RPKI Engine

1.0

Generated by Doxygen 1.6.3

Wed Apr 14 19:04:13 2010

Contents

1 RPKI Engine Reference Manual **1**

2 Further Reading **2**

3 Installation Guide **2**

4 Configuration Guide **5**

5 Operation Guide **8**

5.1 Common Options 9
5.2 rpkid 10
5.3 pubd 11
5.4 rootd 12
5.5 irdbd 14
5.6 irbe_cli 15
5.7 cross_certify 17
5.8 cronjob 17
5.9 smoketest: 18
5.10 testpoke 20

6 Left-right protocol **21**

6.1 Terminology 22
6.2 initiated by the IRBE 22
6.2.1 <self/> object 22
6.2.2 <bsc/> object 24
6.2.3 <parent/> object 25
6.2.4 <child/> object 26
6.2.5 <repository/> object 27
6.2.6 <route_origin/> object 28
6.3 Operations initiated by the RPKI engine 29
6.3.1 <list_resources/> messages 29
6.4 Error handling 30

7 Publication protocol **31**
7.1 Terminology 31
7.2 Publication control subprotocol 32
7.2.1 <config/> object 32
7.2.2 <client/> object 32
7.3 Publication subprotocol 33
7.3.1 <certificate/> object 33
7.3.2 <crl/> object 33
7.3.3 <manifest/> object 33
7.3.4 <roa/> object 33
7.4 Error handling 34
7.5 Additional access control considerations. 34

8 SQL database schemas **35**
8.1 rpkid SQL schema 37
8.2 pubd SQL Schema 42
8.3 irdbd SQL Schema 43

9 BPKI model **45**

10 Namespace Documentation **48**
10.1 Package irbe_cli 48
10.1.1 Detailed Description 49
10.1.2 Function Documentation 50
10.1.3 Variable Documentation 50
10.2 Package irdbd 52
10.2.1 Detailed Description 53
10.2.2 Function Documentation 53
10.2.3 Variable Documentation 54
10.3 Package pubd 56
10.3.1 Detailed Description 57
10.3.2 Function Documentation 57

10.3.3 Variable Documentation 58
10.4 Package rootd 58
10.4.1 Detailed Description 59
10.4.2 Function Documentation 60
10.4.3 Variable Documentation 62
10.5 Package rpki 66
10.6 Package rpki.__doc__ 66
10.7 Package rpki.async 66
10.7.1 Detailed Description 67
10.7.2 Function Documentation 67
10.7.3 Variable Documentation 68
10.8 Package rpki.cli 69
10.8.1 Detailed Description 69
10.8.2 Function Documentation 69
10.8.3 Variable Documentation 70
10.9 Package rpki.config 70
10.9.1 Detailed Description 70
10.10 Package rpki.exceptions 71
10.10.1 Detailed Description 72
10.11 Package rpki.https 73
10.11.1 Detailed Description 74
10.11.2 Function Documentation 75
10.11.3 Variable Documentation 76
10.12 Package rpki.ipaddrs 78
10.12.1 Detailed Description 78
10.13 Package rpki.left_right 79
10.13.1 Detailed Description 79
10.13.2 Variable Documentation 80
10.14 Package rpki.log 80
10.14.1 Detailed Description 81
10.14.2 Function Documentation 81

10.14.3 Variable Documentation 82
10.15 Package rpki.manifest 83
10.15.1 Detailed Description 84
10.16 Package rpki.oids 84
10.16.1 Detailed Description 84
10.16.2 Variable Documentation 85
10.17 Package rpki.publication 86
10.17.1 Detailed Description 86
10.18 Package rpki.relaxng 87
10.18.1 Variable Documentation 87
10.19 Package rpki.resource_set 87
10.19.1 Detailed Description 88
10.19.2 Function Documentation 89
10.19.3 Variable Documentation 90
10.20 Package rpki.roa 90
10.20.1 Detailed Description 90
10.21 Package rpki.rpki_engine 91
10.21.1 Detailed Description 92
10.22 Package rpki.sql 92
10.22.1 Detailed Description 92
10.23 Package rpki.sundial 93
10.23.1 Detailed Description 93
10.23.2 Function Documentation 94
10.24 Package rpki.up_down 95
10.24.1 Detailed Description 95
10.24.2 Variable Documentation 96
10.25 Package rpki.x509 96
10.25.1 Detailed Description 97
10.25.2 Function Documentation 98
10.26 Package rpki.xml_utils 98
10.26.1 Detailed Description 99

10.27 Package rpkid 99
10.27.1 Detailed Description 99
10.27.2 Function Documentation 100
10.27.3 Variable Documentation 100

11 Class Documentation **101**
11.1 async_chat Class Reference 101
11.2 dispatcher Class Reference 101
11.3 Cmd Class Reference 101
11.4 Exception Class Reference 101
11.5 irbe_cli.bsc_elt Class Reference 101
11.5.1 Detailed Description 103
11.5.2 Member Function Documentation 103
11.5.3 Member Data Documentation 104
11.6 irbe_cli.certificate_elt Class Reference 104
11.6.1 Detailed Description 105
11.7 irbe_cli.child_elt Class Reference 106
11.7.1 Detailed Description 108
11.8 irbe_cli.client_elt Class Reference 108
11.8.1 Detailed Description 110
11.9 irbe_cli.cmd_elt_mixin Class Reference 110
11.9.1 Detailed Description 112
11.9.2 Member Function Documentation 112
11.9.3 Member Data Documentation 114
11.10 irbe_cli.cmd_msg_mixin Class Reference 115
11.10.1 Detailed Description 116
11.10.2 Member Function Documentation 116
11.11 irbe_cli.config_elt Class Reference 116
11.11.1 Detailed Description 118
11.11.2 Member Function Documentation 118
11.11.3 Member Data Documentation 118

11.12irbe_cli.crl_elt Class Reference 118
11.12.1 Detailed Description 119
11.13irbe_cli.left_right_cms_msg Class Reference 120
11.13.1 Detailed Description 121
11.13.2 Member Data Documentation 121
11.14irbe_cli.left_right_msg Class Reference 121
11.14.1 Detailed Description 123
11.14.2 Member Data Documentation 123
11.15irbe_cli.left_right_proto Class Reference 123
11.15.1 Detailed Description 124
11.15.2 Member Data Documentation 124
11.16irbe_cli.left_right_sax_handler Class Reference 125
11.16.1 Detailed Description 126
11.16.2 Member Data Documentation 126
11.17irbe_cli.list_published_objects_elt Class Reference 126
11.17.1 Detailed Description 128
11.17.2 Member Data Documentation 128
11.18irbe_cli.list_received_resources_elt Class Reference 128
11.18.1 Detailed Description 130
11.18.2 Member Data Documentation 130
11.19irbe_cli.manifest_elt Class Reference 130
11.19.1 Detailed Description 131
11.20irbe_cli.parent_elt Class Reference 132
11.20.1 Detailed Description 134
11.21irbe_cli.publication_cms_msg Class Reference 134
11.21.1 Detailed Description 135
11.21.2 Member Data Documentation 136
11.22irbe_cli.publication_msg Class Reference 136
11.22.1 Detailed Description 138
11.22.2 Member Data Documentation 138
11.23irbe_cli.publication_proto Class Reference 138

11.23.1 Detailed Description 139
11.23.2 Member Data Documentation 139
11.24 irbe_cli.publication_sax_handler Class Reference 140
11.24.1 Detailed Description 141
11.24.2 Member Data Documentation 141
11.25 irbe_cli.reply_elt_mixin Class Reference 141
11.25.1 Detailed Description 142
11.25.2 Member Function Documentation 142
11.25.3 Member Data Documentation 143
11.26 irbe_cli.report_error_elt Class Reference 143
11.26.1 Detailed Description 144
11.27 irbe_cli.repository_elt Class Reference 144
11.27.1 Detailed Description 146
11.28 irbe_cli.roa_elt Class Reference 146
11.28.1 Detailed Description 147
11.29 irbe_cli.self_elt Class Reference 148
11.29.1 Detailed Description 150
11.30 irbe_cli.UsageWrapper Class Reference 150
11.30.1 Detailed Description 150
11.30.2 Member Function Documentation 151
11.31 long Class Reference 151
11.32 object Class Reference 151
11.33 pubd.pubd_context Class Reference 151
11.33.1 Detailed Description 153
11.33.2 Member Function Documentation 153
11.33.3 Member Data Documentation 154
11.34 datetime Class Reference 156
11.35 timedelta Class Reference 156
11.36 rootd.cms_msg Class Reference 156
11.36.1 Detailed Description 157
11.36.2 Member Data Documentation 158

11.37 rootd.issue_pdu Class Reference 158
11.37.1 Detailed Description 159
11.37.2 Member Function Documentation 160
11.38 rootd.list_pdu Class Reference 160
11.38.1 Detailed Description 161
11.38.2 Member Function Documentation 162
11.39 rootd.message_pdu Class Reference 162
11.39.1 Detailed Description 164
11.39.2 Member Function Documentation 164
11.39.3 Member Data Documentation 164
11.40 rootd.revoke_pdu Class Reference 165
11.40.1 Detailed Description 166
11.40.2 Member Function Documentation 166
11.41 rootd.sax_handler Class Reference 166
11.41.1 Detailed Description 167
11.41.2 Member Data Documentation 168
11.42 rpki.async.gc_summary Class Reference 168
11.42.1 Detailed Description 169
11.42.2 Member Function Documentation 169
11.42.3 Member Data Documentation 169
11.43 rpki.async.iterator Class Reference 170
11.43.1 Detailed Description 171
11.43.2 Member Function Documentation 171
11.43.3 Member Data Documentation 172
11.44 rpki.async.sync_wrapper Class Reference 173
11.44.1 Detailed Description 175
11.44.2 Member Function Documentation 175
11.44.3 Member Data Documentation 176
11.45 rpki.async.timer Class Reference 176
11.45.1 Detailed Description 178
11.45.2 Member Function Documentation 179

11.45.3 Member Data Documentation 181
11.46 rpki.cli.Cmd Class Reference 182
11.46.1 Detailed Description 184
11.46.2 Member Function Documentation 184
11.46.3 Member Data Documentation 186
11.47 rpki.config.parser Class Reference 187
11.47.1 Detailed Description 189
11.47.2 Member Function Documentation 189
11.47.3 Member Data Documentation 191
11.48 rpki.exceptions.BadClassNameSyntax Class Reference 192
11.48.1 Detailed Description 193
11.49 rpki.exceptions.BadClientURL Class Reference 193
11.49.1 Detailed Description 194
11.50 rpki.exceptions.BadContactURL Class Reference 194
11.50.1 Detailed Description 195
11.51 rpki.exceptions.BadExtension Class Reference 195
11.51.1 Detailed Description 196
11.52 rpki.exceptions.BadIRDBReply Class Reference 196
11.52.1 Detailed Description 197
11.53 rpki.exceptions.BadIssueResponse Class Reference 197
11.53.1 Detailed Description 198
11.54 rpki.exceptions.BadPKCS10 Class Reference 198
11.54.1 Detailed Description 199
11.55 rpki.exceptions.BadPublicationReply Class Reference 199
11.55.1 Detailed Description 200
11.56 rpki.exceptions.BadQuery Class Reference 200
11.56.1 Detailed Description 201
11.57 rpki.exceptions.BadSender Class Reference 201
11.57.1 Detailed Description 202
11.58 rpki.exceptions.BadStatusCode Class Reference 202
11.58.1 Detailed Description 203

11.59 rpki.exceptions.BadURISyntax Class Reference 203
11.59.1 Detailed Description 204
11.60 rpki.exceptions.BSCNotFound Class Reference 204
11.60.1 Detailed Description 205
11.61 rpki.exceptions.BSCNotReady Class Reference 205
11.61.1 Detailed Description 206
11.62 rpki.exceptions.ChildNotFound Class Reference 206
11.62.1 Detailed Description 207
11.63 rpki.exceptions.ClassNameMismatch Class Reference 207
11.63.1 Detailed Description 208
11.64 rpki.exceptions.ClassNameUnknown Class Reference 208
11.64.1 Detailed Description 209
11.65 rpki.exceptions.ClientNotFound Class Reference 209
11.65.1 Detailed Description 210
11.66 rpki.exceptions.CMSContentNotSet Class Reference 210
11.66.1 Detailed Description 211
11.67 rpki.exceptions.CMSCRLNotSet Class Reference 212
11.67.1 Detailed Description 212
11.68 rpki.exceptions.CMSVerificationFailed Class Reference 213
11.68.1 Detailed Description 213
11.69 rpki.exceptions.DBConsistancyError Class Reference 214
11.69.1 Detailed Description 214
11.70 rpki.exceptions.DERObjectConversionError Class Reference 215
11.70.1 Detailed Description 215
11.71 rpki.exceptions.DuplicateObject Class Reference 216
11.71.1 Detailed Description 216
11.72 rpki.exceptions.EmptyPEM Class Reference 217
11.72.1 Detailed Description 217
11.73 rpki.exceptions.EmptyROAPrefixList Class Reference 218
11.73.1 Detailed Description 218
11.74 rpki.exceptions.ForbiddenURI Class Reference 219

11.74.1 Detailed Description 219
11.75 rpki.exceptions.HandleTranslationError Class Reference 220
11.75.1 Detailed Description 220
11.76 rpki.exceptions.HTTPRequestFailed Class Reference 221
11.76.1 Detailed Description 221
11.77 rpki.exceptions.HTTPSBadVersion Class Reference 222
11.77.1 Detailed Description 222
11.78 rpki.exceptions.HTTPSClientAborted Class Reference 223
11.78.1 Detailed Description 223
11.79 rpki.exceptions.HTTPSUnexpectedState Class Reference 224
11.79.1 Detailed Description 224
11.80 rpki.exceptions.MissingCMSCRL Class Reference 225
11.80.1 Detailed Description 225
11.81 rpki.exceptions.MissingCMSEEcert Class Reference 226
11.81.1 Detailed Description 226
11.82 rpki.exceptions.MultipleTLSEECert Class Reference 227
11.82.1 Detailed Description 228
11.83 rpki.exceptions.MustBePrefix Class Reference 228
11.83.1 Detailed Description 229
11.84 rpki.exceptions.NoActiveCA Class Reference 229
11.84.1 Detailed Description 230
11.85 rpki.exceptions.NoCoveringCertForROA Class Reference 230
11.85.1 Detailed Description 231
11.86 rpki.exceptions.NoObjectAtURI Class Reference 231
11.86.1 Detailed Description 232
11.87 rpki.exceptions.NotACertificateChain Class Reference 232
11.87.1 Detailed Description 233
11.88 rpki.exceptions.NotFound Class Reference 233
11.88.1 Detailed Description 234
11.89 rpki.exceptions.NotImplementedYet Class Reference 234
11.89.1 Detailed Description 235

11.90 rpki.exceptions.NotInDatabase Class Reference 235
11.90.1 Detailed Description 236
11.91 rpki.exceptions.ReceivedTLSCACert Class Reference 236
11.91.1 Detailed Description 237
11.92 rpki.exceptions.RPKI_Exception Class Reference 238
11.92.1 Detailed Description 239
11.93 rpki.exceptions.ServerShuttingDown Class Reference 239
11.93.1 Detailed Description 240
11.94 rpki.exceptions.SKIMismatch Class Reference 240
11.94.1 Detailed Description 241
11.95 rpki.exceptions.SubprocessError Class Reference 241
11.95.1 Detailed Description 242
11.96 rpki.exceptions.TLSValidationError Class Reference 242
11.96.1 Detailed Description 243
11.97 rpki.exceptions.UnexpectedCMSCerts Class Reference 244
11.97.1 Detailed Description 244
11.98 rpki.exceptions.UnexpectedCMSCRLs Class Reference 245
11.98.1 Detailed Description 245
11.99 rpki.exceptions.UnparsableCMSDER Class Reference 246
11.99.1 Detailed Description 246
11.100 rpki.exceptions.UpstreamError Class Reference 247
11.100.1 Detailed Description 247
11.101 rpki.exceptions.WrongEContentType Class Reference 248
11.101.1 Detailed Description 248
11.102 rpki.https.caller Class Reference 249
11.102.1 Detailed Description 250
11.102.2 Member Function Documentation 250
11.102.3 Member Data Documentation 250
11.103 rpki.https.http_client Class Reference 251
11.103.1 Detailed Description 253
11.103.2 Member Function Documentation 253

