_CCM\_EN, [647](#)

- ATCAB\_AES\_CTR\_EN, 648
- ATCAB\_AES\_CTR RAND\_IV\_EN, 648
- ATCAB\_AES\_EXTRAS\_EN, 648
- ATCAB\_AES\_UPDATE\_EN, 648
- crypto\_sw\_config\_check.h, 648
- ATCA\_CRYPT\_SHA1\_EN, 649
- ATCA\_CRYPT\_SHA2\_HMAC\_CTR\_EN, 649
- ATCA\_CRYPT\_SHA2\_HMAC\_EN, 649
- ATCAB\_PBKDF2\_SHA256\_EN, 650
- ATCAC\_AES\_GCM\_EN, 650
- ATCAC\_PBKDF2\_SHA256\_EN, 650
- ATCAC\_RANDOM\_EN, 650
- ATCAC\_SHA1\_EN, 650
- ATCAC\_SHA256\_EN, 651
- ATCAC\_SIGN\_EN, 651
- ATCAC\_VERIFY\_EN, 651
- cryptoauthlib, 277
- cryptoauthlib.atcab, 277
  - atcab\_aes, 280
  - atcab\_aes\_cbc\_decrypt\_block, 280
  - atcab\_aes\_cbc\_encrypt\_block, 281
  - atcab\_aes\_cbc\_init, 281
  - atcab\_aes\_ccmac\_finish, 282
  - atcab\_aes\_ccmac\_init, 282
  - atcab\_aes\_ccmac\_update, 282
  - atcab\_aes\_ccm\_aad\_finish, 283
  - atcab\_aes\_ccm\_aad\_update, 283
  - atcab\_aes\_ccm\_decrypt\_finish, 283
  - atcab\_aes\_ccm\_decrypt\_update, 284
  - atcab\_aes\_ccm\_encrypt\_finish, 284
  - atcab\_aes\_ccm\_encrypt\_update, 284
  - atcab\_aes\_ccm\_init, 285
  - atcab\_aes\_ccm\_init\_rand, 285
  - atcab\_aes\_cmac\_finish, 286
  - atcab\_aes\_cmac\_init, 286
  - atcab\_aes\_cmac\_update, 286
  - atcab\_aes\_ctr\_decrypt\_block, 287
  - atcab\_aes\_ctr\_encrypt\_block, 287
  - atcab\_aes\_ctr\_init, 287
  - atcab\_aes\_ctr\_init\_rand, 288
  - atcab\_aes\_decrypt, 288
  - atcab\_aes\_encrypt, 289
  - atcab\_aes\_gcm\_aad\_update, 289
  - atcab\_aes\_gcm\_decrypt\_finish, 290
  - atcab\_aes\_gcm\_decrypt\_update, 290
  - atcab\_aes\_gcm\_encrypt\_finish, 290
  - atcab\_aes\_gcm\_encrypt\_update, 291
  - atcab\_aes\_gcm\_init, 291
  - atcab\_aes\_gcm\_init\_rand, 291
  - atcab\_aes\_gfm, 292
  - atcab\_challenge, 292
  - atcab\_challenge\_seed\_update, 293
  - atcab\_checkmac, 293
  - atcab\_cmp\_config\_zone, 293
  - atcab\_counter, 294
  - atcab\_counter\_increment, 294
  - atcab\_counter\_read, 294
  - atcab\_derivekey, 295
  - atcab\_ecdh, 295
  - atcab\_ecdh\_base, 295
  - atcab\_ecdh\_enc, 296
  - atcab\_ecdh\_ioenc, 296
  - atcab\_ecdh\_tempkey, 297
  - atcab\_ecdh\_tempkey\_ioenc, 297
  - atcab\_gendig, 298
  - atcab\_genkey, 298
  - atcab\_genkey\_base, 298
  - atcab\_get\_device, 299
  - atcab\_get\_device\_type, 299
  - atcab\_get\_pubkey, 299
  - atcab\_hmac, 300
  - atcab\_hw\_sha2\_256, 300
  - atcab\_hw\_sha2\_256\_finish, 300
  - atcab\_hw\_sha2\_256\_init, 301
  - atcab\_hw\_sha2\_256\_update, 301
  - atcab\_info, 301
  - atcab\_info\_base, 302
  - atcab\_info\_get\_latch, 302
  - atcab\_info\_set\_latch, 302
  - atcab\_init, 303
  - atcab\_is\_locked, 303
  - atcab\_is\_slot\_locked, 303
  - atcab\_kdf, 304
  - atcab\_lock, 304
  - atcab\_lock\_config\_zone, 305
  - atcab\_lock\_config\_zone\_crc, 305
  - atcab\_lock\_data\_slot, 305
  - atcab\_lock\_data\_zone, 306
  - atcab\_lock\_data\_zone\_crc, 306
  - atcab\_mac, 306
  - atcab\_nonce, 307
  - atcab\_nonce\_base, 307
  - atcab\_nonce\_load, 308
  - atcab\_nonce\_rand, 308
  - atcab\_priv\_write, 309
  - atcab\_random, 309
  - atcab\_read\_bytes\_zone, 309
  - atcab\_read\_config\_zone, 310
  - atcab\_read\_enc, 310
  - atcab\_read\_pubkey, 311
  - atcab\_read\_serial\_number, 311
  - atcab\_read\_sig, 311
  - atcab\_read\_zone, 312
  - atcab\_release, 312
  - atcab\_secureboot, 312
  - atcab\_secureboot\_mac, 313
  - atcab\_selftest, 313
  - atcab\_sha, 314
  - atcab\_sha\_base, 314
  - atcab\_sha\_end, 315
  - atcab\_sha\_hmac, 315
  - atcab\_sha\_hmac\_finish, 316
  - atcab\_sha\_hmac\_init, 316
  - atcab\_sha\_hmac\_update, 316
  - atcab\_sha\_read\_context, 317
  - atcab\_sha\_start, 317

- atcab\_sha\_update, 317
- atcab\_sha\_write\_context, 318
- atcab\_sign, 318
- atcab\_sign\_base, 318
- atcab\_sign\_internal, 319
- atcab\_updateextra, 319
- atcab\_verify, 319
- atcab\_verify\_extern, 320
- atcab\_verify\_extern\_mac, 321
- atcab\_verify\_extern\_stored\_mac, 321
- atcab\_verify\_invalidate, 322
- atcab\_verify\_stored, 322
- atcab\_verify\_stored\_mac, 323
- atcab\_verify\_validate, 323
- atcab\_write, 324
- atcab\_write\_bytes\_zone, 324
- atcab\_write\_config\_counter, 325
- atcab\_write\_config\_zone, 325
- atcab\_write\_enc, 325
- atcab\_write\_pubkey, 326
- atcab\_write\_zone, 326
- cryptoauthlib.atcab.atca\_aes\_cbc\_ctx, 369
  - \_fields\_, 369
- cryptoauthlib.atcab.atca\_aes\_cbcmac\_ctx, 369
  - \_fields\_, 370
- cryptoauthlib.atcab.atca\_aes\_ccm\_ctx, 370
  - \_fields\_, 370
- cryptoauthlib.atcab.atca\_aes\_cmac\_ctx, 371
  - \_fields\_, 371
- cryptoauthlib.atcab.atca\_aes\_ctr\_ctx, 372
  - \_fields\_, 372
- cryptoauthlib.atcab.atca\_aes\_gcm\_ctx, 372
  - \_fields\_, 373
- cryptoauthlib.atcab.atca\_hmac\_sha256\_ctx, 381
- cryptoauthlib.atcab.atca\_sha256\_ctx, 387
  - \_fields\_, 388
- cryptoauthlib.atcacert, 327
  - \_atcacert\_convert\_bytes, 328
  - \_atcacert\_convert\_enum, 328
  - atcacert\_create\_csr, 328