11.103.3 Member Data Documentation 256
11.104 rpki.https.http_listener Class Reference 258
11.104.1 Detailed Description 259
11.104.2 Member Function Documentation 259
11.104.3 Member Data Documentation 260
11.105 rpki.https.http_message Class Reference 261
11.105.1 Detailed Description 262
11.105.2 Member Function Documentation 262
11.105.3 Member Data Documentation 264
11.106 rpki.https.http_queue Class Reference 264
11.106.1 Detailed Description 266
11.106.2 Member Function Documentation 266
11.106.3 Member Data Documentation 267
11.107 rpki.https.http_request Class Reference 268
11.107.1 Detailed Description 270
11.107.2 Member Function Documentation 270
11.107.3 Member Data Documentation 271
11.108 rpki.https.http_response Class Reference 271
11.108.1 Detailed Description 273
11.108.2 Member Function Documentation 273
11.108.3 Member Data Documentation 273
11.109 rpki.https.http_server Class Reference 274
11.109.1 Detailed Description 276
11.109.2 Member Function Documentation 276
11.109.3 Member Data Documentation 278
11.110 rpki.https.http_stream Class Reference 279
11.110.1 Detailed Description 281
11.110.2 Member Function Documentation 282
11.110.3 Member Data Documentation 287
11.111 rpki.ipaddrs.v4addr Class Reference 288
11.111.1 Detailed Description 289

11.111.2 Member Function Documentation 289
11.111.3 Member Data Documentation 290
11.112 pki.ipaddrs.v6addr Class Reference 290
11.112.1 Detailed Description 291
11.112.2 Member Function Documentation 292
11.112.3 Member Data Documentation 292
11.113 pki.left_right.bsc_elt Class Reference 293
11.113.1 Detailed Description 295
11.113.2 Member Function Documentation 295
11.113.3 Member Data Documentation 296
11.114 pki.left_right.child_elt Class Reference 298
11.114.1 Detailed Description 300
11.114.2 Member Function Documentation 300
11.114.3 Member Data Documentation 302
11.115 pki.left_right.cms_msg Class Reference 303
11.115.1 Detailed Description 305
11.115.2 Member Data Documentation 305
11.116 pki.left_right.data_elt Class Reference 305
11.116.1 Detailed Description 307
11.116.2 Member Function Documentation 307
11.116.3 Member Data Documentation 309
11.117 pki.left_right.left_right_namespace Class Reference 309
11.117.1 Detailed Description 310
11.117.2 Member Data Documentation 310
11.118 pki.left_right.list_published_objects_elt Class Reference 311
11.118.1 Detailed Description 313
11.118.2 Member Function Documentation 313
11.118.3 Member Data Documentation 314
11.119 pki.left_right.list_received_resources_elt Class Reference 314
11.119.1 Detailed Description 316
11.119.2 Member Function Documentation 316

11.119.3 Member Data Documentation 316
11.120 rpki.left_right.list_resources_elt Class Reference 317
11.120.1 Detailed Description 319
11.120.2 Member Function Documentation 319
11.120.3 Member Data Documentation 320
11.121 rpki.left_right.list_roa_requests_elt Class Reference 321
11.121.1 Detailed Description 322
11.121.2 Member Function Documentation 322
11.121.3 Member Data Documentation 322
11.122 rpki.left_right.msg Class Reference 323
11.122.1 Detailed Description 325
11.122.2 Member Function Documentation 325
11.122.3 Member Data Documentation 325
11.123 rpki.left_right.parent_elt Class Reference 326
11.123.1 Detailed Description 328
11.123.2 Member Function Documentation 328
11.123.3 Member Data Documentation 330
11.124 rpki.left_right.report_error_elt Class Reference 332
11.124.1 Detailed Description 334
11.124.2 Member Function Documentation 334
11.124.3 Member Data Documentation 335
11.125 rpki.left_right.repository_elt Class Reference 336
11.125.1 Detailed Description 338
11.125.2 Member Function Documentation 338
11.125.3 Member Data Documentation 339
11.126 rpki.left_right.sax_handler Class Reference 340
11.126.1 Detailed Description 342
11.126.2 Member Data Documentation 342
11.127 rpki.left_right.self_elt Class Reference 342
11.127.1 Detailed Description 345
11.127.2 Member Function Documentation 345

11.127.3 Member Data Documentation 349
11.128 rpki.log.logger Class Reference 351
11.128.1 Detailed Description 352
11.128.2 Member Function Documentation 352
11.128.3 Member Data Documentation 352
11.129 rpki.manifest.FileAndHash Class Reference 353
11.129.1 Detailed Description 353
11.129.2 Member Function Documentation 354
11.129.3 Member Data Documentation 354
11.130 rpki.manifest.FilesAndHashes Class Reference 354
11.130.1 Detailed Description 355
11.130.2 Member Function Documentation 355
11.131 rpki.manifest.Manifest Class Reference 356
11.131.1 Detailed Description 357
11.131.2 Member Function Documentation 357
11.131.3 Member Data Documentation 357
11.132 rpki.publication.certificate_elt Class Reference 358
11.132.1 Detailed Description 360
11.132.2 Member Data Documentation 360
11.133 rpki.publication.client_elt Class Reference 360
11.133.1 Detailed Description 362
11.133.2 Member Function Documentation 362
11.133.3 Member Data Documentation 363
11.134 rpki.publication.cms_msg Class Reference 365
11.134.1 Detailed Description 367
11.134.2 Member Data Documentation 367
11.135 rpki.publication.config_elt Class Reference 367
11.135.1 Detailed Description 369
11.135.2 Member Function Documentation 369
11.135.3 Member Data Documentation 370
11.136 rpki.publication.control_elt Class Reference 371

11.136.1 Detailed Description 374
11.136.2 Member Function Documentation 374
11.137 rpki.publication.crl_elt Class Reference 374
11.137.1 Detailed Description 376
11.137.2 Member Data Documentation 376
11.138 rpki.publication.manifest_elt Class Reference 376
11.138.1 Detailed Description 378
11.138.2 Member Data Documentation 378
11.139 rpki.publication.msg Class Reference 378
11.139.1 Detailed Description 380
11.139.2 Member Function Documentation 380
11.139.3 Member Data Documentation 380
11.140 rpki.publication.publication_namespace Class Reference 381
11.140.1 Detailed Description 381
11.140.2 Member Data Documentation 382
11.141 rpki.publication.publication_object_elt Class Reference 382
11.141.1 Detailed Description 384
11.141.2 Member Function Documentation 384
11.141.3 Member Data Documentation 386
11.142 rpki.publication.report_error_elt Class Reference 387
11.142.1 Detailed Description 389
11.142.2 Member Function Documentation 389
11.142.3 Member Data Documentation 390
11.143 rpki.publication.roa_elt Class Reference 391
11.143.1 Detailed Description 393
11.143.2 Member Data Documentation 393
11.144 rpki.publication.sax_handler Class Reference 393
11.144.1 Detailed Description 395
11.144.2 Member Data Documentation 395
11.145 rpki.resource_set.resource_bag Class Reference 395
11.145.1 Detailed Description 397

11.145.2 Member Function Documentation 397
11.145.3 Member Data Documentation 399
11.146 rpki.resource_set.resource_range Class Reference 400
11.146.1 Detailed Description 401
11.146.2 Member Function Documentation 401
11.146.3 Member Data Documentation 401
11.147 rpki.resource_set.resource_range_as Class Reference 402
11.147.1 Detailed Description 403
11.147.2 Member Function Documentation 403
11.147.3 Member Data Documentation 403
11.148 rpki.resource_set.resource_range_ip Class Reference 404
11.148.1 Detailed Description 406
11.148.2 Member Function Documentation 406
11.149 rpki.resource_set.resource_range_ipv4 Class Reference 407
11.149.1 Detailed Description 409
11.149.2 Member Data Documentation 409
11.150 rpki.resource_set.resource_range_ipv6 Class Reference 409
11.150.1 Detailed Description 411
11.150.2 Member Data Documentation 411
11.151 rpki.resource_set.resource_set Class Reference 411
11.151.1 Detailed Description 413
11.151.2 Member Function Documentation 413
11.151.3 Member Data Documentation 415
11.152 rpki.resource_set.resource_set_as Class Reference 416
11.152.1 Detailed Description 417
11.152.2 Member Function Documentation 417
11.152.3 Member Data Documentation 418
11.153 rpki.resource_set.resource_set_ip Class Reference 418
11.153.1 Detailed Description 420
11.153.2 Member Function Documentation 420
11.153.3 Member Data Documentation 421

11.154 rpki.resource_set.resource_set_ipv4 Class Reference 421
11.154.1 Detailed Description 423
11.154.2 Member Data Documentation 423
11.155 rpki.resource_set.resource_set_ipv6 Class Reference 423
11.155.1 Detailed Description 425
11.155.2 Member Data Documentation 425
11.156 rpki.resource_set.roa_prefix Class Reference 425
11.156.1 Detailed Description 427
11.156.2 Member Function Documentation 427
11.156.3 Member Data Documentation 428
11.157 rpki.resource_set.roa_prefix_ipv4 Class Reference 429
11.157.1 Detailed Description 431
11.157.2 Member Data Documentation 431
11.158 rpki.resource_set.roa_prefix_ipv6 Class Reference 431
11.158.1 Detailed Description 433
11.158.2 Member Data Documentation 433
11.159 rpki.resource_set.roa_prefix_set Class Reference 433
11.159.1 Detailed Description 434
11.159.2 Member Function Documentation 435
11.160 rpki.resource_set.roa_prefix_set_ipv4 Class Reference 436
11.160.1 Detailed Description 438
11.160.2 Member Data Documentation 438
11.161 rpki.resource_set.roa_prefix_set_ipv6 Class Reference 438
11.161.1 Detailed Description 440
11.161.2 Member Data Documentation 440
11.162 rpki.roa.ROAIPAddress Class Reference 440
11.162.1 Detailed Description 441
11.162.2 Member Function Documentation 441
11.162.3 Member Data Documentation 442
11.163 rpki.roa.ROAIPAddresses Class Reference 442
11.163.1 Detailed Description 443

11.163.2 Member Function Documentation 443
11.164 rpki.roa.ROAIPAddressFamilies Class Reference 443
11.164.1 Detailed Description 444
11.164.2 Member Function Documentation 444
11.165 rpki.roa.ROAIPAddressFamily Class Reference 444
11.165.1 Detailed Description 445
11.165.2 Member Function Documentation 445
11.165.3 Member Data Documentation 446
11.166 rpki.roa.RouteOriginAttestation Class Reference 446
11.166.1 Detailed Description 447
11.166.2 Member Function Documentation 447
11.166.3 Member Data Documentation 447
11.167 rpki.rpki_engine.ca_detail_obj Class Reference 448
11.167.1 Detailed Description 450
11.167.2 Member Function Documentation 451
11.167.3 Member Data Documentation 455
11.168 rpki.rpki_engine.ca_obj Class Reference 457
11.168.1 Detailed Description 459
11.168.2 Member Function Documentation 459
11.168.3 Member Data Documentation 463
11.169 rpki.rpki_engine.child_cert_obj Class Reference 464
11.169.1 Detailed Description 466
11.169.2 Member Function Documentation 466
11.169.3 Member Data Documentation 468
11.170 rpki.rpki_engine.publication_queue Class Reference 469
11.170.1 Detailed Description 471
11.170.2 Member Function Documentation 471
11.170.3 Member Data Documentation 472
11.171 rpki.rpki_engine.revoked_cert_obj Class Reference 473
11.171.1 Detailed Description 474
11.171.2 Member Function Documentation 474

11.171.3 Member Data Documentation 475
11.172 rpki.rpki_engine.roa_obj Class Reference 476
11.172.1 Detailed Description 478
11.172.2 Member Function Documentation 478
11.172.3 Member Data Documentation 481
11.173 rpki.rpki_engine.rpkid_context Class Reference 483
11.173.1 Detailed Description 485
11.173.2 Member Function Documentation 486
11.173.3 Member Data Documentation 488
11.174 rpki.sql.session Class Reference 491
11.174.1 Detailed Description 492
11.174.2 Member Function Documentation 493
11.174.3 Member Data Documentation 494
11.175 rpki.sql.sql_persistent Class Reference 496
11.175.1 Detailed Description 498
11.175.2 Member Function Documentation 498
11.175.3 Member Data Documentation 502
11.176 rpki.sql.template Class Reference 503
11.176.1 Detailed Description 505
11.176.2 Member Function Documentation 505
11.176.3 Member Data Documentation 505
11.177 rpki.sundial.datetime Class Reference 506
11.177.1 Detailed Description 508
11.177.2 Member Function Documentation 508
11.177.3 Member Data Documentation 512
11.178 rpki.sundial.timedelta Class Reference 512
11.178.1 Detailed Description 514
11.178.2 Member Function Documentation 515
11.178.3 Member Data Documentation 517
11.179 rpki.up_down.base_elt Class Reference 518
11.179.1 Detailed Description 519

11.179.2 Member Function Documentation 519
11.180 pki.up_down.certificate_elt Class Reference 520
11.180.1 Detailed Description 522
11.180.2 Member Function Documentation 522
11.180.3 Member Data Documentation 523
11.181 pki.up_down.class_elt Class Reference 523
11.181.1 Detailed Description 525
11.181.2 Member Function Documentation 525
11.181.3 Member Data Documentation 526
11.182 pki.up_down.class_response_syntax Class Reference 528
11.182.1 Detailed Description 529
11.182.2 Member Function Documentation 529
11.182.3 Member Data Documentation 530
11.183 pki.up_down.cms_msg Class Reference 530
11.183.1 Detailed Description 532
11.183.2 Member Data Documentation 532
11.184 pki.up_down.error_response_pdu Class Reference 532
11.184.1 Detailed Description 534
11.184.2 Member Function Documentation 534
11.184.3 Member Data Documentation 535
11.185 pki.up_down.issue_pdu Class Reference 536
11.185.1 Detailed Description 538
11.185.2 Member Function Documentation 538
11.185.3 Member Data Documentation 539
11.186 pki.up_down.issue_response_pdu Class Reference 540
11.186.1 Detailed Description 541
11.186.2 Member Function Documentation 542
11.187 pki.up_down.list_pdu Class Reference 542
11.187.1 Detailed Description 544
11.187.2 Member Function Documentation 544
11.188 pki.up_down.list_response_pdu Class Reference 545

11.188.1 Detailed Description 545
11.189 rpki.up_down.message_pdu Class Reference 546
11.189.1 Detailed Description 548
11.189.2 Member Function Documentation 548
11.189.3 Member Data Documentation 550
11.190 rpki.up_down.multi_uri Class Reference 551
11.190.1 Detailed Description 552
11.190.2 Member Function Documentation 552
11.191 rpki.up_down.revoke_pdu Class Reference 553
11.191.1 Detailed Description 555
11.191.2 Member Function Documentation 555
11.191.3 Member Data Documentation 556
11.192 rpki.up_down.revoke_response_pdu Class Reference 556
11.192.1 Detailed Description 557
11.193 rpki.up_down.revoke_syntax Class Reference 558
11.193.1 Detailed Description 559
11.193.2 Member Function Documentation 559
11.193.3 Member Data Documentation 559
11.194 rpki.up_down.sax_handler Class Reference 560
11.194.1 Detailed Description 562
11.194.2 Member Data Documentation 562
11.195 rpki.x509.CMS_object Class Reference 562
11.195.1 Detailed Description 565
11.195.2 Member Function Documentation 565
11.195.3 Member Data Documentation 566
11.196 rpki.x509.CRL Class Reference 569
11.196.1 Detailed Description 570
11.196.2 Member Function Documentation 570
11.196.3 Member Data Documentation 572
11.197 rpki.x509.DeadDrop Class Reference 573
11.197.1 Detailed Description 574

11.197.2 Member Function Documentation 574
11.197.3 Member Data Documentation 574
11.198 pki.x509.DER_CMS_object Class Reference 575
11.198.1 Detailed Description 576
11.198.2 Member Function Documentation 576
11.198.3 Member Data Documentation 576
11.199 pki.x509.DER_object Class Reference 577
11.199.1 Detailed Description 579
11.199.2 Member Function Documentation 579
11.199.3 Member Data Documentation 584
11.200 pki.x509.PEM_converter Class Reference 585
11.200.1 Detailed Description 586
11.200.2 Member Function Documentation 586
11.200.3 Member Data Documentation 587
11.201 pki.x509.PKCS10 Class Reference 587
11.201.1 Detailed Description 589
11.201.2 Member Function Documentation 589
11.201.3 Member Data Documentation 590
11.202 pki.x509.ROA Class Reference 591
11.202.1 Detailed Description 593
11.202.2 Member Function Documentation 593
11.202.3 Member Data Documentation 593
11.203 pki.x509.RSA Class Reference 594
11.203.1 Detailed Description 596
11.203.2 Member Function Documentation 596
11.203.3 Member Data Documentation 597
11.204 pki.x509.RSApublic Class Reference 598
11.204.1 Detailed Description 600
11.204.2 Member Function Documentation 600
11.204.3 Member Data Documentation 601
11.205 pki.x509.SignedManifest Class Reference 602

11.205.1 Detailed Description 603
11.205.2 Member Function Documentation 603
11.205.3 Member Data Documentation 604
11.206 rpki.x509.X509 Class Reference 604
11.206.1 Detailed Description 606
11.206.2 Member Function Documentation 606
11.206.3 Member Data Documentation 609
11.207 rpki.x509.XML_CMS_object Class Reference 610
11.207.1 Detailed Description 612
11.207.2 Member Function Documentation 612
11.207.3 Member Data Documentation 614
11.208 rpki.xml_utils.base_elt Class Reference 614
11.208.1 Detailed Description 616
11.208.2 Member Function Documentation 616
11.208.3 Member Data Documentation 618
11.209 rpki.xml_utils.data_elt Class Reference 619
11.209.1 Detailed Description 621
11.209.2 Member Function Documentation 621
11.210 rpki.xml_utils.msg Class Reference 624
11.210.1 Detailed Description 626
11.210.2 Member Function Documentation 626
11.210.3 Member Data Documentation 627
11.211 rpki.xml_utils.sax_handler Class Reference 628
11.211.1 Detailed Description 629
11.211.2 Member Function Documentation 629
11.211.3 Member Data Documentation 631
11.212 rpki.xml_utils.text_elt Class Reference 632
11.212.1 Detailed Description 633
11.212.2 Member Function Documentation 633
11.212.3 Member Data Documentation 633
11.213 Sequence Class Reference 634

11.214 SequenceOf Class Reference 634
11.215 TextWrapper Class Reference 634
11.216 ContentHandler Class Reference 634

12 File Documentation **635**
12.1 __doc__.py File Reference 635
12.1.1 Detailed Description 635
12.2 __init__.py File Reference 636
12.3 async.py File Reference 636
12.4 cli.py File Reference 636
12.5 config.py File Reference 637
12.6 exceptions.py File Reference 637
12.7 https.py File Reference 639
12.8 ipaddrs.py File Reference 640
12.9 irbe_cli.py File Reference 640
12.10 irdbd.py File Reference 642
12.11 left_right.py File Reference 642
12.12 log.py File Reference 643
12.13 manifest.py File Reference 644
12.14 oids.py File Reference 644
12.15 pubd.py File Reference 645
12.16 publication.py File Reference 645
12.17 relaxng.py File Reference 646
12.18 resource_set.py File Reference 646
12.19 roa.py File Reference 647
12.20 rootd.py File Reference 647
12.21 rpki_engine.py File Reference 649
12.22 rpkid.py File Reference 649
12.23 sql.py File Reference 650
12.24 sundial.py File Reference 650
12.25 up_down.py File Reference 650

12.26x509.py File Reference 651
12.27xml_utils.py File Reference 652

1 RPKI Engine Reference Manual

This collection of Python modules implements a prototype of the RPKI Engine. This is a work in progress.

See http://viewvc.hactrn.net/subvert-rpki.hactrn.net/ for code and design documents.

The RPKI Engine is an implementation of the production-side tools for generating certificates, CRLs, and ROAs. The relying party tools are a separate (and much simpler) package.

The Subversion repository for the entire project is available for (read-only) anonymous access at http://subvert-rpki.hactrn.net/.

The documentation you're reading is generated automatically by Doxygen from comments and documentation in the code.

Besides the automatically-generated code documentation, this manual also includes documentation of the overall package:

- The installation instructions
- The configuration instructions
- The operation instructions
- A description of the left-right protocol
- A description of the publication protocol
- A description of the BPKI model used to secure the up-down, left-right, and publication protocols
- A description of the several SQL database schemas
- Some suggestions for further reading

This work was funded from 2006 through 2008 by ARIN, in collaboration with the other Regional Internet Registries. Current work is funded by DHS.

2 Further Reading

If you're interested in this package you might also be interested in:

- The rcynic validation tool
- A live sample of rcynic's summary output
- APNIC's project Trac instance

3 Installation Guide

Installation instructions for rpkid et al.

These are the production-side RPKI tools, for Internet Registries (RIRs, LIRs, etc). See the "rcynic" program for relying party tools.

rpkid is a set of Python modules supporting generation and maintenance of resource certificates. Most of the code is in the rpkid/rpki/ directory. rpkid itself is a relatively small program that calls the library modules. There are several other programs that make use of the same libraries, as well as a collection of test programs.

At present the package is intended to be run out of its build directory. Setting up proper installation in a system area using the Python distutils package would likely not be very hard but has not yet been done.

Note that initial development of this code has been on FreeBSD, so installation will probably be easiest on FreeBSD.

Before attempting to build the package, you need to install any missing prerequisites. Note that the Python code requires Python version 2.5 or 2.6. rpkid et al are mostly self-contained, but do require a small number of external packages to run.

- If your Python installation does not already include the sources files needed to compile new Python extension modules, you will need to install whatever package does include those source files. The need for and name of this package varies from system to system. On FreeBSD, the base Python interpreter package includes the development sources; on at least some Linux distributions, you have to install a separate "python-devel" package or something similar. If you get compilation errors trying to build the POW code (below) and the error message says something about the file "Python.h" being missing, this is almost certainly your problem.
- http://codespeak.net/lxml/, a Pythonic interface to the Gnome LibXML2 libraries. lxml in turn requires the LibXML2 C libraries.

  - FreeBSD: /usr/ports/devel/py-lxml
  - Fedora: python-lxml.i386
  - Ubuntu: python-lxml

- http://sourceforge.net/projects/mysql-python/, the Python "db" interface to MySQL. MySQLdb in turn requires MySQL client and server. rpkid et al have been tested with MySQL 5.0 and 5.1.
  - FreeBSD: /usr/ports/databases/py-MySQLdb
  - Fedora: MySQL-python.i386
  - Ubuntu: python-mysqldb

rpkid et al also make heavy use of a modified copy of the Python OpenSSL Wrappers (POW) package, but this copy has enough modifications and additions that it's included in the subversion tree.

The next step is to build the OpenSSL and POW binaries. At present the OpenSSL code is just a snapshot of the OpenSSL development sources, compiled with special options to enable RFC 3779 support that ISC wrote under previous contract to ARIN. The POW (Python OpenSSL Wrapper) library is an extended copy of the stock POW release.

To build these, cd to the top-level directory in the distribution and type "make".

```
$ cd $top
$ make
```

This should automatically build everything, in the right order, including staticly linking the POW extension module with the OpenSSL library to provide RFC 3779 support. If you get errors building POW, see the above discussion of Python development sources.

The architecture is intended to support hardware signing modules (HSMs), but the code to support them has not been written.

At this point, you should have all the necessary software installed to run the core programs, but you will probably want to test it. The test suite requires a few more external packages, only one of which is Python code.

- http://pyyaml.org/. Several of the test programs use PyYAML to parse a YAML description of a simulated allocation hierarchy to test.
  - FreeBSD: /usr/ports/devel/py-yaml
  - Ubuntu: python-yaml
- http://xmlsoft.org/XSLT/. Some of the test code uses xsltproc, from the Gnome LibXSLT package.

  - FreeBSD: /usr/ports/textproc/libxslt
  - Ubuntu: xsltproc

All tests should be run from the rpkid/ or myrpki/ directories.

Some of the tests require MySQL databases to store their data. To set up all the databases that the tests will need, run the SQL commands in rpkid/smoketest.setup.sql. The MySQL command line client is usually the easiest way to do this, eg:

```
$ cd $top/rpkid
$ mysql -u root -p <smoketest.setup.sql
```

To run the tests, run "make all-tests":

```
$ cd $top/rpkid
$ make all-tests
```

If nothing explodes, your installation is probably ok. Any Python backtraces in the output indicate a problem.

There's a last set of tools that only developers should need, as they're only used when modifying schemas or regenerating the documentation. These tools are listed here for completeness.

- http://www.doxygen.org/. Doxygen in turn pulls in several other tools, notably Graphviz, pdfLaTeX, and Ghostscript.
  - FreeBSD: /usr/ports/devel/doxygen
  - Ubuntu: doxygen
- http://lynx.isc.org/current/. The documentation build process uses xsltproc and Lynx to dump flat text versions of a few critical documentation pages.
  - FreeBSD: /usr/ports/www/lynx
  - Ubuntu: lynx
- http://www.thaiopensource.com/relaxng/trang.html. Trang is used to convert RelaxNG schemas from the human-readable "compact" form to the XML form that LibXML2 understands. Trang in turn requires Java.
  - FreeBSD: /usr/ports/textproc/trang
- http://search.cpan.org/dist/SQL-Translator/. SQL-Translator, also known as "SQL Fairy", includes code to parse an SQL schema and dump a description of it as Graphviz input. SQL Fairy in turn requires Perl.

- FreeBSD: /usr/ports/databases/p5-SQL-Translator

Once you've finished with installation, the next thing you should read is the Configuration Guide.

4 Configuration Guide

This section describes the configuration file syntax and settings.

Each of the programs that make up the RPKI tookit can potentially take its own configuration file, but for most uses this is unnecessarily complicated. The recommended approach is to use a single configuration file, and to put all of the parameters that a normal user might need to change into a single section of that configuration file, then reference these common settings from the program-specific sections of the configuration file via macro expansion. The configuration file parser supports a limited version of the macro facility used in OpenSSL's configuration parser. An expression such as

```
foo = ${bar::baz}
```

sets foo to the value of the `baz` variable from section `bar`. The section name `ENV` is special: it refers to environment variables.

The default name for the shared configuration file is `myrpki.conf`.

```
[myrpki]
```

The [myrpki] section of `myrpki.conf` contains all the parameters that you really need to configure.

```
# Handle naming hosted resource-holding entity (<self/>) represented
# by this myrpki instance.  Syntax is an identifier (ASCII letters,
# digits, hyphen, underscore -- no whitespace, non-ASCII characters,
# or other punctuation).  You need to set this.

handle                          = Me
```

Every resource-holding or server-operating entity needs a "handle", which is just an identifier by which the entity calls itself. Handles do not need to be globally unique, but should be chosen with an eye towards debugging operational problems: it's best if you use a handle that your parents and children will recognize as being you.

Warning

The rest of this section of the configuration file isn't documented yet, beyond the comments already present in the example file.

```
# Names of various files and directories.  Don't change these without
# a good reason.

roa_csv                         = roas.csv
prefix_csv                      = prefixes.csv
asn_csv                         = asns.csv
xml_filename                    = myrpki.xml
bpki_resources_directory        = bpki/resources
bpki_servers_directory          = bpki/servers

# Whether you want to run your own copy of rpkid (and irdbd).  In
# general, if you're running myirbe.py at all, you want this on.

run_rpkid                       = true

# DNS hostname and server port numbers for rpkid and irdbd, if you're
# running them.  rpkid's server host has to be a publicly reachable
# name to be useful; irdbd's server host should always be localhost
# unless you really know what you are doing.  Port numbers can be any
# legal TCP port number that you're not using for something else.

rpkid_server_host               = rpkid.example.org
rpkid_server_port               = 4404
irdbd_server_host               = localhost
irdbd_server_port               = 4403

# Whether you want to run your own copy of pubd.  In general, it's
# best to use your parent's pubd if you can, to reduce the overall
# number of publication sites that relying parties need to check, so
# don't enable this unless you have a good reason.

run_pubd                        = true

# DNS hostname and server port number for pubd, if you're running it.
# Hostname has to be a publicly reachable name to be useful, port can
# be any legal TCP port number that you're not using for something
# else.

pubd_server_host                = pubd.example.org
pubd_server_port                = 4402

# Contact information to include in offers of repository service.
# This only matters when we're running pubd.  This should be a human
# readable string, perhaps containing an email address or URL.

pubd_contact_info               = repo-man@rpki.example.org

# Whether to offer repository service to our children.
# This only matters when we're running pubd.

pubd_offer_service_to_children  = false

# Whether you want to run your very own copy of rootd.  Don't enable
# this unless you really know what you're doing.

run_rootd                       = false
```

```
# Server port number for rootd, if you're running it.  This can be any
# legal TCP port number that you're not using for something else.

rootd_server_port               = 4401

# Root of local directory tree where pubd (and rootd, sigh) should
# write out published data.  You need to configure this, and the
# configuration should match up with the directory where you point
# rsyncd.  Neither pubd nor rsyncd much cares -where- you tell them to
# put this stuff, the important thing is that the rsync:// URIs in
# generated certificates match up with the published objects so that
# relying parties can find and verify rpkid's published outputs.

publication_base_directory      = publication/

# rsyncd module name corresponding to publication_base_directory.
# This has to match the module you configured into rsyncd.conf.
# Leave this alone unless you have some need to change it.

publication_rsync_module        = rpki

# Hostname and optional port number for rsync:// URIs.  In most cases
# this should just be the same value as pubd_server_host.

publication_rsync_server        = ${myrpki::pubd_server_host}

# SQL configuration.  You can ignore this if you're not running any of
# the daemons yourself.

# If you're comfortable with having all of the databases use the same
# MySQL username and password, set those values here.  It's ok to
# leave the default username alone, but you should use a locally
# generated password either here or in the individual settings below.

shared_sql_username             = rpki
shared_sql_password             = fnord

# If you want different usernames and passwords for the separate SQL
# databases, enter those settings here; the shared_sql_* settings are
# only referenced here, so you can remove them entirely if you're
# setting everything in this block.

rpkid_sql_database              = rpkid
rpkid_sql_username              = ${myrpki::shared_sql_username}
rpkid_sql_password              = ${myrpki::shared_sql_password}

irdbd_sql_database              = irdbd
irdbd_sql_username              = ${myrpki::shared_sql_username}
irdbd_sql_password              = ${myrpki::shared_sql_password}

pubd_sql_database               = pubd
pubd_sql_username               = ${myrpki::shared_sql_username}
pubd_sql_password               = ${myrpki::shared_sql_password}

# Name of OpenSSL binary.  You might need to change this if you have
# no system copy installed, or if the system copy doesn't support CMS.
```

```
# The copy of openssl built by this package should suffice.

openssl                         = openssl

# End of [myrpki] section
```

Once you've finished with configuration, the next thing you should read is the Operation Guide.

5 Operation Guide

Production-side RPKI tools, for Internet Registries (RIRs, LIRs, etc).

See rcynic/README for relying party tools.

Warning

> rpkid is still in development, and the code changes more often than the hand-maintained portions of this documentation. The following text was reasonably accurate at the time it was written but may be obsolete by the time you read it.

At present the package is intended to be run out of the `rpkid/` directory.

In addition to the library routines in the `rpkid/rpki/` directory, the package includes the following programs:

- `rpkid` : The main RPKI engine daemon.
- `pubd` : The publication engine daemon.
- `rootd` : A separate daemon for handling the root of an RPKI certificate tree. This is essentially a stripped down version of rpkid with no SQL database, no left-right protocol implementation, and only the parent side of the up-down protocol. It's separate because the root is a special case in several ways and it was simpler to keep the special cases out of the main daemon.
- `irdbd` : A sample implementation of an IR database daemon. rpkid calls into this to perform lookups via the left-right protocol.
- `irbe_cli` : A command-line client for the left-right control protocol. Very obscure syntax, badly needs rewriting.
- `smoketest` : A test tool for running a collection of rpkid and irdb instances under common control, driven by a unified test script.

- `yamltest` : Another test tool which takes the same input format as `smoketest.py`, but with slightly different purpose. `smoketest.py` is intended to support regression tests, while `yamltest.py` is intended for automated testing of something closer to a real operational environment. There's a fair amount of code duplication between the two, and at some point they will probably be merged into a single program that supports both modes of operation.

- `testpoke:` A simple client for the up-down protocol, mostly compatable with APNIC's rpki_poke.pl tool.

Most of these programs take configuration files in a common format similar to that used by the OpenSSL command line tool. The test programs also take input in YAML format to drive the tests. Runs of the `yamltest` test tool will generate a fairly complete set configuration files which may be useful as examples.

Basic operation consists of creating the appropriate MySQL databases, configuring relationships between parents and children and between publication clients and repositories, starting rpkid, pubd, rootd, and irdbd, and using the left-right and publication control protocols to set up rpkid's and pubd's internal state. All other operations should occur either as a result of cron events or as a result of incoming left-right and up-down protocol requests.

The core programs are all event-driven, and are (in theory) capable of supporting an arbitrary number of hosted RPKI engines to run in a single rpkid instance, up to the performance limits of the underlying hardware.

At present the daemon programs all run in foreground, that is, if one wants them to run in background one must do so manually, eg, using Bourne shell syntax:

```
$ python whatever.py &
$ echo >whatever.pid  "$!"
```

All of the daemons use syslog by default. To make them log to stderr instead, use the "-d" option.

5.1 Common Options

Some of the options that the several daemons take are common to all daemons. Which daemon they affect depends only on which sections of which config files they are in.

The first group of options are debugging flags, which can be set to "true" or "false". If not specified, default values will be chosen (generally false).

- `debug_http` Enable verbose http debug logging.

- `debug_tls_certs` Enable verbose logging about tls certs.