  - atcacert\_create\_csr\_pem, 328
  - atcacert\_date\_dec, 329
  - atcacert\_date\_dec\_compcert, 329
  - atcacert\_date\_enc, 330
  - atcacert\_date\_enc\_compcert, 330
  - atcacert\_date\_get\_max\_date, 330
  - atcacert\_get\_response, 331
  - atcacert\_max\_cert\_size, 331
  - atcacert\_read\_cert, 331
  - atcacert\_write\_cert, 332
- cryptoauthlib.atcacert.atcacert\_cert\_element\_t, 398
  - \_def\_, 399
- cryptoauthlib.atcacert.atcacert\_cert\_loc\_t, 399
- cryptoauthlib.atcacert.atcacert\_cert\_sn\_src\_t, 400
- cryptoauthlib.atcacert.atcacert\_cert\_type\_t, 401
- cryptoauthlib.atcacert.atcacert\_comp\_data\_t, 402
  - \_fields\_, 403
- cryptoauthlib.atcacert.atcacert\_date\_format\_t, 403
- cryptoauthlib.atcacert.atcacert\_def\_t, 404
- cryptoauthlib.atcacert.atcacert\_device\_loc\_t, 405
  - \_def\_, 406
- cryptoauthlib.atcacert.atcacert\_device\_zone\_t, 406
- cryptoauthlib.atcacert.atcacert\_std\_cert\_element\_t, 407
- cryptoauthlib.atcacert.atcacert\_tm\_utc\_t, 408
  - \_fields\_, 409
- cryptoauthlib.atcacert.atcacert\_transform\_t, 409
- cryptoauthlib.atcacert.CertStatus, 429
- cryptoauthlib.atcaenum, 332
- cryptoauthlib.atcaenum.AtcaEnum, 411
- cryptoauthlib.atjwt, 333
- cryptoauthlib.atjwt.HwEcAlgorithm, 453
  - sign, 454
- cryptoauthlib.atjwt.HwHmacAlgorithm, 454
  - sign, 454
  - verify, 455
- cryptoauthlib.atjwt.PyJWT, 468
- cryptoauthlib.device, 333
- cryptoauthlib.device.AesEnable, 368
  - \_fields\_, 368
- cryptoauthlib.device.Atecc508aConfig, 422
  - \_fields\_, 422
- cryptoauthlib.device.Atecc608Config, 424
  - \_fields\_, 424
- cryptoauthlib.device.Atsha204aConfig, 426
  - \_fields\_, 426
- cryptoauthlib.device.ChipMode508, 430
  - \_fields\_, 430
- cryptoauthlib.device.ChipMode608, 431
  - \_fields\_, 431
- cryptoauthlib.device.ChipOptions, 431
  - \_fields\_, 432
- cryptoauthlib.device.Counter204, 447
  - \_fields\_, 448
- cryptoauthlib.device.CountMatch, 448
  - \_fields\_, 448
- cryptoauthlib.device.I2cEnable, 456
  - \_fields\_, 456
- cryptoauthlib.device.KeyConfig, 457
  - \_fields\_, 457
- cryptoauthlib.device.SecureBoot, 470
  - \_fields\_, 470
- cryptoauthlib.device.SlotConfig, 471
  - \_fields\_, 471
- cryptoauthlib.device.UseLock, 475
  - \_fields\_, 476
- cryptoauthlib.device.VolatileKeyPermission, 476
  - \_fields\_, 476
- cryptoauthlib.device.X509Format, 477
  - \_fields\_, 477
- cryptoauthlib.exceptions, 334
- cryptoauthlib.exceptions.AssertionFailure, 368
- cryptoauthlib.exceptions.BadArgumentError, 427
- cryptoauthlib.exceptions.BadCrcError, 427
- cryptoauthlib.exceptions.BadOpcodeError, 427
- cryptoauthlib.exceptions.CheckmacVerifyFailedError, 430

- cryptoauthlib.exceptions.CommunicationError, [447](#)
- cryptoauthlib.exceptions.ConfigZoneLockedError, [447](#)
- cryptoauthlib.exceptions.CrcError, [449](#)
- cryptoauthlib.exceptions.CryptoError, [450](#)
- cryptoauthlib.exceptions.DataZoneLockedError, [450](#)
- cryptoauthlib.exceptions.EccFaultError, [451](#)
- cryptoauthlib.exceptions.ExecutionError, [452](#)
- cryptoauthlib.exceptions.FunctionError, [452](#)
- cryptoauthlib.exceptions.GenericError, [452](#)
- cryptoauthlib.exceptions.HealthTestError, [453](#)
- cryptoauthlib.exceptions.InvalidIdentifierError, [456](#)
- cryptoauthlib.exceptions.InvalidSizeError, [457](#)
- cryptoauthlib.exceptions.LibraryLoadError, [458](#)
- cryptoauthlib.exceptions.LibraryMemoryError, [458](#)
- cryptoauthlib.exceptions.LibraryNotInitialized, [459](#)
- cryptoauthlib.exceptions.NoDevicesFoundError, [459](#)
- cryptoauthlib.exceptions.NoResponseError, [460](#)
- cryptoauthlib.exceptions.NoUseFlagError, [460](#)
- cryptoauthlib.exceptions.ParityError, [460](#)
- cryptoauthlib.exceptions.ParseError, [461](#)
- cryptoauthlib.exceptions.ReceiveError, [468](#)
- cryptoauthlib.exceptions.ReceiveTimeoutError, [469](#)
- cryptoauthlib.exceptions.ResyncWithWakeupError, [469](#)
- cryptoauthlib.exceptions.StatusUnknownError, [473](#)
- cryptoauthlib.exceptions.TimeOutError, [473](#)
- cryptoauthlib.exceptions.TransmissionError, [474](#)
- cryptoauthlib.exceptions.TransmissionTimeoutError, [474](#)
- cryptoauthlib.exceptions.UnimplementedError, [475](#)
- cryptoauthlib.exceptions.UnsupportedInterface, [475](#)
- cryptoauthlib.exceptions.WakeFailedError, [477](#)
- cryptoauthlib.exceptions.ZoneNotLockedError, [478](#)
- cryptoauthlib.h, [654](#)
  - ATCA\_SHA256\_BLOCK\_SIZE, [655](#)
  - SHA\_MODE\_TARGET\_MSGDIGBUF, [655](#)
  - SHA\_MODE\_TARGET\_OUT\_ONLY, [655](#)
  - SHA\_MODE\_TARGET\_TEMPKEY, [655](#)
- cryptoauthlib.iface, [335](#)
  - \_iface\_load\_default\_config, [335](#)
  - cfg\_ateccx08a\_i2c\_default, [335](#)
  - cfg\_ateccx08a\_kithid\_default, [336](#)
  - cfg\_ateccx08a\_swi\_default, [336](#)
  - cfg\_atsha20xa\_i2c\_default, [336](#)
  - cfg\_atsha20xa\_kithid\_default, [336](#)
  - cfg\_atsha20xa\_swi\_default, [336](#)
- cryptoauthlib.iface.\_ATCACUSTOM, [357](#)