- `want_persistent_client` Enable http 1.1 persistence, client side.
- `want_persistent_server` Enable http 1.1 persistence, server side.
- `debug_cms_certs` Enable verbose logging about cms certs.
- `sql_debug` Enable verbose logging about sql operations.
- `gc_debug` Enable scary garbage collector debugging.
- `timer_debug` Enable verbose logging of timer system.

There are also a few options that allow you to save CMS messages for audit or debugging. The save format is a simple MIME encoding in a Maildir-format mailbox. The current options are very crude, at some point we may provide finer grain controls.

- `dump_outbound_cms` Dump messages we send to this mailbox.
- `dump_inbound_cms` Dump messages we receive to this mailbox.

5.2 rpkid

rpkid is the main RPKI engine daemon. Configuration of rpkid is a two step process: a config file to bootstrap rpkid to the point where it can speak using the left-right protocol, followed by dynamic configuration via the left-right protocol. In production use the latter stage would be handled by the IRBE stub; for test and develoment purposes it's handled by the `irbe_cli` command line interface or by the smoketest test framework.

rpkid stores dynamic data in an SQL database, which must have been created for it, as explained in the installation guide.

The default config file is rpkid.conf, start rpkid with "-c filename" to choose a different config file. All options are in the section "[rpkid]". Certificates, keys, and trust anchors may be in either DER or PEM format.

Config file options:

- `startup-message`: String to log on startup, useful when debugging a collection of rpkid instances at once.
- `sql-username`: Username to hand to MySQL when connecting to rpkid's database.
- `sql-database`: MySQL's database name for rpkid's database.

- `sql-password`: Password to hand to MySQL when connecting to rpkid's database.

- `bpki-ta`: Name of file containing BPKI trust anchor. All BPKI certificate verification within rpkid traces back to this trust anchor.

- `rpkid-cert`: Name of file containing rpkid's own BPKI EE certificate.

- `rpkid-key`: Name of file containing RSA key corresponding to rpkid-cert.

- `irbe-cert`: Name of file containing BPKI certificate used by IRBE when talking to rpkid.

- `irdb-cert`: Name of file containing BPKI certificate used by irdbd.

- `irdb-url`: Service URL for irdbd. Must be a https:// URL.

- `server-host`: Hostname or IP address on which to listen for HTTPS connections. Current default is INADDR_ANY (IPv4 0.0.0.0); this will need to be hacked to support IPv6 for production.

- `server-port`: TCP port on which to listen for HTTPS connections.

5.3 pubd

pubd is the publication daemon. It implements the server side of the publication protocol, and is used by rpkid to publish the certificates and other objects that rpkid generates.

pubd is separate from rpkid for two reasons:

- The hosting model allows entities which choose to run their own copies of rpkid to publish their output under a common publication point. In general, encouraging shared publication services where practical is a good thing for relying parties, as it will speed up rcynic synchronization time.

- The publication server has to run on (or at least close to) the publication point itself, which in turn must be on a publically reachable server to be useful. rpkid, on the other hand, need only be reachable by the IRBE and its children in the RPKI tree. rpkid is a much more complex piece of software than pubd, so in some situations it might make sense to wrap tighter firewall constraints around rpkid than would be practical if rpkid and pubd were a single program.

pubd stores dynamic data in an SQL database, which must have been created for it, as explained in the installation guide. pubd also stores the published objects themselves as disk files in a configurable location which should correspond to an appropriate module definition in rsync.conf.

The default config file is pubd.conf, start pubd with "-c filename" to choose a different config file. ALl options are in the section "[pubd]". Certifiates, keys, and trust anchors may be either DER or PEM format.

Config file options:

- `sql-username`: Username to hand to MySQL when connecting to pubd's database.
- `sql-database`: MySQL's database name for pubd's database.
- `sql-password`: Password to hand to MySQL when connecting to pubd's database.
- `bpki-ta`: Name of file containing master BPKI trust anchor for pubd. All BPKI validation in pubd traces back to this trust anchor.
- `irbe-cert`: Name of file containing BPKI certificate used by IRBE when talking to pubd.
- `pubd-cert`: Name of file containing BPKI certificate used by pubd.
- `pubd-key`: Name of file containing RSA key corresponding to `pubd-cert`.
- `server-host`: Hostname or IP address on which to listen for HTTPS connections. Current default is INADDR_ANY (IPv4 0.0.0.0); this will need to be hacked to support IPv6 for production.
- `server-port`: TCP port on which to listen for HTTPS connections.
- `publication-base`: Path to base of filesystem tree where pubd should store publishable objects. Default is "publication/".

5.4 rootd

rootd is a stripped down implmenetation of (only) the server side of the up-down protocol. It's a separate program because the root certificate of an RPKI certificate tree requires special handling and may also require a special handling policy. rootd is a

simple implementation intended for test use, it's not suitable for use in a production system. All configuration comes via the config file.

The default config file is rootd.conf, start rootd with "-c filename" to choose a different config file. All options are in the section "[rootd]". Certificates, keys, and trust anchors may be in either DER or PEM format.

Config file options:

- `bpki-ta`: Name of file containing BPKI trust anchor. All BPKI certificate validation in rootd traces back to this trust anchor.
- `rootd-bpki-cert`: Name of file containing rootd's own BPKI certificate.
- `rootd-bpki-key`: Name of file containing RSA key corresponding to rootd-bpki-cert.
- `rootd-bpki-crl`: Name of file containing BPKI CRL that would cover rootd-bpki-cert had it been revoked.
- `child-bpki-cert`: Name of file containing BPKI certificate for rootd's one and only child (RPKI engine to which rootd issues an RPKI certificate).
- `server-host`: Hostname or IP address on which to listen for HTTPS connections. Default is localhost.
- `server-port`: TCP port on which to listen for HTTPS connections.
- `rpki-root-key`: Name of file containing RSA key to use in signing resource certificates.
- `rpki-root-cert`: Name of file containing self-signed root resource certificate corresponding to rpki-root-key.
- `rpki-root-dir`: Name of directory where rootd should write RPKI subject certificate, manifest, and CRL.
- `rpki-subject-cert`: Name of file that rootd should use to save the one and only certificate it issues. Default is "Subroot.cer".
- `rpki-root-crl`: Name of file to which rootd should save its RPKI CRL. Default is "Root.crl".
- `rpki-root-manifest`: Name of file to which rootd should save its RPKI manifest. Default is "Root.mnf".

- `rpki-subject-pkcs10`: Name of file that rootd should use when saving a copy of the received PKCS #10 request for a resource certificate. This is only used for debugging. Default is not to save the PKCS #10 request.

5.5 irdbd

irdbd is a sample implemntation of the server side of the IRDB callback subset of the left-right protocol. In production use this service is a function of the IRBE stub; irdbd may be suitable for production use in simple cases, but an IR with a complex IRDB may need to extend or rewrite irdbd.

irdbd requires a pre-populated database to represent the IR's customers. irdbd expects this database to use the SQL schema defined in rpkid/irdbd.sql. Once this database has been populated, the IRBE stub needs to create the appropriate objects in rpkid's database via the control subset of the left-right protocol, and store the linkage IDs (foreign keys into rpkid's database, basicly) in the IRDB.

irdbd's default config file is irdbd.conf, start irdbd with "-c filename" to choose a different config file. All options are in the section "[irdbd]". Certificates, keys, and trust anchors may be in either DER or PEM format.

Config file options:

- `startup-message`: String to log on startup, useful when debugging a collection of irdbd instances at once.
- `sql-username`: Username to hand to MySQL when connecting to irdbd's database.
- `sql-database`: MySQL's database name for irdbd's database.
- `sql-password`: Password to hand to MySQL when connecting to irdbd's database.
- `bpki-ta`: Name of file containing BPKI trust anchor. All BPKI certificate validation in irdbd traces back to this trust anchor.
- `irdbd-cert`: Name of file containing irdbd's own BPKI certificate.
- `irdbd-key`: Name of file containing RSA key corresponding to irdbd-cert.
- `rpkid-cert`: Name of file containing certificate used the one and only by rpkid instance authorized to contact this irdbd instance.
- `https-url`: Service URL for irdbd. Must be a https:// URL.

5.6 irbe_cli

irbe_cli is a simple command line client for the control subsets of the left-right and publication protocols. In production use this functionality would be part of the IRBE stub.

Basic configuration of irbe_cli is handled via a config file. The specific action or actions to be performed are specified on the command line, and map closely to the protocols themselves.

At present the user is assumed to be able to read the (XML) left-right and publication protocol messages, and with one exception, irdbd-cli makes no attempt to interpret the responses other than to check for signature and syntax errors. The one exception is that, if the `--pem_out` option is specified on the command line, any PKCS #10 requests received from rpkid will be written in PEM format to that file; this makes it easier to hand these requests off to the business PKI (BPKI in order to issue signing certs corresponding to newly generated business keys.

```
Command line IR back-end control program for rpkid and pubd.

$Id: irbe_cli.py 2799 2009-09-30 02:33:36Z sra $

Copyright (C) 2009  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Usage:

# Top-level options:
--config= --help --pem_out= --quiet --verbose
```

```
# left-right protocol:
parent --action= --tag= --self_handle= --parent_handle= --bsc_handle=
    --repository_handle= --peer_contact_uri= --sia_base=
    --sender_name= --recipient_name= --bpki_cms_cert= --bpki_cms_glue=
    --bpki_https_cert= --bpki_https_glue= --rekey --reissue --revoke
    --revoke_forgotten
repository --action= --tag= --self_handle= --repository_handle=
    --bsc_handle= --peer_contact_uri= --bpki_cert= --bpki_glue=
self --action= --tag= --self_handle= --crl_interval= --regen_margin=
    --bpki_cert= --bpki_glue= --rekey --reissue --revoke --run_now
    --publish_world_now --revoke_forgotten
child --action= --tag= --self_handle= --child_handle= --bsc_handle=
    --bpki_cert= --bpki_glue= --reissue
list_published_objects --self_handle= --tag=
bsc --action= --tag= --self_handle= --bsc_handle= --key_type=
    --hash_alg= --key_length= --signing_cert= --signing_cert_crl=
    --generate_keypair

# publication protocol:
certificate --action= --tag= --client_handle= --uri=
roa --action= --tag= --client_handle= --uri=
manifest --action= --tag= --client_handle= --uri=
client --action= --tag= --client_handle= --base_uri= --bpki_cert=
    --bpki_glue=
config --action= --tag= --bpki_crl=
crl --action= --tag= --client_handle= --uri=
```

Global options (`--config`, `--help`, `--pem_out`) come first, then zero or more commands (`parent`, `repository`, `self`, `child`, `bsc`, `config`, `client`), each followed by its own set of options. The commands map to elements in the protocols, and the command-specific options map to attributes or subelements for those commands.

`--tag` is an optional arbitrary tag (think IMAP) to simplify matching up replies with batched queries.

`--*_handle` options refer to object primary keys.

The remaining options are specific to the particular commands, and follow directly from the protocol specifications.

A trailing "=" in the above option summary indicates that an option takes a value, eg, "--action create" or "--action=create". Options without a trailing "=" correspond to boolean control attributes.

The default config file for irbe_cli is irbe_cli.conf, start irbe_cli with "-c filename" (or "--config filename") to choose a different config file. All options are in the section "[irbe_cli]". Certificates, keys, and trust anchors may be in either DER or PEM format.

Config file options:

- `rpkid-bpki-ta`: Name of file containing BPKI trust anchor to use when authenticating messages from rpkid.

- `rpkid-irbe-cert`: Name of file containing BPKI certificate irbe_cli should use when talking to rpkid.
- `rpkid-irbe-key`: Name of file containing RSA key corresponding to rpkid-irbe-cert.
- `rpkid-cert`: Name of file containing rpkid's BPKI certificate.
- `rpkid-url`: Service URL for rpkid. Must be a https:// URL.
- `pubd-bpki-ta`: Name of file containing BPKI trust anchor to use when authenticating messages from pubd.
- `pubd-irbe-cert`: Name of file containing BPKI certificate irbe_cli should use when talking to pubd.
- `pubd-irbe-key`: Name of file containing RSA key corresponding to pubd-irbe-cert.
- `pubd-cert`: Name of file containing pubd's BPKI certificate.
- `pubd-url`: Service URL for pubd. Must be a https:// URL.

5.7 cross_certify

cross_certify is a small tool to extract certain fields from an existing X.509 certificate and generate issue a new certificate that can be used as part of a cross-certification chain. cross_certify doesn't take a config file, all of its arguments are specified on the command line.

```
python cross_certify.py { -i | --in     } input_cert
                        { -c | --ca     } issuing_cert
                        { -k | --key    } issuing_cert_key
                        { -s | --serial } serial_filename
                        [ { -h | --help } ]
                        [ { -o | --out  }     filename ]
                        [ { -l | --lifetime } timedelta ]
```

5.8 cronjob

This is a trivial program to trigger a cron run within rpkid. Ordinarilly rpkid runs its own internal cron process, but for scripted testing it is sometimes useful to be able to control when cron cycles occur.

The default config file is cronjob.conf, start cronjob with "-c filename" to choose a different config file. All options are in the section "[cronjob]". Certificates, keys, and trust anchors may be in either DER or PEM format.

Config file options:

- `bpki-ta`: Name of file containing BPKI trust anchor.
- `irbe-cert`: Name of file containing cronjob's BPKI certificate.
- `https-key`: Name of file containing RSA key corresponding to irbe-cert.
- `rpkid-cert`: Name of file containing rpkid's BPKI certificate.
- `https-url`: Service URL for rpkid. Must be a https:// URL.

5.9 smoketest:

smoketest is a test harness to set up and run a collection of rpkid and irdbd instances under scripted control.

Unlike the programs described above, smoketest takes two configuration files in different languages. The first configuration file uses the same syntax as the above configuration files but is completely optional. The second configuration file is the test script, which is encoded using the YAML serialization language (see http://www.yaml.org/ for more information on YAML). The YAML script is not optional, as it describes the test layout. smoketest is designed to support running a fairly wide set of test configurations as canned scripts without writing any new control code. The intent is to make it possible to write meaningful regression tests.

All of the options in in the first (optional) configuration file are just overrides for wired-in default values. In most cases the defaults will suffice, and the set of options is still in flux, so only a few of the options are described here. The default name for this configuration file is smoketest.conf, run smoketest with "-c filename" to change it.

smoketest.conf options:

- `smoketest_dir`: Working directory into which smoketest should write the (many) files it generates. Default is "smoketest.dir".
- `irdb_db_pass`: MySQL password for the "irdb" user. Default is "fnord". You may want to override this.
- `rpki_db_pass`: MySQL password for the "rpki" user. Default is "fnord". You may want to override this.

- `rootd_sia:` rsync URI naming a (perhaps fictious) directory to use as the id-ad-caRepository SIA value in the generated root resource certificate. Default is "rsync://wombat.invalid/". You may want to override this if you intend to run an rsync server and test against the generated results using rcynic. This default will likely change if and when smoketest learns how to run rcynic itself as part of the test suite.

The second configuration file is named smoketest.yaml by default, run smoketest with "-y filename" to change it. The YAML file contains multiple YAML "documents". The first document describes the initial test layout and resource allocations, subsequent documents describe modifications to the initial allocations and other parameters. Resources listed in the initial layout are aggregated automatically, so that a node in the resource hierarchy automatically receives the resources it needs to issue whatever its children are listed as holding. Actions in the subsequent documents are modifications to the current resource set, modifications to validity dates or other non-resource parameters, or special commands like "sleep". The details are still evolving, but here's an example of current usage:

```
name:           RIR
valid_for:      2d
sia_base:       "rsync://wombat.invalid/"
kids:
  - name: LIR0
 kids:
   - name: Alice
     ipv4: 192.0.2.1-192.0.2.33
     asn:  64533
---
- name: Alice
  valid_add:   10
---
- name: Alice
  add_as: 33
  valid_add:   2d
---
- name: Alice
  valid_sub:   2d
---
- name: Alice
  valid_for:   10d
```

This specifies an initial layout consisting of an RPKI engine named "RIR", with one child "LIR0", which in turn has one child "Alice". Alice has a set of assigned resources, and all resources in the system are initially set to be valid for two days from the time at which the test is started. The first subsequent document adds ten seconds to the validity interval for Alice's resources and makes no other modifications. The second subsequent document grants Alice additional resources and adds another two days to the validity interval for Alice's resources. The next document subtracts two days from the validity interval for Alice's resources. The final document sets the validity interval for Alice's resources to ten days.

Operators in subsequent (update) documents:

- `add_as`, `add_v4`, `add_v6`: These add ASN, IPv4, or IPv6 resources, respectively.
- `sub_as`, `sub_v4`, `sub_v6`: These subtract resources.
- `valid_until`: Set an absolute expiration date.
- `valid_for`: Set a relative expiration date.
- `valid_add`, `valid_sub`: Add to or subtract from validity interval.
- `sleep` [interval]: Sleep for specified interval, or until smoketest receives a SIGALRM signal.

Absolute timestamps should be in the form shown (UTC timestamp format as used in XML).

Intervals (`valid_add`, `valid_sub`, `valid_for`, `sleep`) are either integers, in which case they're interpreted as seconds, or are a string of the form "wD xH yM zS" where w, x, y, and z are integers and D, H, M, and S indicate days, hours, minutes, and seconds. In the latter case all of the fields are optional, but at least one must be specified. For example, "3D4H" means "three days plus four hours".

5.10 testpoke

This is a command-line client for the up-down protocol. Unlike all of the above programs, testpoke does not accept a config file in OpenSSL-compatable format at all. Instead, it is configured exclusively by a YAML script. testpoke's design was constrained by a desire to have it be compatable with APNIC's rpki_poke.pl tool, so that the two tools could use a common configuration language to simplify scripted testing. There are minor variations due to slightly different feature sets, but YAML files intended for one program will usually work with the other.

README for APNIC's tool describing the input language can be found at http://mirin.apnic.net/svn/rpki_-engine/branches/gary-poker/client/poke/README.

testpoke takes a simplified command line and uses only one YAML input file.

```
Usage: python testpoke.py [ { -y | --yaml }    configfile ]
                          [ { -r | --request } requestname ]
                          [ { -h | --help } ]
```

Default configuration file is testpoke.yaml, override with --yaml option.

The --request option specifies the specific command within the YAML file to execute.

Sample configuration file:

```
---
# Sample YAML configuration file for testpoke

version: 1
posturl: https://localhost:4433/up-down/1
recipient-id: wombat
sender-id: "1"

cms-cert-file: biz-certs/Frank-EE.cer
cms-key-file: biz-certs/Frank-EE.key
cms-ca-cert-file: biz-certs/Bob-Root.cer
cms-cert-chain-file: [ biz-certs/Frank-CA.cer ]

ssl-cert-file: biz-certs/Frank-EE.cer
ssl-key-file: biz-certs/Frank-EE.key
ssl-ca-cert-file: biz-certs/Bob-Root.cer

requests:
  list:
 type: list
  issue:
 type: issue
 class: 1
 sia: [ "rsync://bandicoot.invalid/some/where/" ]
  revoke:
 type: revoke
 class: 1
 ski: "CB5K6APY-4KcGAW9jaK_cVPXKX0"
```

testpoke adds one extension to the language described in APNIC's README: the cms-cert-chain-∗ and ssl-cert-chain-∗ options, which allow one to specify a chain of intermediate certificates to be presented in the CMS or TLS protocol. APNIC's initial implementation required direct knowledge of the issuing certificate (ie, it supported a maximum chain length of one); subsequent APNIC code changes have probably relaxed this restriction, and with luck APNIC has copied testpoke's syntax to express chains of intermediate certificates.

6 Left-right protocol

The left-right protocol is really two separate client/server protocols over separate channels between the RPKI engine and the IR back end (IRBE).

The IRBE is the client for one of the subprotocols, the RPKI engine is the client for the other.

6.1 Terminology

- *IRBE:* Internet Registry Back End
- *IRDB:* Internet Registry Data Base
- *BPKI:* Business PKI
- *RPKI:* Resource PKI

6.2 initiated by the IRBE

This part of the protcol uses a kind of message-passing. Each object that the RPKI engine knows about takes five messages: "create", "set", "get", "list", and "destroy". Actions which are not just data operations on objects are handled via an SNMP-like mechanism, as if they were fields to be set. For example, to generate a keypair one "sets" the "generate-keypair" field of a BSC object, even though there is no such field in the object itself as stored in SQL. This is a bit of a kludge, but the reason for doing it as if these were variables being set is to allow composite operations such as creating a BSC, populating all of its data fields, and generating a keypair, all as a single operation. With this model, that's trivial, otherwise it's at least two round trips.

Fields can be set in either "create" or "set" operations, the difference just being whether the object already exists. A "get" operation returns all visible fields of the object. A "list" operation returns a list containing what "get" would have returned on each of those objects.

Left-right protocol objects are encoded as signed CMS messages containing XML as eContent and using an eContentType OID of `id-ct-xml` (1.2.840.113549.1.9.16.1.28). These CMS messages are in turn passed as the data for HTTPS POST operations, with an HTTP content type of "application/x-rpki" for both the POST data and the response data.

All operations allow an optional "tag" attribute which can be any alphanumeric token. The main purpose of the tag attribute is to allow batching of multiple requests into a single PDU.

6.2.1 <self/> object

A `<self/>` object represents one virtual RPKI engine. In simple cases where the RPKI engine operator operates the engine only on their own behalf, there will only be one `<self/>` object, representing the engine operator's organization, but in environments where the engine operator hosts other entities, there will be one `<self/> object` per hosted entity (probably including the engine operator's own organization, considered as a hosted customer of itself).

Some of the RPKI engine's configured parameters and data are shared by all hosted entities, but most are tied to a specific `<self/>` object. Data which are shared by all hosted entities are referred to as "per-engine" data, data which are specific to a particular `<self/>` object are "per-self" data.

Since all other RPKI engine objects refer to a `<self/>` object via a "self_handle" value, one must create a `<self/>` object before one can usefully configure any other left-right protocol objects.

Every `<self/>` object has a self_handle attribute, which must be specified for the "create", "set", "get", and "destroy" actions.

Payload data which can be configured in a `<self/>` object:

- `use_hsm` (attribute): Whether to use a Hardware Signing Module. At present this option has no effect, as the implementation does not yet support HSMs.

- `crl_interval` (attribute): Positive integer representing the planned lifetime of an RPKI CRL for this `<self/>`, measured in seconds.

- `regen_margin` (attribute): Positive integer representing how long before expiration of an RPKI certificiate a new one should be generated, measured in seconds. At present this only affects the one-off EE certificates associated with ROAs.

- `bpki_cert` (element): BPKI CA certificate for this `<self/>`. This is used as part of the certificate chain when validating incoming TLS and CMS messages, and should be the issuer of cross-certification BPKI certificates used in `<repository/>`, `<parent/>`, and `<child/>` objects. If the bpki_glue certificate is in use (below), the bpki_cert certificate should be issued by the bpki_glue certificate; otherwise, the bpki_cert certificate should be issued by the per-engine bpki_ta certificate.

- `bpki_glue` (element): Another BPKI CA certificate for this `<self/>`, usually not needed. Certain pathological cross-certification cases require a two-certificate chain due to issuer name conflicts. If used, the bpki_glue certificate should be the issuer of the bpki_cert certificate and should be issued by the per-engine bpki_ta certificate; if not needed, the bpki_glue certificate should be left unset.

Control attributes that can be set to "yes" to force actions:

- `rekey:` Start a key rollover for every RPKI CA associated with every `<parent/>` object associated with this `<self/>` object. This is the first phase of a key rollover operation.

- `revoke`: Revoke any remaining certificates for any expired key associated with any RPKI CA for any `<parent/>` object associated with this `<self/>` object. This is the second (cleanup) phase for a key rollover operation; it's separate from the first phase to leave time for new RPKI certificates to propegate and be installed.

- `reissue`: Not implemented, may be removed from protocol. Original theory was that this operation would force reissuance of any object with a changed key, but as that happens automatically as part of the key rollover mechanism this operation seems unnecessary.

- `run_now`: Force immediate processing for all tasks associated with this `<self/>` object that would ordinarily be performed under cron. Not currently implemented.

- `publish_world_now`: Force (re)publication of every publishable object for this `<self/>` object. Not currently implemented. Intended to aid in recovery if RPKI engine and publication engine somehow get out of sync.

6.2.2 <bsc/> object

The `<bsc/>` ("business signing context") object represents all the BPKI data needed to sign outgoing CMS or HTTPS messages. Various other objects include pointers to a `<bsc/>` object. Whether a particular `<self/>` uses only one `<bsc/>` or multiple is a configuration decision based on external requirements: the RPKI engine code doesn't care, it just cares that, for any object representing a relationship for which it must sign messages, there be a `<bsc/>` object that it can use to produce that signature.

Every `<bsc/>` object has a bsc_handle, which must be specified for the "create", "get", "set", and "destroy" actions. Every `<bsc/>` also has a self_handle attribute which indicates the `<self/>` object with which this `<bsc/>` object is associated.

Payload data which can be configured in a `<isc/>` object:

- `signing_cert` (element): BPKI certificate to use when generating a signature.

- `signing_cert_crl` (element): CRL which would list signing_cert if it had been revoked.

Control attributes that can be set to "yes" to force actions:

- `generate_keypair`: Generate a new BPKI keypair and return a PKCS #10 certificate request. The resulting certificate, once issued, should be configured as this `<bsc/>` object's signing_cert.

Additional attributes which may be specified when specifying "generate_keypair":

- `key_type`: Type of BPKI keypair to generate. "rsa" is both the default and, at the moment, the only allowed value.
- `hash_alg`: Cryptographic hash algorithm to use with this keypair. "sha256" is both the default and, at the moment, the only allowed value.
- `key_length`: Length in bits of the keypair to be generated. "2048" is both the default and, at the moment, the only allowed value.

Replies to "create" and "set" actions that specify "generate-keypair" include a <bsc_-pkcs10/> element, as do replies to "get" and "list" actions for a `<bsc/>` object for which a "generate-keypair" command has been issued. The RPKI engine stores the PKCS #10 request, which allows the IRBE to reuse the request if and when it needs to reissue the corresponding BPKI signing certificate.

6.2.3 <parent/> object

The `<parent/>` object represents the RPKI engine's view of a particular parent of the current `<self/>` object in the up-down protocol. Due to the way that the resource hierarchy works, a given `<self/>` may obtain resources from multiple parents, but it will always have at least one; in the case of IANA or an RIR, the parent RPKI engine may be a trivial stub.

Every `<parent/>` object has a parent_handle, which must be specified for the "create", "get", "set", and "destroy" actions. Every `<parent/>` also has a self_handle attribute which indicates the `<self/>` object with which this `<parent/>` object is associated, a bsc_handle attribute indicating the `<bsc/>` object to be used when signing messages sent to this parent, and a repository_handle indicating the `<repository/>` object to be used when publishing issued by the certificate issued by this parent.

Payload data which can be configured in a `<parent/>` object:

- `peer_contact_uri` (attribute): HTTPS URI used to contact this parent.
- `sia_base` (attribute): The leading portion of an rsync URI that the RPKI engine should use when composing the publication URI for objects issued by the RPKI certificate issued by this parent.
- `sender_name` (attribute): Sender name to use in the up-down protocol when talking to this parent. The RPKI engine doesn't really care what this value is, but other implementations of the up-down protocol do care.

- `recipient_name` (attribute): Recipient name to use in the up-down protocol when talking to this parent. The RPKI engine doesn't really care what this value is, but other implementations of the up-down protocol do care.

- `bpki_cms_cert` (element): BPKI CMS CA certificate for this `<parent/>`. This is used as part of the certificate chain when validating incoming CMS messages If the bpki_cms_glue certificate is in use (below), the bpki_cms_-cert certificate should be issued by the bpki_cms_glue certificate; otherwise, the bpki_cms_cert certificate should be issued by the bpki_cert certificate in the `<self/>` object.

- `bpki_cms_glue` (element): Another BPKI CMS CA certificate for this `<parent/>`, usually not needed. Certain pathological cross-certification cases require a two-certificate chain due to issuer name conflicts. If used, the bpki_-cms_glue certificate should be the issuer of the bpki_cms_cert certificate and should be issued by the bpki_cert certificate in the `<self/>` object; if not needed, the bpki_cms_glue certificate should be left unset.

- `bpki_https_cert` (element): BPKI HTTPS CA certificate for this `<parent/>`. This is like the bpki_cms_cert object, only used for validating incoming TLS messages rather than CMS.

- `bpki_cms_glue` (element): Another BPKI HTTPS CA certificate for this `<parent/>`, usually not needed. This is like the bpki_cms_glue certificate, only used for validating incoming TLS messages rather than CMS.

Control attributes that can be set to "yes" to force actions:

- `rekey`: This is like the rekey command in the `<self/>` object, but limited to RPKI CAs under this parent.

- `reissue`: This is like the reissue command in the `<self/>` object, but limited to RPKI CAs under this parent.

- `revoke`: This is like the revoke command in the `<self/>` object, but limited to RPKI CAs under this parent.

6.2.4 <child/> object

The `<child/>` object represents the RPKI engine's view of particular child of the current `<self/>` in the up-down protocol.

Every `<child/>` object has a child_handle, which must be specified for the "create", "get", "set", and "destroy" actions. Every `<child/>` also has a self_handle

attribute which indicates the <self/> object with which this <child/> object is associated.

Payload data which can be configured in a <child/> object:

- bpki_cert (element): BPKI CA certificate for this <child/>. This is used as part of the certificate chain when validating incoming TLS and CMS messages. If the bpki_glue certificate is in use (below), the bpki_cert certificate should be issued by the bpki_glue certificate; otherwise, the bpki_cert certificate should be issued by the bpki_cert certificate in the <self/> object.

- bpki_glue (element): Another BPKI CA certificate for this <child/>, usually not needed. Certain pathological cross-certification cases require a two-certificate chain due to issuer name conflicts. If used, the bpki_glue certificate should be the issuer of the bpki_cert certificate and should be issued by the bpki_-cert certificate in the <self/> object; if not needed, the bpki_glue certificate should be left unset.

Control attributes that can be set to "yes" to force actions:

- reissue: Not implemented, may be removed from protocol.

6.2.5 <repository/> object

The <repository/> object represents the RPKI engine's view of a particular publication repository used by the current <self/> object.

Every <repository/> object has a repository_handle, which must be specified for the "create", "get", "set", and "destroy" actions. Every <repository/> also has a self_handle attribute which indicates the <self/> object with which this <repository/> object is associated.

Payload data which can be configured in a <repository/> object:

- peer_contact_uri (attribute): HTTPS URI used to contact this repository.

- bpki_cms_cert (element): BPKI CMS CA certificate for this <repository/>. This is used as part of the certificate chain when validating incoming CMS messages If the bpki_cms_glue certificate is in use (below), the bpki_cms_cert certificate should be issued by the bpki_cms_glue certificate; otherwise, the bpki_cms_cert certificate should be issued by the bpki_cert certificate in the <self/> object.

- bpki_cms_glue (element): Another BPKI CMS CA certificate for this <repository/>, usually not needed. Certain pathological cross-certification

cases require a two-certificate chain due to issuer name conflicts. If used, the bpki_cms_glue certificate should be the issuer of the bpki_cms_cert certificate and should be issued by the bpki_cert certificate in the <self/> object; if not needed, the bpki_cms_glue certificate should be left unset.

- bpki_https_cert (element): BPKI HTTPS CA certificate for this <repository/>. This is like the bpki_cms_cert object, only used for validating incoming TLS messages rather than CMS.

- bpki_cms_glue (element): Another BPKI HTTPS CA certificate for this <repository/>, usually not needed. This is like the bpki_cms_glue certificate, only used for validating incoming TLS messages rather than CMS.

At present there are no control attributes for <repository/> objects.

6.2.6 <route_origin/> object

This section is out-of-date. The <route_origin/> object has been replaced by the <list_roa_requests/> IRDB query, but the documentation for that hasn't been written yet.

The <route_origin/> object is a kind of prototype for a ROA. It contains all the information needed to generate a ROA once the RPKI engine obtains the appropriate RPKI certificates from its parent(s).

Note that a <route_origin/> object represents a ROA to be generated on behalf of <self/>, not on behalf of a <child/>. Thus, a hosted entity that has no children but which does need to generate ROAs would be represented by a hosted <self/> with no <child/> objects but one or more <route_origin/> objects. While lumping ROA generation in with the other RPKI engine activities may seem a little odd at first, it's a natural consequence of the design requirement that the RPKI daemon never transmit private keys across the network in any form; given this requirement, the RPKI engine that holds the private keys for an RPKI certificate must also be the engine which generates any ROAs that derive from that RPKI certificate.

The precise content of the <route_origin/> has changed over time as the underlying ROA specification has changed. The current implementation as of this writing matches what we expect to see in draft-ietf-sidr-roa-format-03, once it is issued. In particular, note that the exactMatch boolean from the -02 draft has been replaced by the prefix and maxLength encoding used in the -03 draft.

Payload data which can be configured in a <route_origin/> object:

- asn (attribute): Autonomous System Number (ASN) to place in the generated ROA. A single ROA can only grant authorization to a single ASN; multiple ASNs require multiple ROAs, thus multiple <route_origin/> objects.

- `ipv4` (attribute): List of IPv4 prefix and maxLength values, see below for format.
- `ipv6` (attribute): List of IPv6 prefix and maxLength values, see below for format.

Control attributes that can be set to "yes" to force actions:

- `suppress_publication`: Not implemented, may be removed from protocol.