  - \_fields\_, [358](#)
- cryptoauthlib.iface.\_ATCAHID, [358](#)
  - \_def\_, [359](#)
- cryptoauthlib.iface.\_ATCAI2C, [359](#)
  - \_fields\_, [360](#)
  - \_map\_, [360](#)
- cryptoauthlib.iface.\_ATCAIfaceParams, [361](#)
  - \_fields\_, [361](#)
- cryptoauthlib.iface.\_ATCAKIT, [362](#)
  - \_def\_, [362](#)
- cryptoauthlib.iface.\_ATCASPI, [363](#)
  - \_fields\_, [363](#)
- cryptoauthlib.iface.\_ATCASWI, [364](#)
  - \_fields\_, [364](#)
- cryptoauthlib.iface.\_ATCAUART, [365](#)
  - \_def\_, [365](#)
- cryptoauthlib.iface.\_U\_Address, [367](#)
  - \_fields\_, [367](#)
- cryptoauthlib.iface.ATCADeviceType, [410](#)
- cryptoauthlib.iface.ATCAIfaceCfg, [414](#)
  - \_def\_, [415](#)
  - \_map\_, [415](#)
- cryptoauthlib.iface.ATCAIfaceType, [416](#)
- cryptoauthlib.iface.ATCAKitType, [417](#)
- cryptoauthlib.library, [337](#)
  - \_array\_to\_code, [338](#)
  - \_check\_type\_rationality, [338](#)
  - \_convert\_pointer\_to\_list, [338](#)
  - \_ctype\_from\_definition, [338](#)
  - \_def\_to\_field, [339](#)
  - \_force\_local\_library, [339](#)
  - \_get\_attribute\_from\_ctypes, [339](#)
  - \_get\_field\_definition, [339](#)
  - \_is\_pointer, [340](#)
  - \_obj\_to\_code, [340](#)
  - \_object\_definition\_code, [340](#)
  - \_pointer\_to\_code, [340](#)
  - \_structure\_to\_code, [341](#)
  - \_structure\_to\_string, [341](#)
  - \_to\_code, [341](#)
  - ctypes\_to\_bytes, [341](#)
  - get\_cryptoauthlib, [342](#)
  - get\_ctype\_array\_instance, [342](#)
  - get\_ctype\_by\_name, [342](#)
  - get\_ctype\_structure\_instance, [342](#)
  - get\_device\_name, [342](#)
  - get\_device\_name\_with\_device\_id, [343](#)
  - get\_device\_type\_id, [343](#)
  - get\_size\_by\_name, [343](#)
  - load\_cryptoauthlib, [343](#)
- cryptoauthlib.library.\_CtypeIterator, [366](#)
- cryptoauthlib.library.AtcaReference, [418](#)
- cryptoauthlib.library.AtcaStructure, [418](#)
  - check\_rationality, [419](#)
  - from\_definition, [419](#)
- cryptoauthlib.library.AtcaUnion, [420](#)
  - check\_rationality, [420](#)
  - from\_definition, [421](#)
- cryptoauthlib.sha206\_api, [344](#)
  - sha206a\_authenticate, [344](#)
  - sha206a\_check\_dk\_useflag\_validity, [344](#)
  - sha206a\_check\_pk\_useflag\_validity, [345](#)
  - sha206a\_diversify\_parent\_key, [345](#)
  - sha206a\_generate\_challenge\_response\_pair, [345](#)
  - sha206a\_generate\_derive\_key, [346](#)
  - sha206a\_get\_data\_store\_lock\_status, [346](#)
  - sha206a\_get\_dk\_update\_count, [347](#)
  - sha206a\_get\_dk\_useflag\_count, [347](#)
  - sha206a\_get\_pk\_useflag\_count, [347](#)
  - sha206a\_read\_data\_store, [347](#)

- sha206a\_verify\_device\_consumption, 348
- sha206a\_write\_data\_store, 348
- cryptoauthlib.status, 349
  - check\_status, 349
- cryptoauthlib.status.Status, 471
- cryptoauthlib.tng, 350
  - tng\_atcacert\_device\_public\_key, 350
  - tng\_atcacert\_max\_device\_cert\_size, 350
  - tng\_atcacert\_max\_signer\_cert\_size, 351
  - tng\_atcacert\_read\_device\_cert, 351
  - tng\_atcacert\_read\_signer\_cert, 351
  - tng\_atcacert\_root\_cert, 352
  - tng\_atcacert\_root\_cert\_size, 352
  - tng\_atcacert\_root\_public\_key, 352
  - tng\_atcacert\_signer\_public\_key, 353
  - tng\_get\_device\_pubkey, 353
- cryptoauthlib\_mock.atcab\_mock, 391
- ctypes\_to\_bytes
  - cryptoauthlib.library, 341
- DATEFMT\_ISO8601\_SEP
  - Certificate manipulation methods (atcacert\_), 181
- deleteATCADevice
  - ATCADevice (atca\_), 165
- deleteATCAIface
  - ATCAIface (atca\_), 172
- dev\_lock
  - pkcs11\_dev\_state, 462
- dev\_lock\_enabled
  - pkcs11\_lib\_ctx\_s, 464
- dev\_state
  - pkcs11\_lib\_ctx\_s, 464
- device\_execution\_time\_t, 451
- device\_state
  - atca\_device, 376
- devtype\_names\_t, 451
- DEVZONE\_CONFIG
  - Certificate manipulation methods (atcacert\_), 183
- DEVZONE\_DATA
  - Certificate manipulation methods (atcacert\_), 183
- DEVZONE\_GENKEY
  - Certificate manipulation methods (atcacert\_), 183
- DEVZONE\_NONE
  - Certificate manipulation methods (atcacert\_), 183
- DEVZONE\_OTP
  - Certificate manipulation methods (atcacert\_), 183
- ec\_key\_data\_table
  - Attributes (pkcs11\_attrib\_), 273
- from\_definition
  - cryptoauthlib.library.AtcaStructure, 419
  - cryptoauthlib.library.AtcaUnion, 421
- g\_tngtls\_cert\_elements\_1\_signer
  - tngtls\_cert\_def\_1\_signer.c, 514
- get\_cryptoauthlib
  - cryptoauthlib.library, 342
- get\_ctype\_array\_instance
  - cryptoauthlib.library, 342
- get\_ctype\_by\_name
  - cryptoauthlib.library, 342
- get\_ctype\_structure\_instance
  - cryptoauthlib.library, 342
- get\_device\_name
  - cryptoauthlib.library, 342
- get\_device\_name\_with\_device\_id
  - cryptoauthlib.library, 343
- get\_device\_type\_id
  - cryptoauthlib.library, 343
- get\_size\_by\_name
  - cryptoauthlib.library, 343
- hal
  - atca\_iface, 382
  - hal\_all\_platforms\_kit\_hidapi.c, 658