The lists of IPv4 and IPv6 prefix and maxLength values are represented as comma-separated text strings, with no whitespace permitted. Each entry in such a string represents a single prefix/maxLength pair.

ABNF for these address lists:

```
<ROAIPAddress> ::= <address> "/" <prefixlen> [ "-" <max_prefixlen> ]
                     ; Where <max_prefixlen> defaults to the same
                     ; value as <prefixlen>.

<ROAIPAddressList> ::= <ROAIPAddress> *( "," <ROAIPAddress> )
```

For example, `"10.0.1.0/24-32,10.0.2.0/24"`, which is a shorthand form of `"10.0.1.0/24-32,10.0.2.0/24-24"`.

6.3 Operations initiated by the RPKI engine

The left-right protocol also includes queries from the RPKI engine back to the IRDB. These queries do not follow the message-passing pattern used in the IRBE-initiated part of the protocol. Instead, there's a single query back to the IRDB, with a corresponding response. The CMS and HTTPS encoding are the same as in the rest of the protocol, but the BPKI certificates will be different as the back-queries and responses form a separate communication channel.

6.3.1 <list_resources/> messages

The `<list_resources/>` query and response allow the RPKI engine to ask the IRDB for information about resources assigned to a particular child. The query must include both a `"self_handle"` attribute naming the `<self/>` that is making the request and also a `"child_handle"` attribute naming the child that is the subject of

the query. The query and response also allow an optional "tag" attribute of the same form used elsewhere in this protocol, to allow batching.

A <list_resources/> response includes the following attributes, along with the tag (if specified), self_handle, and child_handle copied from the request:

- valid_until: A timestamp indicating the date and time at which certificates generated by the RPKI engine for these data should expire. The timestamp is expressed as an XML xsd:dateTime, must be expressed in UTC, and must carry the "Z" suffix indicating UTC.

- asn: A list of autonomous sequence numbers, expressed as a comma-separated sequence of decimal integers with no whitespace.

- ipv4: A list of IPv4 address prefixes and ranges, expressed as a comma-separated list of prefixes and ranges with no whitespace. See below for format details.

- ipv6: A list of IPv6 address prefixes and ranges, expressed as a comma-separated list of prefixes and ranges with no whitespace. See below for format details.

Entries in a list of address prefixes and ranges can be either prefixes, which are written in the usual address/prefixlen notation, or ranges, which are expressed as a pair of addresses denoting the beginning and end of the range, written in ascending order separated by a single "-" character. This format is superficially similar to the format used for prefix and maxLength values in the <route_origin/> object, but the semantics differ: note in particular that <route_origin/> objects don't allow ranges, while <list_resources/> messages don't allow a maxLength specification.

6.4 Error handling

Error in this protocol are handled at two levels.

Since all messages in this protocol are conveyed over HTTPS connections, basic errors are indicated via the HTTP response code. 4xx and 5xx responses indicate that something bad happened. Errors that make it impossible to decode a query or encode a response are handled in this way.

Where possible, errors will result in a <report_error/> message which takes the place of the expected protocol response message. <report_error/> messages are CMS-signed XML messages like the rest of this protocol, and thus can be archived to provide an audit trail.

<report_error/> messages only appear in replies, never in queries. The <report_error/> message can appear on either the "forward" (IRBE as client of RPKI engine) or "back" (RPKI engine as client of IRDB) communication channel.

The `<report_error/>` message includes an optional `"tag"` attribute to assist in matching the error with a particular query when using batching, and also includes a `"self_handle"` attribute indicating the `<self/>` that issued the error.

The error itself is conveyed in the `error_code` (attribute). The value of this attribute is a token indicating the specific error that occurred. At present this will be the name of a Python exception; the production version of this protocol will nail down the allowed error tokens here, probably in the RelaxNG schema.

The body of the `<report_error/>` element itself is an optional text string; if present, this is debugging information. At present this capabilty is not used, debugging information goes to syslog.

7 Publication protocol

The publication protocol is really two separate client/server protocols, between different parties.

The first is a configuration protocol for an IRBE to use to configure a publication engine, the second is the interface by which authorized clients request publication of specific objects.

Much of the architecture of the publication protocol is borrowed from the left-right protocol: like the left-right protocol, the publication protocol uses CMS-wrapped XML over HTTPS with the same eContentType OID and the same HTTPS content-type, and the overall style of the XML messages is very similar to the left-right protocol. All operations allow an optional "tag" attribute to allow batching.

The publication engine operates a single HTTPS server which serves both of these subprotocols. The two subprotocols share a single server port, but use distinct URLs to allow demultiplexing.

7.1 Terminology

- *IRBE:* Internet Registry Back End
- *IRDB:* Internet Registry Data Base
- *BPKI:* Business PKI
- *RPKI:* Resource PKI

7.2 Publication control subprotocol

The control subprotocol reuses the message-passing design of the left-right protocol. Configured objects support the "create", "set", "get", "list", and "destroy" actions, or a subset thereof when the full set of actions doesn't make sense.

7.2.1 <config/> object

The <config/> object allows configuration of data that apply to the entire publication server rather than a particular client.

There is exactly one <config/> object in the publication server, and it only supports the "set" and "get" actions -- it cannot be created or destroyed.

Payload data which can be configured in a <config/> object:

- `bpki_crl` (element): This is the BPKI CRL used by the publication server when signing the CMS wrapper on responses in the publication subprotocol. As the CRL must be updated at regular intervals, it's not practical to restart the publication server when the BPKI CRL needs to be updated. The BPKI model doesn't require use of a BPKI CRL between the IRBE and the publication server, so we can use the publication control subprotocol to update the BPKI CRL.

7.2.2 <client/> object

The <client/> object represents one client authorized to use the publication server.

The <client/> object supports the full set of "create", "set", "get", "list", and "destroy" actions. Each client has a "client_handle" attribute, which is used in responses and must be specified in "create", "set", "get", or "destroy" actions.

Payload data which can be configured in a <client/> object:

- `base_uri` (attribute): This is the base URI below which this client is allowed to publish data. The publication server may impose additional constraints in the case of a child publishing beneath its parent.

- `bpki_cert` (element): BPKI CA certificate for this <client/>. This is used as part of the certificate chain when validating incoming TLS and CMS messages. If the bpki_glue certificate is in use (below), the bpki_cert certificate should be issued by the bpki_glue certificate; otherwise, the bpki_cert certificate should be issued by the publication engine's bpki_ta certificate.

- `bpki_glue` (element): Another BPKI CA certificate for this <client/>, usually not needed. Certain pathological cross-certification cases require a two-certificate chain due to issuer name conflicts. If used, the bpki_glue certificate

should be the issuer of the bpki_cert certificate and should be issued by the publication engine's bpki_ta certificate; if not needed, the bpki_glue certificate should be left unset.

7.3 Publication subprotocol

The publication subprotocol is structured somewhat differently from the publication control protocol. Objects in the publication subprotocol represent objects to be published or objects to be withdrawn from publication. Each kind of object supports two actions: "publish" and "withdraw". In each case the XML element representing hte object to be published or withdrawn has a "uri" attribute which contains the publication URI. For "publish" actions, the XML element body contains the DER object to be published, encoded in Base64; for "withdraw" actions, the XML element body is empty.

In theory, the detailed access control for each kind of object might be different. In practice, as of this writing, access control for all objects is a simple check that the client's `"base_uri"` is a leading substring of the publication URI. Details of why access control might need to become more complicated are discussed in a later section.

7.3.1 <certificate/> object

The <certificate/> object represents an RPKI certificate to be published or withdrawn.

7.3.2 <crl/> object

The <crl/> object represents an RPKI CRL to be published or withdrawn.

7.3.3 <manifest/> object

The <manifest/> object represents an RPKI publication manifest to be published or withdrawn.

Note that part of the reason for the batching support in the publication protocol is because *every* publication or withdrawal action requires a new manifest, thus every publication or withdrawal action will involve at least two objects.

7.3.4 <roa/> object

The <roa/> object represents a ROA to be published or withdrawn.

7.4 Error handling

Error in this protocol are handled at two levels.

Since all messages in this protocol are conveyed over HTTPS connections, basic errors are indicated via the HTTP response code. 4xx and 5xx responses indicate that something bad happened. Errors that make it impossible to decode a query or encode a response are handled in this way.

Where possible, errors will result in a <report_error/> message which takes the place of the expected protocol response message. <report_error/> messages are CMS-signed XML messages like the rest of this protocol, and thus can be archived to provide an audit trail.

<report_error/> messages only appear in replies, never in queries. The <report_error/> message can appear in both the control and publication subprotocols.

The <report_error/> message includes an optional `"tag"` attribute to assist in matching the error with a particular query when using batching.

The error itself is conveyed in the `error_code` (attribute). The value of this attribute is a token indicating the specific error that occurred. At present this will be the name of a Python exception; the production version of this protocol will nail down the allowed error tokens here, probably in the RelaxNG schema.

The body of the <report_error/> element itself is an optional text string; if present, this is debugging information. At present this capabilty is not used, debugging information goes to syslog.

7.5 Additional access control considerations.

As detailed above, the publication protocol is trivially simple. This glosses over two bits of potential complexity:

- In the case where parent and child are sharing a repository, we'd like to nest child under parent, because testing has demonstrated that even on relatively slow hardware the delays involved in setting up separate rsync connections tend to dominate synchronization time for relying parties.

- The repository operator might also want to do some checks to assure itself that what it's about to allow the RPKI engine to publish is not dangerous toxic waste.

The up-down protocol includes a mechanism by which a parent can suggest a publication URI to each of its children. The children are not required to accept this hint, and the children must make separate arrangements with the repository operator (who might or might not be the same as the entity that hosts the children's RPKI engine operations) to use the suggested publication point, but if everything works out, this al-

lows children to nest cleanly under their parents publication points, which helps reduce synchronization time for relying parties.

In this case, one could argue that the publication server is responsible for preventing one of its clients (the child in the above description) from stomping on data published by another of its clients (the parent in the above description). This goes beyond the basic access check and requires the publication server to determine whether the parent has given its consent for the child to publish under the parent. Since the RPKI certificate profile requires the child's publication point to be indicated in an SIA extension in a certificate issued by the parent to the child, the publication engine can infer this permission from the parent's issuance of a certificate to the child. Since, by definition, the parent also uses this publication server, this is an easy check, as the publication server should already have the parent's certificate available by the time it needs to check the child's certificate.

The previous paragraph only covers a "publish" action for a <certificate/> object. For "publish" actions on other objects, the publication server would need to trace permission back to the certificate issued by the parent; for "withdraw" actions, the publication server would have to perform the same checks it would perform for a "publish" action, using the current published data before withdrawing it. The latter in turn implies an ordering constraint on "withdraw" actions in order to preserve the data necessary for these access control decisions; as this may prove impractical, the publication server may probably need to make periodic sweeps over its published data looking for orphaned objects, but that's probably a good idea anyway.

Note that, in this publication model, any agreement that the repository makes to publish the RPKI engine's output is conditional upon the object to be published passing whatever access control checks the publication server imposes.

8 SQL database schemas

- rpkid database schema
- pubd database schema
- irdbd database schema

8.1 rpkid SQL schema

Figure 1: Diagram of rpkid.sql

```
-- $Id: rpkid.sql 2953 2010-01-15 02:50:16Z sra $

-- Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")
--
-- Permission to use, copy, modify, and distribute this software for any
-- purpose with or without fee is hereby granted, provided that the above
-- copyright notice and this permission notice appear in all copies.
--
-- THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
-- REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
-- AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
-- INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
-- LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
-- OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
-- PERFORMANCE OF THIS SOFTWARE.

-- Copyright (C) 2007-2008  American Registry for Internet Numbers ("ARIN")
--
-- Permission to use, copy, modify, and distribute this software for any
-- purpose with or without fee is hereby granted, provided that the above
-- copyright notice and this permission notice appear in all copies.
--
-- THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
-- REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
-- AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
-- INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
-- LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
-- OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
-- PERFORMANCE OF THIS SOFTWARE.

-- SQL objects needed by the RPKI engine (rpkid.py).

-- DROP TABLE commands must be in correct (reverse dependency) order
-- to satisfy FOREIGN KEY constraints.

DROP TABLE IF EXISTS roa_prefix;
DROP TABLE IF EXISTS roa;
DROP TABLE IF EXISTS revoked_cert;
DROP TABLE IF EXISTS child_cert;
DROP TABLE IF EXISTS child;
DROP TABLE IF EXISTS ca_detail;
DROP TABLE IF EXISTS ca;
DROP TABLE IF EXISTS parent;
DROP TABLE IF EXISTS repository;
DROP TABLE IF EXISTS bsc;
DROP TABLE IF EXISTS self;

CREATE TABLE self (
        self_id                 SERIAL NOT NULL,
        self_handle             VARCHAR(255) NOT NULL,
        use_hsm                 BOOLEAN NOT NULL DEFAULT FALSE,
        crl_interval            BIGINT UNSIGNED,
        regen_margin            BIGINT UNSIGNED,
        bpki_cert               LONGBLOB,
        bpki_glue               LONGBLOB,
        PRIMARY KEY             (self_id),
        UNIQUE                  (self_handle)
```

```
) ENGINE=InnoDB;

CREATE TABLE bsc (
        bsc_id                  SERIAL NOT NULL,
        bsc_handle              VARCHAR(255) NOT NULL,
        private_key_id          LONGBLOB,
        pkcs10_request          LONGBLOB,
        hash_alg                ENUM ('sha256'),
        signing_cert            LONGBLOB,
        signing_cert_crl        LONGBLOB,
        self_id                 BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (bsc_id),
        CONSTRAINT              bsc_self_id
        FOREIGN KEY             (self_id) REFERENCES self (self_id) ON DELETE CASCADE,
        UNIQUE                  (self_id, bsc_handle)
) ENGINE=InnoDB;

CREATE TABLE repository (
        repository_id           SERIAL NOT NULL,
        repository_handle       VARCHAR(255) NOT NULL,
        peer_contact_uri        TEXT,
        bpki_cert               LONGBLOB,
        bpki_glue               LONGBLOB,
        bsc_id                  BIGINT UNSIGNED NOT NULL,
        self_id                 BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (repository_id),
        CONSTRAINT              repository_self_id
        FOREIGN KEY             (self_id) REFERENCES self (self_id) ON DELETE CASCADE,
        CONSTRAINT              repository_bsc_id
        FOREIGN KEY             (bsc_id) REFERENCES bsc (bsc_id) ON DELETE CASCADE,
        UNIQUE                  (self_id, repository_handle)
) ENGINE=InnoDB;

CREATE TABLE parent (
        parent_id               SERIAL NOT NULL,
        parent_handle           VARCHAR(255) NOT NULL,
        bpki_cms_cert           LONGBLOB,
        bpki_cms_glue           LONGBLOB,
        bpki_https_cert         LONGBLOB,
        bpki_https_glue         LONGBLOB,
        peer_contact_uri        TEXT,
        sia_base                TEXT,
        sender_name             TEXT,
        recipient_name          TEXT,
        self_id                 BIGINT UNSIGNED NOT NULL,
        bsc_id                  BIGINT UNSIGNED NOT NULL,
        repository_id           BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (parent_id),
        CONSTRAINT              parent_repository_id
        FOREIGN KEY             (repository_id) REFERENCES repository (repository_id) ON DELETE CASC
        CONSTRAINT              parent_bsc_id
        FOREIGN KEY             (bsc_id) REFERENCES bsc (bsc_id) ON DELETE CASCADE,
        CONSTRAINT              parent_self_id
        FOREIGN KEY             (self_id) REFERENCES self (self_id) ON DELETE CASCADE,
        UNIQUE                  (self_id, parent_handle)
) ENGINE=InnoDB;
```

```
CREATE TABLE ca (
        ca_id                   SERIAL NOT NULL,
        last_crl_sn             BIGINT UNSIGNED NOT NULL,
        last_manifest_sn        BIGINT UNSIGNED NOT NULL,
        next_manifest_update    DATETIME,
        next_crl_update         DATETIME,
        last_issued_sn          BIGINT UNSIGNED NOT NULL,
        sia_uri                 TEXT,
        parent_resource_class   TEXT,
        parent_id               BIGINT UNSIGNED,
        PRIMARY KEY             (ca_id),
        CONSTRAINT              ca_parent_id
        FOREIGN KEY             (parent_id) REFERENCES parent (parent_id) ON DELETE CASCADE
) ENGINE=InnoDB;

CREATE TABLE ca_detail (
        ca_detail_id            SERIAL NOT NULL,
        public_key              LONGBLOB,
        private_key_id          LONGBLOB,
        latest_crl              LONGBLOB,
        crl_published           DATETIME,
        latest_ca_cert          LONGBLOB,
        manifest_private_key_id LONGBLOB,
        manifest_public_key     LONGBLOB,
        latest_manifest_cert    LONGBLOB,
        latest_manifest         LONGBLOB,
        manifest_published      DATETIME,
        state                   ENUM ('pending', 'active', 'deprecated', 'revoked') NOT NULL,
        ca_cert_uri             TEXT,
        ca_id                   BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (ca_detail_id),
        CONSTRAINT              ca_detail_ca_id
        FOREIGN KEY             (ca_id) REFERENCES ca (ca_id) ON DELETE CASCADE
) ENGINE=InnoDB;

CREATE TABLE child (
        child_id                SERIAL NOT NULL,
        child_handle            VARCHAR(255) NOT NULL,
        bpki_cert               LONGBLOB,
        bpki_glue               LONGBLOB,
        self_id                 BIGINT UNSIGNED NOT NULL,
        bsc_id                  BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (child_id),
        CONSTRAINT              child_bsc_id
        FOREIGN KEY             (bsc_id) REFERENCES bsc (bsc_id) ON DELETE CASCADE,
        CONSTRAINT              child_self_id
        FOREIGN KEY             (self_id) REFERENCES self (self_id) ON DELETE CASCADE,
        UNIQUE                  (self_id, child_handle)
) ENGINE=InnoDB;

CREATE TABLE child_cert (
        child_cert_id           SERIAL NOT NULL,
        cert                    LONGBLOB NOT NULL,
        published               DATETIME,
        ski                     TINYBLOB NOT NULL,
        child_id                BIGINT UNSIGNED NOT NULL,
        ca_detail_id            BIGINT UNSIGNED NOT NULL,
```

```
        PRIMARY KEY             (child_cert_id),
        CONSTRAINT              child_cert_ca_detail_id
        FOREIGN KEY             (ca_detail_id) REFERENCES ca_detail (ca_detail_id) ON DELETE CASCADE
        CONSTRAINT              child_cert_child_id
        FOREIGN KEY             (child_id) REFERENCES child (child_id) ON DELETE CASCADE
) ENGINE=InnoDB;

CREATE TABLE revoked_cert (
        revoked_cert_id         SERIAL NOT NULL,
        serial                  BIGINT UNSIGNED NOT NULL,
        revoked                 DATETIME NOT NULL,
        expires                 DATETIME NOT NULL,
        ca_detail_id            BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (revoked_cert_id),
        CONSTRAINT              revoked_cert_ca_detail_id
        FOREIGN KEY             (ca_detail_id) REFERENCES ca_detail (ca_detail_id) ON DELETE CASCADE
) ENGINE=InnoDB;

CREATE TABLE roa (
        roa_id                  SERIAL NOT NULL,
        asn                     BIGINT UNSIGNED,
        cert                    LONGBLOB,
        roa                     LONGBLOB,
        published               DATETIME,
        self_id                 BIGINT UNSIGNED NOT NULL,
        ca_detail_id            BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (roa_id),
        CONSTRAINT              roa_self_id
        FOREIGN KEY             (self_id) REFERENCES self (self_id) ON DELETE CASCADE,
        CONSTRAINT              roa_ca_detail_id
        FOREIGN KEY             (ca_detail_id) REFERENCES ca_detail (ca_detail_id) ON DELETE CASCADE
) ENGINE=InnoDB;

CREATE TABLE roa_prefix (
        prefix                  VARCHAR(40) NOT NULL,
        prefixlen               TINYINT UNSIGNED NOT NULL,
        max_prefixlen           TINYINT UNSIGNED NOT NULL,
        version                 TINYINT UNSIGNED NOT NULL,
        roa_id                  BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (roa_id, prefix, prefixlen, max_prefixlen),
        CONSTRAINT              roa_prefix_roa_id
        FOREIGN KEY             (roa_id) REFERENCES roa (roa_id) ON DELETE CASCADE
) ENGINE=InnoDB;

-- Local Variables:
-- indent-tabs-mode: nil
-- End:
```