  - hal\_check\_wake
    - Hardware abstraction layer (hal\_), 226
  - hal\_create\_mutex
    - Hardware abstraction layer (hal\_), 226
  - hal\_data
    - atca\_hal\_kit\_phy\_t, 379
    - atca\_iface, 382
  - hal\_delay\_ms
    - Hardware abstraction layer (hal\_), 226
  - hal\_delay\_us
    - Hardware abstraction layer (hal\_), 227
  - hal\_freertos.c, 659
  - hal\_gpio\_harmony.c, 660
    - hal\_gpio\_init, 660
    - hal\_gpio\_post\_init, 661
    - hal\_gpio\_receive, 661
    - hal\_gpio\_release, 661
    - hal\_gpio\_send, 662
  - hal\_gpio\_init
    - hal\_gpio\_harmony.c, 660
  - hal\_gpio\_post\_init
    - hal\_gpio\_harmony.c, 661
  - hal\_gpio\_receive
    - hal\_gpio\_harmony.c, 661
  - hal\_gpio\_release
    - hal\_gpio\_harmony.c, 661
  - hal\_gpio\_send
    - hal\_gpio\_harmony.c, 662
  - hal\_i2c\_control
    - Hardware abstraction layer (hal\_), 227
  - hal\_i2c\_discover\_buses
    - Hardware abstraction layer (hal\_), 228
  - hal\_i2c\_discover\_devices
    - Hardware abstraction layer (hal\_), 229
  - hal\_i2c\_harmony.c, 662
  - hal\_i2c\_idle
    - Hardware abstraction layer (hal\_), 229
  - hal\_i2c\_init
    - Hardware abstraction layer (hal\_), 230, 231
  - hal\_i2c\_post\_init
    - Hardware abstraction layer (hal\_), 232
  - hal\_i2c\_receive

- Hardware abstraction layer (hal\_), 233
- hal\_i2c\_release
  - Hardware abstraction layer (hal\_), 234
- hal\_i2c\_send
  - Hardware abstraction layer (hal\_), 235
- hal\_i2c\_sleep
  - Hardware abstraction layer (hal\_), 236
- hal\_i2c\_start.c, 663
- hal\_i2c\_start.h, 664
- hal\_i2c\_wake
  - Hardware abstraction layer (hal\_), 237
- hal\_iface\_init
  - Hardware abstraction layer (hal\_), 237
- hal\_iface\_register\_hal
  - Hardware abstraction layer (hal\_), 238
- hal\_iface\_release
  - Hardware abstraction layer (hal\_), 238
- hal\_is\_command\_word
  - Hardware abstraction layer (hal\_), 238
- hal\_kit\_attach\_phy
  - Hardware abstraction layer (hal\_), 239
- hal\_kit\_bridge.c, 665
- hal\_kit\_bridge.h, 666
- hal\_kit\_control
  - Hardware abstraction layer (hal\_), 239
- hal\_kit\_hid\_control
  - Hardware abstraction layer (hal\_), 239
- hal\_kit\_hid\_init
  - Hardware abstraction layer (hal\_), 240
- hal\_kit\_hid\_post\_init
  - Hardware abstraction layer (hal\_), 240
- hal\_kit\_hid\_receive
  - Hardware abstraction layer (hal\_), 241
- hal\_kit\_hid\_release
  - Hardware abstraction layer (hal\_), 241
- hal\_kit\_hid\_send
  - Hardware abstraction layer (hal\_), 241
- hal\_kit\_init
  - Hardware abstraction layer (hal\_), 242
- hal\_kit\_post\_init
  - Hardware abstraction layer (hal\_), 242
- hal\_kit\_receive
  - Hardware abstraction layer (hal\_), 243
- hal\_kit\_release
  - Hardware abstraction layer (hal\_), 243
- hal\_kit\_send
  - Hardware abstraction layer (hal\_), 243
- hal\_linux.c, 667
- hal\_linux\_i2c\_userspace.c, 667
- hal\_linux\_uart\_userspace.c, 668
  - hal\_uart\_control, 669
  - hal\_uart\_init, 670
  - hal\_uart\_post\_init, 670
  - hal\_uart\_receive, 670
  - hal\_uart\_release, 671
  - hal\_uart\_send, 671
- hal\_rtos\_delay\_ms
  - Hardware abstraction layer (hal\_), 244
- hal\_sam0\_i2c\_asf.c, 672
- hal\_sam0\_i2c\_asf.h, 673
- hal\_sam\_i2c\_asf.c, 673
- hal\_sam\_i2c\_asf.h, 674
- hal\_sam\_timer\_asf.c, 675
- hal\_spi\_control
  - Hardware abstraction layer (hal\_), 244
- hal\_spi\_deselect
  - Hardware abstraction layer (hal\_), 245
- hal\_spi\_discover\_buses
  - Hardware abstraction layer (hal\_), 245
- hal\_spi\_discover\_devices
  - Hardware abstraction layer (hal\_), 245
- hal\_spi\_harmony.c, 676
- hal\_spi\_init
  - Hardware abstraction layer (hal\_), 246
- hal\_spi\_post\_init
  - Hardware abstraction layer (hal\_), 246
- hal\_spi\_receive
  - Hardware abstraction layer (hal\_), 247
- hal\_spi\_release
  - Hardware abstraction layer (hal\_), 247
- hal\_spi\_select
  - Hardware abstraction layer (hal\_), 247
- hal\_spi\_send
  - Hardware abstraction layer (hal\_), 248
- hal\_swi\_control
  - Hardware abstraction layer (hal\_), 248
- hal\_swi\_gpio.c, 677
  - hal\_swi\_gpio\_control, 677
  - hal\_swi\_gpio\_init, 678
  - hal\_swi\_gpio\_post\_init, 678
  - hal\_swi\_gpio\_receive, 678
  - hal\_swi\_gpio\_release, 679
  - hal\_swi\_gpio\_send, 679
- hal\_swi\_gpio.h, 680
  - ATCA\_SWI\_WAKE\_WORD\_ADDR, 682
  - BIT\_DELAY\_1L, 682
  - BIT\_DELAY\_5, 682
  - BIT\_DELAY\_7, 682
  - RX\_TX\_DELAY, 682
- hal\_swi\_gpio\_control
  - hal\_swi\_gpio.c, 677
- hal\_swi\_gpio\_init
  - hal\_swi\_gpio.c, 678
- hal\_swi\_gpio\_post\_init
  - hal\_swi\_gpio.c, 678
- hal\_swi\_gpio\_receive
  - hal\_swi\_gpio.c, 678
- hal\_swi\_gpio\_release
  - hal\_swi\_gpio.c, 679
- hal\_swi\_gpio\_send
  - hal\_swi\_gpio.c, 679
- hal\_swi\_idle
  - Hardware abstraction layer (hal\_), 249
- hal\_swi\_init
  - Hardware abstraction layer (hal\_), 249
- hal\_swi\_post\_init



Hardware abstraction layer (hal\_), 249  
 hal\_swi\_receive  
   Hardware abstraction layer (hal\_), 250  
 hal\_swi\_release  
   Hardware abstraction layer (hal\_), 250  
 hal\_swi\_send  
   Hardware abstraction layer (hal\_), 251  
 hal\_swi\_sleep  
   Hardware abstraction layer (hal\_), 251  
 hal\_swi\_uart.c, 682  
 hal\_swi\_wake  
   Hardware abstraction layer (hal\_), 252  
 hal\_timer\_start.c, 683  
 hal\_uart\_control  
   hal\_linux\_uart\_userspace.c, 669  
   hal\_windows\_kit\_uart.c, 692  
 hal\_uart\_harmony.c, 684  
   hal\_uart\_init, 685  
   hal\_uart\_post\_init, 686  
   hal\_uart\_receive, 686  
   hal\_uart\_release, 687  
   hal\_uart\_send, 687  
   serial\_setup, 687  
 hal\_uart\_init  
   hal\_linux\_uart\_userspace.c, 670  
   hal\_uart\_harmony.c, 685  
   hal\_windows\_kit\_uart.c, 692  
 hal\_uart\_post\_init  
   hal\_linux\_uart\_userspace.c, 670  
   hal\_uart\_harmony.c, 686  
   hal\_windows\_kit\_uart.c, 693  
 hal\_uart\_receive  
   hal\_linux\_uart\_userspace.c, 670  
   hal\_uart\_harmony.c, 686  
   hal\_windows\_kit\_uart.c, 693  
 hal\_uart\_release  
   hal\_linux\_uart\_userspace.c, 671  
   hal\_uart\_harmony.c, 687  
   hal\_windows\_kit\_uart.c, 693  
 hal\_uart\_send  
   hal\_linux\_uart\_userspace.c, 671  
   hal\_uart\_harmony.c, 687  
   hal\_windows\_kit\_uart.c, 695  
 hal\_uc3\_i2c\_asf.c, 688  
 hal\_uc3\_i2c\_asf.h, 689  
 hal\_uc3\_timer\_asf.c, 690  
 hal\_windows.c, 690  
 hal\_windows\_kit\_uart.c, 691  
   hal\_uart\_control, 692  
   hal\_uart\_init, 692  
   hal\_uart\_post\_init, 693  
   hal\_uart\_receive, 693  
   hal\_uart\_release, 693  
   hal\_uart\_send, 695  
 handle  
   pkcs11\_object\_cache\_s, 465  
 Hardware abstraction layer (hal\_), 216  
   atca\_delay\_10us, 224  
   atca\_delay\_ms, 224  
   atca\_delay\_us, 225  
   change\_i2c\_speed, 225  
   hal\_check\_wake, 226  
   hal\_create\_mutex, 226  
   hal\_delay\_ms, 226  
   hal\_delay\_us, 227  
   hal\_i2c\_control, 227  
   hal\_i2c\_discover\_buses, 228  
   hal\_i2c\_discover\_devices, 229  
   hal\_i2c\_idle, 229  
   hal\_i2c\_init, 230, 231  
   hal\_i2c\_post\_init, 232  
   hal\_i2c\_receive, 233  
   hal\_i2c\_release, 234  
   hal\_i2c\_send, 235  
   hal\_i2c\_sleep, 236  
   hal\_i2c\_wake, 237  
   hal\_iface\_init, 237  
   hal\_iface\_register\_hal, 238  
   hal\_iface\_release, 238  
   hal\_is\_command\_word, 238  
   hal\_kit\_attach\_phy, 239  
   hal\_kit\_control, 239  
   hal\_kit\_hid\_control, 239  
   hal\_kit\_hid\_init, 240  
   hal\_kit\_hid\_post\_init, 240  
   hal\_kit\_hid\_receive, 241  
   hal\_kit\_hid\_release, 241  
   hal\_kit\_hid\_send, 241  
   hal\_kit\_init, 242  
   hal\_kit\_post\_init, 242  
   hal\_kit\_receive, 243  
   hal\_kit\_release, 243  
   hal\_kit\_send, 243  
   hal\_rtos\_delay\_ms, 244  
   hal\_spi\_control, 244  
   hal\_spi\_deselect, 245  
   hal\_spi\_discover\_buses, 245  
   hal\_spi\_discover\_devices, 245  
   hal\_spi\_init, 246  
   hal\_spi\_post\_init, 246  
   hal\_spi\_receive, 247  
   hal\_spi\_release, 247  
   hal\_spi\_select, 247  
   hal\_spi\_send, 248  
   hal\_swi\_control, 248  
   hal\_swi\_idle, 249  
   hal\_swi\_init, 249  
   hal\_swi\_post\_init, 249  
   hal\_swi\_receive, 250  
   hal\_swi\_release, 250  
   hal\_swi\_send, 251  
   hal\_swi\_sleep, 251  
   hal\_swi\_wake, 252  
   kit\_id\_from\_devtype, 252  
   kit\_interface, 252  
   kit\_interface\_from\_kittype, 252

- MAX\_SWI\_BUSES, 223
- swi\_uart\_deinit, 252
- swi\_uart\_discover\_buses, 253
- swi\_uart\_init, 253
- swi\_uart\_mode, 254
- swi\_uart\_receive\_byte, 254
- swi\_uart\_send\_byte, 255
- swi\_uart\_setbaud, 255
- Host side crypto methods (atca\_), 255
- HOSTLIB\_CERT\_EN
  - atca\_mbedtls\_interface.h, 712
  - atca\_openssl\_interface.h, 742
- i2c\_sam0\_instance, 455
- i2c\_sam\_instance, 455
- i2c\_start\_instance, 455
- ifacecfg\_set\_address
  - ATCAIface (atca\_), 173
- ifacetype\_is\_kit
  - ATCAIface (atca\_), 173
- init\_args
  - pkcs11\_lib\_ctx\_s, 464
- initATCADevice
  - ATCADevice (atca\_), 165
- initATCAIface
  - ATCAIface (atca\_), 173
- initialized
  - pkcs11\_lib\_ctx\_s, 464
- io\_protection\_key.h, 498
- isAlpha
  - atca\_helpers.c, 550
  - Basic Crypto API methods (atcab\_), 159
- isATCAError
  - calib\_command.c, 596
  - calib\_command.h, 617
- isBase64
  - atca\_helpers.c, 550
  - Basic Crypto API methods (atcab\_), 160
- isBase64Digit
  - atca\_helpers.c, 551
  - Basic Crypto API methods (atcab\_), 160
- isBlankSpace
  - atca\_helpers.c, 551
  - Basic Crypto API methods (atcab\_), 160
- isDigit
  - atca\_helpers.c, 551
  - Basic Crypto API methods (atcab\_), 161
- isHex
  - atca\_helpers.c, 552
  - Basic Crypto API methods (atcab\_), 161
- isHexAlpha
  - atca\_helpers.c, 552
  - Basic Crypto API methods (atcab\_), 162
- isHexDigit
  - atca\_helpers.c, 552