8.2 pubd SQL Schema

Figure 2: Diagram of pubd.sql

```
-- $Id: pubd.sql 2953 2010-01-15 02:50:16Z sra $

-- Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")
--
-- Permission to use, copy, modify, and distribute this software for any
-- purpose with or without fee is hereby granted, provided that the above
-- copyright notice and this permission notice appear in all copies.
--
-- THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
-- REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
-- AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
-- INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
-- LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
-- OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
-- PERFORMANCE OF THIS SOFTWARE.

-- Copyright (C) 2008  American Registry for Internet Numbers ("ARIN")
--
-- Permission to use, copy, modify, and distribute this software for any
-- purpose with or without fee is hereby granted, provided that the above
-- copyright notice and this permission notice appear in all copies.
--
-- THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
-- REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
-- AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
-- INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
-- LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
-- OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
-- PERFORMANCE OF THIS SOFTWARE.

-- SQL objects needed by pubd.py.

-- The config table is weird because we're really only using it
-- to store one BPKI CRL, but putting this here lets us use a lot of
-- existing machinery and the alternatives are whacky in other ways.

DROP TABLE IF EXISTS client;
```

```
DROP TABLE IF EXISTS config;

CREATE TABLE config (
        config_id       SERIAL NOT NULL,
        bpki_crl        LONGBLOB,
        PRIMARY KEY     (config_id)
) ENGINE=InnoDB;

CREATE TABLE client (
        client_id       SERIAL NOT NULL,
        client_handle   VARCHAR(255) NOT NULL,
        base_uri        TEXT,
        bpki_cert       LONGBLOB,
        bpki_glue       LONGBLOB,
        PRIMARY KEY     (client_id),
        UNIQUE          (client_handle)
) ENGINE=InnoDB;

-- Local Variables:
-- indent-tabs-mode: nil
-- End:
```

8.3 irdbd SQL Schema

Figure 3: Diagram of irdbd.sql

```
-- $Id: irdbd.sql 2953 2010-01-15 02:50:16Z sra $

-- Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")
--
-- Permission to use, copy, modify, and distribute this software for any
-- purpose with or without fee is hereby granted, provided that the above
-- copyright notice and this permission notice appear in all copies.
--
-- THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
-- REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
```

```
-- AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
-- INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
-- LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
-- OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
-- PERFORMANCE OF THIS SOFTWARE.

-- Copyright (C) 2007-2008  American Registry for Internet Numbers ("ARIN")
--
-- Permission to use, copy, modify, and distribute this software for any
-- purpose with or without fee is hereby granted, provided that the above
-- copyright notice and this permission notice appear in all copies.
--
-- THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
-- REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
-- AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
-- INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
-- LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
-- OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
-- PERFORMANCE OF THIS SOFTWARE.

-- SQL objects needed by irdbd.py.  You only need this if you're using
-- irdbd.py as your IRDB; if you have a "real" backend you can do
-- anything you like so long as you implement the relevant portion of
-- the left-right protocol.

-- DROP TABLE commands must be in correct (reverse dependency) order
-- to satisfy FOREIGN KEY constraints.

DROP TABLE IF EXISTS roa_request_prefix;
DROP TABLE IF EXISTS roa_request;
DROP TABLE IF EXISTS registrant_net;
DROP TABLE IF EXISTS registrant_asn;
DROP TABLE IF EXISTS registrant;

CREATE TABLE registrant (
        registrant_id           SERIAL NOT NULL,
        registrant_handle       VARCHAR(255) NOT NULL,
        registrant_name         TEXT,
        registry_handle         VARCHAR(255),
        valid_until             DATETIME NOT NULL,
        PRIMARY KEY             (registrant_id),
        UNIQUE                  (registry_handle, registrant_handle)
) ENGINE=InnoDB;

CREATE TABLE registrant_asn (
        registrant_asn_id       SERIAL NOT NULL,
        start_as                BIGINT UNSIGNED NOT NULL,
        end_as                  BIGINT UNSIGNED NOT NULL,
        registrant_id           BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (registrant_asn_id),
        CONSTRAINT              registrant_asn_registrant_id
        FOREIGN KEY             (registrant_id) REFERENCES registrant (registrant_id) ON DELETE CASC
) ENGINE=InnoDB;

CREATE TABLE registrant_net (
        registrant_net_id       SERIAL NOT NULL,
        start_ip                VARCHAR(40) NOT NULL,
```

```
        end_ip                  VARCHAR(40) NOT NULL,
        version                 TINYINT UNSIGNED NOT NULL,
        registrant_id           BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (registrant_net_id),
        CONSTRAINT              registrant_net_registrant_id
        FOREIGN KEY             (registrant_id) REFERENCES registrant (registrant_id) ON DELETE CASC
) ENGINE=InnoDB;

CREATE TABLE roa_request (
        roa_request_id          SERIAL NOT NULL,
        roa_request_handle      VARCHAR(255) NOT NULL,
        asn                     BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (roa_request_id)
) ENGINE=InnoDB;

CREATE TABLE roa_request_prefix (
        prefix                  VARCHAR(40) NOT NULL,
        prefixlen               TINYINT UNSIGNED NOT NULL,
        max_prefixlen           TINYINT UNSIGNED NOT NULL,
        version                 TINYINT UNSIGNED NOT NULL,
        roa_request_id          BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (roa_request_id, prefix, prefixlen, max_prefixlen),
        CONSTRAINT              roa_request_prefix_roa_request_id
        FOREIGN KEY             (roa_request_id) REFERENCES roa_request (roa_request_id) ON DELETE C
) ENGINE=InnoDB;

-- Local Variables:
-- indent-tabs-mode: nil
-- End:
```

9 BPKI model

The "business PKI" (BPKI) is the PKI used to authenticate communication on the up-down, left-right, and publication protocols.

BPKI certificates are *not* resource PKI (RPKI) certificates. The BPKI is a separate PKI that represents relationships between the various entities involved in the production side of the RPKI system. In most cases the BPKI tree will follow existing business relationships, hence the name "BPKI".

Setup of the BPKI is handled by the back end; for the most part, rpkid and pubd just use the result. The one place where the engines are directly involved in creation of new BPKI certificates is in the production of end-entity certificates for use by the engines.

There are a few design principals that underly the chosen BPKI model:

- Each engine should rely on a single BPKI trust anchor which is controlled by the back end entity that runs the engine; all other trust material should be cross-certified into the engine's BPKI tree.
- Private keys must never transit the network.

- Except for end entity certificates, the engine should only have access to the BPKI certificates; in particular, the private key for the BPKI trust anchor should not be accessible to the engine.
- The number of BPKI keys and certificates that the engine has to manage should be no larger than is necessary.

rpkid's hosting model adds an additional constraint: rpkid's BPKI trust anchor belongs to the entity operating rpkid, but the entities hosted by rpkid should have control of their own BPKI private keys. This implies the need for an additional layer of BPKI certificate hierarchy within rpkid.

Here is a simplified picture of what the BPKI might look like for an rpkid operator that hosts two entities, "Alice" and "Ellen":

Black objects belong to the hosting entity, blue objects belong to the hosted entities, red objects are cross-certified objects from the hosted entities' peers. The arrows indicate certificate issuance: solid arrows are the ones that rpkid will care about during certificate validation, dotted arrows show the origin of the EE certificates that rpkid uses to sign CMS and TLS messages.

There's one nasty bit where the model had to bend to fit the current state of the underlying protocols: it's not possible to use exactly the same BPKI keys and certificates for HTTPS and CMS. The reason for this is simple: each hosted entity has its own BPKI, as does the hosting entity, but the HTTPS listener is shared. The only ways to avoid sharing the HTTPS server certificate would be to use separate listeners for each hosted entity, which scales poorly, or to rely on the TLS "Server Name Indication" extension (RFC 4366 3.1) which is not yet widely implemented.

The certificate tree looks complicated, but the set of certificates needed to build any particular validation chain is obvious, again excepting the HTTPS server case, where the client certificate is the first hint that the engine has of the client's identity, so the server must be prepared to accept any current client certificate.

Detailed instructions on how to build a BPKI are beyond the scope of this document, but one can handle simple cases using the OpenSSL command line tool and cross_-certify; the latter is a tool designed specifically for the purpose of generating the cross-certification certificates needed to splice foreign trust material into a BPKI tree.

The BPKI tree for a pubd instance is similar to to the BPKI tree for an rpkid instance, but is a bit simpler, as pubd does not provide hosting in the same sense that rpkid does:

pubd is a relatively simple server that publishes objects as instructed by its clients.

Here's a simplified picture of what the BPKI might look like for a pubd operator that serves two clients, "Alice" and "Bob":

While it is likely that RIRs (at least) will operate both rpkid and pubd instances, the two functions are conceptually separate. As far as pubd is concerned, it doesn't matter who operates the rpkid instance: pubd just has clients, each of which has trust material that has been cross-certified into pubd's BPKI. Similarly, rpkid doesn't really care who operates a pubd instance that it's been configured to use, it just treats that pubd as a foreign BPKI whose trust material has to be cross-certified into its own BPKI. Cross certification itself is done by the back end operator, using cross_certify or some equivalent tool; the resulting BPKI certificates are configured into rpkid and pubd via the left-right protocol and the control subprotocol of the publication protocol, respectively.

Because the BPKI tree is almost entirely controlled by the operating entity, CRLs are not necessary for most of the BPKI. The one exception to this is the EE certificates issued under the cross-certification points. These EE certificates are generated by the peer, not the local operator, and thus require CRLs. Because of this, both rpkid and pubd require regular updates of certain BPKI CRLs, again via the left-right and publication control protocols.

Because the left-right protocol and the publication control subprotocol are used to configure BPKI certificates and CRLs, they cannot themselves use certificates and CRLs configured in this way. This is why the configuration files for rpkid and pubd require static configuration of the left-right and publication control certificates.

10 Namespace Documentation

10.1 Package irbe_cli

Classes

- class bsc_elt
- class certificate_elt
- class child_elt
- class client_elt
- class cmd_elt_mixin
- class cmd_msg_mixin
- class config_elt
- class crl_elt
- class left_right_cms_msg
- class left_right_msg
- class left_right_proto
- class left_right_sax_handler
- class list_published_objects_elt
- class list_received_resources_elt
- class manifest_elt
- class parent_elt
- class publication_cms_msg
- class publication_msg
- class publication_proto
- class publication_sax_handler
- class reply_elt_mixin
- class report_error_elt
- class repository_elt
- class roa_elt
- class self_elt
- class UsageWrapper

Functions

- def usage

Variables

- list argv = sys.argv[1:]
- tuple call_pubd
- tuple call_rpkid
- tuple cfg = rpki.config.parser(cfg_file, "irbe_cli")
- string cfg_file = "irbe.conf"
- pem_out = None
- q_msg = q_msg_left_right
- list q_msg_left_right = [ ]
- list q_msg_publication = [ ]
- list q_pdu = left_right_msg.pdus[argv[0]]
- list top_opts = ["config=", "help", "pem_out=", "quiet", "verbose"]
- tuple usage_fill = UsageWrapper(subsequent_indent = " " ∗ 4)
- verbose = True

10.1.1 Detailed Description

```
Command line IR back-end control program for rpkid and pubd.

$Id: irbe_cli.py 3107 2010-03-16 23:13:08Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

10.1.2 Function Documentation

10.1.2.1 def irbe_cli.usage (*code* = 1)

Definition at line 240 of file irbe_cli.py.

10.1.3 Variable Documentation

10.1.3.1 tuple irbe_cli::argv = sys.argv[1:]

Definition at line 259 of file irbe_cli.py.

10.1.3.2 tuple irbe_cli.call_pubd

Initial value:

```
rpki.async.sync_wrapper(rpki.https.caller(
    proto       = publication_proto,
    client_key  = rpki.x509.RSA( Auto_file = cfg.get("pubd-irbe-key")),
    client_cert = rpki.x509.X509(Auto_file = cfg.get("pubd-irbe-cert")),
    server_ta   = rpki.x509.X509(Auto_file = cfg.get("pubd-bpki-ta")),
    server_cert = rpki.x509.X509(Auto_file = cfg.get("pubd-cert")),
    url         = cfg.get("pubd-url")),
    debug       = verbose)
```

Definition at line 323 of file irbe_cli.py.

10.1.3.3 tuple irbe_cli.call_rpkid

Initial value:

```
rpki.async.sync_wrapper(rpki.https.caller(
    proto       = left_right_proto,
    client_key  = rpki.x509.RSA( Auto_file = cfg.get("rpkid-irbe-key")),
    client_cert = rpki.x509.X509(Auto_file = cfg.get("rpkid-irbe-cert")),
    server_ta   = rpki.x509.X509(Auto_file = cfg.get("rpkid-bpki-ta")),
    server_cert = rpki.x509.X509(Auto_file = cfg.get("rpkid-cert")),
    url         = cfg.get("rpkid-url"),
    debug       = verbose))
```

Definition at line 306 of file irbe_cli.py.

10.1.3.4 tuple irbe_cli.cfg = rpki.config.parser(cfg_file, "irbe_cli")

Definition at line 283 of file irbe_cli.py.

10.1.3.5 irbe_cli.cfg_file = "irbe.conf"

Definition at line 264 of file irbe_cli.py.

10.1.3.6 irbe_cli.pem_out = None

Definition at line 39 of file irbe_cli.py.

10.1.3.7 irbe_cli.q_msg = q_msg_left_right

Definition at line 291 of file irbe_cli.py.

10.1.3.8 list irbe_cli.q_msg_left_right = [ ]

Definition at line 285 of file irbe_cli.py.

10.1.3.9 list irbe_cli.q_msg_publication = [ ]

Definition at line 286 of file irbe_cli.py.

10.1.3.10 list irbe_cli::q_pdu = left_right_msg.pdus[argv[0]]

Definition at line 290 of file irbe_cli.py.

10.1.3.11 list irbe_cli.top_opts = ["config=", "help", "pem_out=", "quiet", "verbose"]

Definition at line 238 of file irbe_cli.py.

10.1.3.12 tuple irbe_cli.usage_fill = UsageWrapper(subsequent_indent = " " * 4)

Definition at line 50 of file irbe_cli.py.

10.1.3.13 irbe_cli.verbose = True

Definition at line 265 of file irbe_cli.py.

10.2 Package irdbd

Functions

- def handle_list_resources
- def handle_list_roa_requests
- def handler

Variables

- tuple bpki_ta = rpki.x509.X509(Auto_file = cfg.get("bpki-ta"))
- tuple cfg = rpki.config.parser(cfg_file, "irdbd")
- string cfg_file = "irdbd.conf"
- tuple client_ta = (bpki_ta, rpkid_cert)
- tuple cur = db.cursor()
- tuple db
- dictionary handle_dispatch
- tuple handlers = ((u.path, handler),)
- string host = "localhost"
- tuple irdbd_cert = rpki.x509.X509(Auto_file = cfg.get("irdbd-cert"))
- tuple irdbd_key = rpki.x509.RSA(Auto_file = cfg.get("irdbd-key"))
- int port = 443
- tuple rpkid_cert = rpki.x509.X509(Auto_file = cfg.get("rpkid-cert"))

- server_cert = irdbd_cert,
- tuple startup_msg = cfg.get("startup-message", "")
- tuple u = urlparse.urlparse(cfg.get("https-url"))

10.2.1 Detailed Description

```
IR database daemon.