  - Basic Crypto API methods (atcab\_), 162
- JSON Web Token (JWT) methods (atca\_jwt\_), 260
- kit\_host\_init
  - ascii\_kit\_host.c, 494
  - ascii\_kit\_host.h, 497
- kit\_host\_init\_phy
  - ascii\_kit\_host.c, 495
  - ascii\_kit\_host.h, 498
- kit\_host\_map\_entry\_t
  - ascii\_kit\_host.h, 497
- kit\_id\_from\_devtype
  - Hardware abstraction layer (hal\_), 252
- kit\_interface
  - Hardware abstraction layer (hal\_), 252
- kit\_interface\_from\_kittype
  - Hardware abstraction layer (hal\_), 252
- KIT\_MESSAGE\_SIZE\_MAX
  - ascii\_kit\_host.h, 496
- kit\_protocol.c, 695
- kit\_protocol.h, 696
- len
  - cal\_buffer\_s, 428
- lib\_lock
  - pkcs11\_lib\_ctx\_s, 464
- load\_cryptoauthlib
  - cryptoauthlib.library, 343
- MAX\_SWI\_BUSES
  - Hardware abstraction layer (hal\_), 223
- mbedtls Wrapper methods (atca\_mbedtls\_), 260
  - atca\_mbedtls\_ecdh\_ioprot\_cb, 261
  - atca\_mbedtls\_ecdh\_slot\_cb, 262
  - atca\_mbedtls\_eckey\_t, 261
  - atca\_mbedtls\_pk\_init, 262
  - atca\_mbedtls\_pk\_init\_ext, 262
- memory\_parameters, 459
- mlface
  - atca\_device, 376
- mlfaceCFG
  - atca\_iface, 382
- MULTIPART\_BUF\_EN
  - atca\_config\_check.h, 542
- newATCADevice
  - ATCADevice (atca\_), 165
- object
  - pkcs11\_object\_cache\_s, 465
- packet\_alloc
  - atca\_hal\_kit\_phy\_t, 379
- packet\_free
  - atca\_hal\_kit\_phy\_t, 379
- packHex
  - atca\_helpers.c, 553
  - Basic Crypto API methods (atcab\_), 162
- pkcs11\_mech\_table\_e, 461
- phy
  - atca\_hal\_list\_entry\_t, 380
  - atca\_iface, 382



pkcs11\_attrib.c, [742](#)  
 pkcs11\_attrib.h, [743](#)  
     attrib\_f, [744](#)  
 pkcs11\_attrib\_fill  
     Attributes (pkcs11\_attrib\_), [271](#)  
 pkcs11\_attrib\_model\_s, [461](#)  
 pkcs11\_cert.c, [744](#)  
 pkcs11\_cert.h, [745](#)  
 pkcs11\_cert\_wtlspublic\_attributes  
     Attributes (pkcs11\_attrib\_), [273](#)  
 pkcs11\_cert\_x509\_attributes  
     Attributes (pkcs11\_attrib\_), [274](#)  
 pkcs11\_cert\_x509public\_attributes  
     Attributes (pkcs11\_attrib\_), [274](#)  
 pkcs11\_conf\_filedata\_s, [461](#)  
 pkcs11\_config.c, [746](#)  
 pkcs11\_debug.c, [747](#)  
 pkcs11\_debug.h, [747](#)  
 pkcs11\_deinit  
     Attributes (pkcs11\_attrib\_), [272](#)  
 pkcs11\_dev\_ctx, [462](#)  
 pkcs11\_dev\_res, [462](#)  
 pkcs11\_dev\_state, [462](#)  
     dev\_lock, [462](#)  
     resources, [463](#)  
 pkcs11\_digest.h, [748](#)  
 pkcs11\_ec\_pbkey\_asn1\_hdr\_p224  
     Attributes (pkcs11\_attrib\_), [274](#)  
 pkcs11\_ec\_pbkey\_asn1\_hdr\_p256  
     Attributes (pkcs11\_attrib\_), [274](#)  
 pkcs11\_ec\_pbkey\_asn1\_hdr\_p384  
     Attributes (pkcs11\_attrib\_), [274](#)  
 pkcs11\_ec\_pbkey\_asn1\_hdr\_p521  
     Attributes (pkcs11\_attrib\_), [275](#)  
 pkcs11\_ecc\_key\_info\_s, [463](#)  
 pkcs11\_encrypt.c, [748](#)  
 pkcs11\_encrypt.h, [749](#)  
 pkcs11\_find.c, [750](#)  
 pkcs11\_find.h, [750](#)  
 pkcs11\_info.c, [751](#)  
 pkcs11\_info.h, [752](#)  
 pkcs11\_init  
     Attributes (pkcs11\_attrib\_), [272](#)  
 pkcs11\_init.c, [752](#)  
 pkcs11\_init.h, [753](#)  
     pkcs11\_lib\_ctx, [754](#)  
 pkcs11\_key.c, [754](#)  
 pkcs11\_key.h, [756](#)  
 pkcs11\_key\_private\_attributes  
     Attributes (pkcs11\_attrib\_), [275](#)  
 pkcs11\_key\_public\_attributes  
     Attributes (pkcs11\_attrib\_), [275](#)  
 pkcs11\_key\_secret\_attributes  
     Attributes (pkcs11\_attrib\_), [275](#)  
 pkcs11\_lib\_ctx  
     pkcs11\_init.h, [754](#)  
 pkcs11\_lib\_ctx\_s, [463](#)  
     config\_path, [464](#)  
     dev\_lock\_enabled, [464](#)  
     dev\_state, [464](#)  
     init\_args, [464](#)  
     initialized, [464](#)  
     lib\_lock, [464](#)  
     slot\_cnt, [464](#)  
     slots, [464](#)  
 pkcs11\_main.c, [757](#)  
 pkcs11\_mech.c, [762](#)  
 pkcs11\_mech.h, [762](#)  
 pkcs11\_object.c, [763](#)  
 pkcs11\_object.h, [764](#)  
 pkcs11\_object\_cache\_s, [465](#)  
     handle, [465](#)  
     object, [465](#)  
 pkcs11\_object\_monotonic\_attributes  
     Attributes (pkcs11\_attrib\_), [275](#)  
 pkcs11\_object\_s, [465](#)  
     attributes, [466](#)  
     class\_id, [466](#)  
     class\_type, [466](#)  
     count, [466](#)  
 pkcs11\_os.c, [766](#)  
 pkcs11\_os.h, [766](#)  
 pkcs11\_os\_create\_mutex  
     Attributes (pkcs11\_attrib\_), [272](#)  
 pkcs11\_session.c, [767](#)  
 pkcs11\_session.h, [768](#)  
     pkcs11\_session\_ctx, [769](#)  
 pkcs11\_session\_closeall  
     Attributes (pkcs11\_attrib\_), [272](#)  
 pkcs11\_session\_ctx  
     pkcs11\_session.h, [769](#)  
 pkcs11\_session\_ctx\_s, [466](#)  
 pkcs11\_session\_login  
     Attributes (pkcs11\_attrib\_), [273](#)  
 pkcs11\_session\_mech\_ctx\_s, [467](#)  
 pkcs11\_signature.c, [769](#)  
 pkcs11\_signature.h, [770](#)  
 pkcs11\_slot.c, [771](#)  
 pkcs11\_slot.h, [772](#)  
     pkcs11\_slot\_ctx, [773](#)  
 pkcs11\_slot\_ctx  
     pkcs11\_slot.h, [773](#)  
 pkcs11\_slot\_ctx\_s, [467](#)  
     read\_key, [468](#)  
 pkcs11\_token.c, [773](#)  
 pkcs11\_token.h, [774](#)  
 pkcs11\_token\_init  
     Attributes (pkcs11\_attrib\_), [273](#)  
 pkcs11\_util.c, [775](#)  
 pkcs11\_util.h, [776](#)  
 pkcs11\_x962\_asn1\_hdr\_ec224  
     Attributes (pkcs11\_attrib\_), [276](#)  
 pkcs11\_x962\_asn1\_hdr\_ec256  
     Attributes (pkcs11\_attrib\_), [276](#)  
 pkcs11\_x962\_asn1\_hdr\_ec384  
     Attributes (pkcs11\_attrib\_), [276](#)

- ul style="list-style-type: none; padding-left: 0;">
- pkcs11\_x962\_asn1\_hdr\_ec521
  - Attributes (pkcs11\_attrib\_), 276
- read\_key
  - pkcs11\_slot\_ctx\_s, 468
- recv
  - atca\_hal\_kit\_phy\_t, 379
- releaseATCADevice
  - ATCADevice (atca\_), 166
- releaseATCAIface
  - ATCAIface (atca\_), 174
- resources
  - pkcs11\_dev\_state, 463
- RX\_TX\_DELAY
  - hal\_swi\_gpio.h, 682
- secure\_boot.c, 499
  - bind\_host\_and\_secure\_element\_with\_io\_protection, 499
  - secure\_boot\_process, 500
- secure\_boot.h, 500
  - bind\_host\_and\_secure\_element\_with\_io\_protection, 501
  - secure\_boot\_process, 501
- secure\_boot\_config\_bits, 469
- secure\_boot\_memory.h, 502
- secure\_boot\_parameters, 470
- secure\_boot\_process
  - secure\_boot.c, 500
  - secure\_boot.h, 501
- send
  - atca\_hal\_kit\_phy\_t, 379
- serial\_setup
  - hal\_uart\_harmony.c, 687
- setup.BinaryDistribution, 428
- setup.CryptoAuthCommandBuildExt, 449
- setup.CryptoAuthCommandInstall, 449
- sha1\_routines.c, 651
- sha1\_routines.h, 652
- sha206a\_authenticate
  - api\_206a.c, 480
  - api\_206a.h, 486
  - cryptoauthlib.sha206\_api, 344
- sha206a\_check\_dk\_useflag\_validity
  - api\_206a.c, 480
  - api\_206a.h, 487
  - cryptoauthlib.sha206\_api, 344
- sha206a\_check\_pk\_useflag\_validity
  - api\_206a.c, 481
  - api\_206a.h, 487
  - cryptoauthlib.sha206\_api, 345
- sha206a\_diversify\_parent\_key
  - api\_206a.c, 481
  - api\_206a.h, 487
  - cryptoauthlib.sha206\_api, 345
- sha206a\_generate\_challenge\_response\_pair
  - api\_206a.c, 481
  - api\_206a.h, 488
  - cryptoauthlib.sha206\_api, 345
- sha206a\_generate\_derive\_key
  - api\_206a.c, 482
  - api\_206a.h, 488
  - cryptoauthlib.sha206\_api, 346
- sha206a\_get\_data\_store\_lock\_status
  - api\_206a.c, 482
  - api\_206a.h, 489
  - cryptoauthlib.sha206\_api, 346
- sha206a\_get\_dk\_update\_count
  - api\_206a.c, 483
  - api\_206a.h, 489
  - cryptoauthlib.sha206\_api, 347
- sha206a\_get\_dk\_useflag\_count
  - api\_206a.c, 483
  - api\_206a.h, 489
  - cryptoauthlib.sha206\_api, 347
- sha206a\_get\_pk\_useflag\_count
  - api\_206a.c, 483
  - api\_206a.h, 490
  - cryptoauthlib.sha206\_api, 347
- sha206a\_read\_data\_store
  - api\_206a.c, 484
  - api\_206a.h, 490
  - cryptoauthlib.sha206\_api, 347
- sha206a\_verify\_device\_consumption
  - api\_206a.c, 484
  - api\_206a.h, 491
  - cryptoauthlib.sha206\_api, 348
- sha206a\_write\_data\_store
  - api\_206a.c, 485
  - api\_206a.h, 491
  - cryptoauthlib.sha206\_api, 348
- sha2\_routines.c, 652
- sha2\_routines.h, 653
- SHA\_MODE\_TARGET\_MSGDIGBUF
  - cryptoauthlib.h, 655
- SHA\_MODE\_TARGET\_OUT\_ONLY
  - cryptoauthlib.h, 655
- SHA\_MODE\_TARGET\_TEMPKEY
  - cryptoauthlib.h, 655
- sign
  - cryptoauthlib.atjwt.HwEcAlgorithm, 454
  - cryptoauthlib.atjwt.HwHmacAlgorithm, 454
- slot\_cnt
  - pkcs11\_lib\_ctx\_s, 464
- slot\_key
  - atca\_check\_mac\_in\_out, 374
- slots
  - pkcs11\_lib\_ctx\_s, 464
- SNSRC\_DEVICE\_SN
  - Certificate manipulation methods (atcacert\_), 183
- SNSRC\_DEVICE\_SN\_HASH
  - Certificate manipulation methods (atcacert\_), 183
- SNSRC\_DEVICE\_SN\_HASH\_POS
  - Certificate manipulation methods (atcacert\_), 183
- SNSRC\_DEVICE\_SN\_HASH\_RAW
  - Certificate manipulation methods (atcacert\_), 183
- SNSRC\_PUB\_KEY\_HASH

- Certificate manipulation methods (atcacert\_), 183
- SNSRC\_PUB\_KEY\_HASH\_POS
  - Certificate manipulation methods (atcacert\_), 183
- SNSRC\_PUB\_KEY\_HASH\_RAW
  - Certificate manipulation methods (atcacert\_), 183
- SNSRC\_SIGNER\_ID
  - Certificate manipulation methods (atcacert\_), 183
- SNSRC\_STORED
  - Certificate manipulation methods (atcacert\_), 183
- SNSRC\_STORED\_DYNAMIC
  - Certificate manipulation methods (atcacert\_), 183
- Software crypto methods (atcac\_), 216
- STDCERT\_NUM\_ELEMENTS
  - Certificate manipulation methods (atcacert\_), 184
- sw\_sha256\_ctx, 473
- swi\_uart\_deinit
  - Hardware abstraction layer (hal\_), 252
- swi\_uart\_discover\_buses
  - Hardware abstraction layer (hal\_), 253
- swi\_uart\_init
  - Hardware abstraction layer (hal\_), 253
- swi\_uart\_mode
  - Hardware abstraction layer (hal\_), 254
- swi\_uart\_receive\_byte
  - Hardware abstraction layer (hal\_), 254
- swi\_uart\_samd21\_asf.c, 697
- swi\_uart\_samd21\_asf.h, 698
- swi\_uart\_send\_byte
  - Hardware abstraction layer (hal\_), 255
- swi\_uart\_setbaud
  - Hardware abstraction layer (hal\_), 255
- swi\_uart\_start.c, 699
- swi\_uart\_start.h, 700
- symmetric\_authenticate
  - symmetric\_authentication.c, 492
  - symmetric\_authentication.h, 493
- symmetric\_authentication.c, 492
  - symmetric\_authenticate, 492
- symmetric\_authentication.h, 493
  - symmetric\_authenticate, 493
- target\_key
  - atca\_check\_mac\_in\_out, 374
- test\_device, 354
  - ATECC508A\_DEVICE\_CONFIG, 354
  - ATECC508A\_DEVICE\_CONFIG\_VECTOR, 354
  - ATECC608\_DEVICE\_CONFIG, 355
  - ATECC608\_DEVICE\_CONFIG\_VECTOR, 355
  - ATSHA204A\_DEVICE\_CONFIG, 355
  - ATSHA204A\_DEVICE\_CONFIG\_VECTOR, 356
- test\_iface, 356
- TF\_BIN2HEX\_LC
  - Certificate manipulation methods (atcacert\_), 184
- TF\_BIN2HEX\_SPACE\_LC
  - Certificate manipulation methods (atcacert\_), 184
- TF\_BIN2HEX\_SPACE\_UC
  - Certificate manipulation methods (atcacert\_), 184
- TF\_BIN2HEX\_UC
  - Certificate manipulation methods (atcacert\_), 184
- TF\_HEX2BIN\_LC
  - Certificate manipulation methods (atcacert\_), 184
- TF\_HEX2BIN\_SPACE\_LC
  - Certificate manipulation methods (atcacert\_), 184
- TF\_HEX2BIN\_SPACE\_UC
  - Certificate manipulation methods (atcacert\_), 184
- TF\_HEX2BIN\_UC
  - Certificate manipulation methods (atcacert\_), 184
- TF\_NONE
  - Certificate manipulation methods (atcacert\_), 184
- TF\_REVERSE
  - Certificate manipulation methods (atcacert\_), 184
- tflxtls\_cert\_def\_4\_device.c, 502
- tflxtls\_cert\_def\_4\_device.h, 503
- TNG API (tng\_), 73
  - tng\_atcacert\_device\_public\_key, 75
  - tng\_atcacert\_max\_device\_cert\_size, 75
  - tng\_atcacert\_max\_signer\_cert\_size, 75
  - tng\_atcacert\_read\_device\_cert, 76
  - tng\_atcacert\_read\_signer\_cert, 76
  - tng\_atcacert\_root\_cert, 77
  - tng\_atcacert\_root\_cert\_size, 77
  - tng\_atcacert\_root\_public\_key, 77
  - tng\_atcacert\_signer\_public\_key, 78
  - tng\_get\_device\_cert\_def, 78
  - tng\_get\_device\_cert\_def\_ext, 78
  - tng\_get\_device\_pubkey, 79
  - tng\_map\_get\_device\_cert\_def, 79
- tng\_atca.c, 503
- tng\_atca.h, 504
- tng\_atcacert\_client.c, 505
  - tng\_atcacert\_device\_public\_key, 506
  - tng\_atcacert\_max\_signer\_cert\_size, 506
  - tng\_atcacert\_read\_device\_cert, 506
  - tng\_atcacert\_read\_signer\_cert, 507
  - tng\_atcacert\_root\_cert, 507
  - tng\_atcacert\_root\_cert\_size, 508
  - tng\_atcacert\_root\_public\_key, 508
  - tng\_atcacert\_signer\_public\_key, 508
- tng\_atcacert\_client.h, 509
- tng\_atcacert\_device\_public\_key
  - cryptoauthlib.tng, 350
  - TNG API (tng\_), 75
  - tng\_atcacert\_client.c, 506
- tng\_atcacert\_max\_device\_cert\_size
  - cryptoauthlib.tng, 350
  - TNG API (tng\_), 75
- tng\_atcacert\_max\_signer\_cert\_size
  - cryptoauthlib.tng, 351
  - TNG API (tng\_), 75
  - tng\_atcacert\_client.c, 506
- tng\_atcacert\_read\_device\_cert
  - cryptoauthlib.tng, 351
  - TNG API (tng\_), 76
  - tng\_atcacert\_client.c, 506
- tng\_atcacert\_read\_signer\_cert
  - cryptoauthlib.tng, 351
  - TNG API (tng\_), 76

- tng\_atcacert\_client.c, [507](#)
- tng\_atcacert\_root\_cert
  - cryptoauthlib.tng, [352](#)
  - TNG API (tng\_), [77](#)
  - tng\_atcacert\_client.c, [507](#)
- tng\_atcacert\_root\_cert\_size
  - cryptoauthlib.tng, [352](#)
  - TNG API (tng\_), [77](#)
  - tng\_atcacert\_client.c, [508](#)
- tng\_atcacert\_root\_public\_key
  - cryptoauthlib.tng, [352](#)
  - TNG API (tng\_), [77](#)
  - tng\_atcacert\_client.c, [508](#)
- tng\_atcacert\_signer\_public\_key
  - cryptoauthlib.tng, [353](#)
  - TNG API (tng\_), [78](#)
  - tng\_atcacert\_client.c, [508](#)
- tng\_cert\_map\_element, [474](#)
- tng\_get\_device\_cert\_def
  - TNG API (tng\_), [78](#)
- tng\_get\_device\_cert\_def\_ext
  - TNG API (tng\_), [78](#)
- tng\_get\_device\_pubkey
  - cryptoauthlib.tng, [353](#)
  - TNG API (tng\_), [79](#)
- tng\_map\_get\_device\_cert\_def
  - TNG API (tng\_), [79](#)
- tng\_root\_cert.c, [510](#)
- tng\_root\_cert.h, [510](#)
- tnglora\_cert\_def\_1\_signer.c, [510](#)
- tnglora\_cert\_def\_1\_signer.h, [511](#)
- tnglora\_cert\_def\_2\_device.c, [511](#)
- tnglora\_cert\_def\_2\_device.h, [512](#)
- tnglora\_cert\_def\_4\_device.c, [512](#)
- tnglora\_cert\_def\_4\_device.h, [513](#)
- tngtls\_cert\_def\_1\_signer.c, [513](#)
  - g\_tngtls\_cert\_elements\_1\_signer, [514](#)
- tngtls\_cert\_def\_1\_signer.h, [514](#)
- tngtls\_cert\_def\_2\_device.c, [514](#)
- tngtls\_cert\_def\_2\_device.h, [515](#)
- tngtls\_cert\_def\_3\_device.c, [515](#)
- tngtls\_cert\_def\_3\_device.h, [516](#)
- trust\_pkcs11\_config.c, [498](#)
- UNUSED\_VAR
  - atca\_compiler.h, [538](#)
- verify
  - cryptoauthlib.atjwt.HwHmacAlgorithm, [455](#)
- wpc\_apis.c, [516](#)
- wpc\_apis.h, [517](#)
- wpccert\_client.c, [518](#)
  - wpccert\_read\_cert, [518](#)
- wpccert\_client.h, [519](#)
  - wpccert\_read\_cert, [519](#)
- wpccert\_read\_cert
  - wpccert\_client.c, [518](#)
  - wpccert\_client.h, [519](#)