Usage: python irdbd.py [ { -c | --config } configfile ] [ { -h | --help } ]

Default configuration file is irdbd.conf, override with --config option.

$Id: irdbd.py 2913 2009-12-28 20:55:38Z sra $

Copyright (C) 2009  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

10.2.2 Function Documentation

10.2.2.1 def irdbd.handle_list_resources (*q_pdu*, *r_msg*)

Definition at line 53 of file irdbd.py.

10.2.2.2 def irdbd.handle_list_roa_requests (*q_pdu*, *r_msg*)

Definition at line 90 of file irdbd.py.

10.2.2.3 def irdbd.handler (*query*, *path*, *cb*)

Definition at line 119 of file irdbd.py.

10.2.3 Variable Documentation

10.2.3.1 tuple irdbd.bpki_ta = rpki.x509.X509(Auto_file = cfg.get("bpki-ta"))

Definition at line 201 of file irdbd.py.

10.2.3.2 tuple irdbd.cfg = rpki.config.parser(cfg_file, "irdbd")

Definition at line 186 of file irdbd.py.

10.2.3.3 irdbd.cfg_file = "irdbd.conf"

Definition at line 170 of file irdbd.py.

10.2.3.4 tuple irdbd.client_ta = (bpki_ta, rpkid_cert)

Definition at line 217 of file irdbd.py.

10.2.3.5 tuple irdbd.cur = db.cursor()

Definition at line 198 of file irdbd.py.

10.2.3.6 tuple irdbd.db

Initial value:

```
MySQLdb.connect(user   = cfg.get("sql-username"),
                     db     = cfg.get("sql-database"),
                     passwd = cfg.get("sql-password"))
```

Definition at line 194 of file irdbd.py.

10.2.3.7 dictionary irdbd.handle_dispatch

Initial value:

```
{
  rpki.left_right.list_resources_elt : handle_list_resources,
  rpki.left_right.list_roa_requests_elt : handle_list_roa_requests }
```

Definition at line 115 of file irdbd.py.

10.2.3.8 tuple irdbd.handlers = ((u.path, handler),)

Definition at line 220 of file irdbd.py.

10.2.3.9 string irdbd.host = "localhost"

Definition at line 218 of file irdbd.py.

10.2.3.10 tuple irdbd.irdbd_cert = rpki.x509.X509(Auto_file = cfg.get("irdbd-cert"))

Definition at line 203 of file irdbd.py.

10.2.3.11 tuple irdbd.irdbd_key = rpki.x509.RSA(Auto_file = cfg.get("irdbd-key"))

Definition at line 204 of file irdbd.py.

10.2.3.12 int irdbd.port = 443

Definition at line 219 of file irdbd.py.

10.2.3.13 tuple irdbd.rpkid_cert = rpki.x509.X509(Auto_file = cfg.get("rpkid-cert"))

Definition at line 202 of file irdbd.py.

10.2.3.14 irdbd.server_cert = irdbd_cert,

Definition at line 216 of file irdbd.py.

10.2.3.15 tuple irdbd.startup_msg = cfg.get("startup-message", "")

Definition at line 188 of file irdbd.py.

10.2.3.16 tuple irdbd.u = urlparse.urlparse(cfg.get("https-url"))

Definition at line 206 of file irdbd.py.

10.3 Package pubd

Classes

- class pubd_context

Functions

- def main

Variables

- string cfg_file = "pubd.conf"
- profile = False

10.3.1 Detailed Description

```
RPKI publication engine.

Usage: python pubd.py [ { -c | --config } configfile ]
                    [ { -h | --help } ]
                    [ { -p | --profile } outputfile ]

Default configuration file is pubd.conf, override with --config option.

$Id: pubd.py 3107 2010-03-16 23:13:08Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

10.3.2 Function Documentation

10.3.2.1 def pubd.main ()

Definition at line 174 of file pubd.py.

10.3.3 Variable Documentation

10.3.3.1 pubd.cfg_file = "pubd.conf"

Definition at line 155 of file pubd.py.

10.3.3.2 pubd.profile = False

Definition at line 156 of file pubd.py.

10.4 Package rootd

Classes

- class cms_msg
- class issue_pdu
- class list_pdu
- class message_pdu
- class revoke_pdu
- class sax_handler

Functions

- def compose_response
- def del_subject_cert
- def del_subject_pkcs10
- def get_root_cert
- def get_subject_cert
- def get_subject_pkcs10
- def issue_subject_cert_maybe
- def root_newer_than_subject
- def set_subject_cert
- def set_subject_pkcs10
- def up_down_handler

Variables

- tuple bpki_ta = rpki.x509.X509(Auto_file = cfg.get("bpki-ta"))
- tuple cfg = rpki.config.parser(cfg_file, "rootd")
- string cfg_file = "rootd.conf"
- tuple child_bpki_cert = rpki.x509.X509(Auto_file = cfg.get("child-bpki-cert"))
- tuple client_ta = (bpki_ta, child_bpki_cert)
- handlers = up_down_handler)
- host = https_server_host,
- tuple https_server_host = cfg.get("server-host", "")
- tuple https_server_port = int(cfg.get("server-port"))
- port = https_server_port,
- tuple rootd_bpki_cert = rpki.x509.X509(Auto_file = cfg.get("rootd-bpki-cert"))
- tuple rootd_bpki_crl = rpki.x509.CRL(Auto_file = cfg.get("rootd-bpki-crl"))
- tuple rootd_bpki_key = rpki.x509.RSA(Auto_file = cfg.get("rootd-bpki-key"))
- tuple rpki_base_uri = cfg.get("rpki-base-uri", "rsync://" + rpki_class_name + ".invalid/")
- tuple rpki_class_name = cfg.get("rpki-class-name", "wombat")
- rpki_root_cert = None
- tuple rpki_root_cert_file = cfg.get("rpki-root-cert")
- tuple rpki_root_cert_uri = cfg.get("rpki-root-cert-uri", rpki_base_uri + "Root.cer")
- tuple rpki_root_crl = cfg.get("rpki-root-crl", "Root.crl")
- tuple rpki_root_dir = cfg.get("rpki-root-dir")
- tuple rpki_root_key = rpki.x509.RSA(Auto_file = cfg.get("rpki-root-key"))
- tuple rpki_root_manifest = cfg.get("rpki-root-manifest", "Root.mnf")
- tuple rpki_subject_cert = cfg.get("rpki-subject-cert", "Child.cer")
- tuple rpki_subject_lifetime = rpki.sundial.timedelta.parse(cfg.get("rpki-subject-lifetime", "30d"))
- tuple rpki_subject_pkcs10 = cfg.get("rpki-subject-pkcs10", "Child.pkcs10")
- tuple rpki_subject_regen = rpki.sundial.timedelta.parse(cfg.get("rpki-subject-regen", rpki_subject_lifetime.convert_to_seconds() / 2))
- server_cert = rootd_bpki_cert,

10.4.1 Detailed Description

```
Trivial RPKI up-down protocol root server, for testing.  Not suitable
for production use.  Overrides a bunch of method definitions from the
rpki.* classes in order to reuse as much code as possible.

Usage: python rootd.py [ { -c | --config } configfile ] [ { -h | --help } ]

Default configuration file is rootd.conf, override with --config option.

$Id: rootd.py 2913 2009-12-28 20:55:38Z sra $
```

Copyright (C) 2009 Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008 American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

10.4.2 Function Documentation

10.4.2.1 def rootd.compose_response (*r_msg*, *pkcs10* = `None`)

Definition at line 175 of file rootd.py.

10.4.2.2 def rootd.del_subject_cert ()

Definition at line 72 of file rootd.py.

10.4.2.3 def rootd.del_subject_pkcs10 ()

Definition at line 91 of file rootd.py.

10.4.2.4 def rootd.get_root_cert ()

Definition at line 48 of file rootd.py.

10.4.2.5 def rootd.get_subject_cert ()

Definition at line 56 of file rootd.py.

10.4.2.6 def rootd.get_subject_pkcs10 ()

Definition at line 77 of file rootd.py.

10.4.2.7 def rootd.issue_subject_cert_maybe (*new_pkcs10*)

Definition at line 98 of file rootd.py.

10.4.2.8 def rootd.root_newer_than_subject ()

Definition at line 53 of file rootd.py.

10.4.2.9 def rootd.set_subject_cert (*cert*)

Definition at line 65 of file rootd.py.

10.4.2.10 def rootd.set_subject_pkcs10 (*pkcs10*)

Definition at line 85 of file rootd.py.

10.4.2.11 def rootd.up_down_handler (*query*, *path*, *cb*)

Definition at line 238 of file rootd.py.

10.4.3 Variable Documentation

10.4.3.1 tuple rootd.bpki_ta = rpki.x509.X509(Auto_file = cfg.get("bpki-ta"))

Definition at line 288 of file rootd.py.

10.4.3.2 tuple rootd.cfg = rpki.config.parser(cfg_file, "rootd")

Definition at line 284 of file rootd.py.

10.4.3.3 rootd.cfg_file = "rootd.conf"

Definition at line 268 of file rootd.py.

10.4.3.4 tuple rootd.child_bpki_cert = rpki.x509.X509(Auto_file = cfg.get("child-bpki-cert"))

Definition at line 292 of file rootd.py.

10.4.3.5 tuple rootd.client_ta = (bpki_ta, child_bpki_cert)

Definition at line 316 of file rootd.py.

10.4.3.6 rootd.handlers = up_down_handler)

Definition at line 319 of file rootd.py.

10.4.3.7 rootd.host = https_server_host,

Definition at line 317 of file rootd.py.

10.4.3.8 tuple rootd.https_server_host = cfg.get("server-host", "")

Definition at line 294 of file rootd.py.

10.4.3.9 tuple rootd.https_server_port = int(cfg.get("server-port"))

Definition at line 295 of file rootd.py.

10.4.3.10 rootd.port = https_server_port,

Definition at line 318 of file rootd.py.

10.4.3.11 tuple rootd.rootd_bpki_cert = rpki.x509.X509(Auto_file = cfg.get("rootd-bpki-cert"))

Definition at line 290 of file rootd.py.

10.4.3.12 tuple rootd.rootd_bpki_crl = rpki.x509.CRL(Auto_file = cfg.get("rootd-bpki-crl"))

Definition at line 291 of file rootd.py.

10.4.3.13 tuple rootd.rootd_bpki_key = rpki.x509.RSA(Auto_file = cfg.get("rootd-bpki-key"))

Definition at line 289 of file rootd.py.

10.4.3.14 tuple rootd.rpki_base_uri = cfg.get("rpki-base-uri", "rsync://" + rpki_class_name + ".invalid/")

Definition at line 300 of file rootd.py.

10.4.3.15 tuple rootd.rpki_class_name = cfg.get("rpki-class-name", "wombat")

Definition at line 297 of file rootd.py.

10.4.3.16 rootd.rpki_root_cert = None

Definition at line 46 of file rootd.py.

10.4.3.17 tuple rootd.rpki_root_cert_file = cfg.get("rpki-root-cert")

Definition at line 303 of file rootd.py.

10.4.3.18 tuple rootd.rpki_root_cert_uri = cfg.get("rpki-root-cert-uri", rpki_base_uri + "Root.cer")

Definition at line 304 of file rootd.py.

10.4.3.19 tuple rootd.rpki_root_crl = cfg.get("rpki-root-crl", "Root.crl")

Definition at line 307 of file rootd.py.

10.4.3.20 tuple rootd.rpki_root_dir = cfg.get("rpki-root-dir")

Definition at line 299 of file rootd.py.

10.4.3.21 tuple rootd.rpki_root_key = rpki.x509.RSA(Auto_file = cfg.get("rpki-root-key"))

Definition at line 302 of file rootd.py.

10.4.3.22 tuple rootd.rpki_root_manifest = cfg.get("rpki-root-manifest", "Root.mnf")

Definition at line 306 of file rootd.py.

10.4.3.23 tuple rootd.rpki_subject_cert = cfg.get("rpki-subject-cert", "Child.cer")

Definition at line 308 of file rootd.py.

10.4.3.24 tuple rootd.rpki_subject_lifetime = rpki.sundial.timedelta.parse(cfg.get("rpki-subject-lifetime", "30d"))

Definition at line 311 of file rootd.py.

10.4.3.25 tuple rootd.rpki_subject_pkcs10 = cfg.get("rpki-subject-pkcs10", "Child.pkcs10")

Definition at line 309 of file rootd.py.

10.4.3.26 tuple rootd.rpki_subject_regen = rpki.sundial.timedelta.parse(cfg.get("rpki-subject-regen", rpki_subject_lifetime.convert_to_seconds() / 2))

Definition at line 312 of file rootd.py.

10.4.3.27 rootd.server_cert = rootd_bpki_cert,

Definition at line 315 of file rootd.py.

10.5 Package rpki

Packages

- package __doc__
- package async
- package cli
- package config
- package exceptions
- package https
- package ipaddrs
- package left_right
- package log
- package manifest
- package oids
- package publication
- package relaxng
- package resource_set
- package roa
- package rpki_engine
- package sql
- package sundial
- package up_down
- package x509
- package xml_utils

10.6 Package rpki.__doc__

10.7 Package rpki.async

Classes

- class gc_summary
- class iterator
- class sync_wrapper
- class timer

Functions

- def _raiseExitNow
- def defer
- def event_loop
- def exit_event_loop
- def run_deferred

Variables

- list deferred_queue = [ ]

  List to hold deferred actions.

- ExitNow = asyncore.ExitNow

10.7.1 Detailed Description

```
Utilities for event-driven programming.

$Id: async.py 3191 2010-04-12 23:07:16Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

10.7.2 Function Documentation

10.7.2.1 def rpki.async._raiseExitNow (*signum*, *frame*) [private]

```
Signal handler for event_loop().
```

Definition at line 269 of file async.py.

10.7.2.2 def rpki.async.defer (*thunk*)

```
Defer an action until the next pass through the event loop.
```

Definition at line 250 of file async.py.

10.7.2.3 def rpki.async.event_loop (*catch_signals* = (signal.SIGINT, signal.SIGTERM))

```
Replacement for asyncore.loop(), adding timer and signal support.
```

Definition at line 273 of file async.py.

10.7.2.4 def rpki.async.exit_event_loop ()

```
Force exit from event_loop().
```

Definition at line 364 of file async.py.

10.7.2.5 def rpki.async.run_deferred ()

```
Run deferred actions.
```

Definition at line 256 of file async.py.

10.7.3 Variable Documentation

10.7.3.1 rpki::async::deferred_queue = [ ]

List to hold deferred actions.

We used to do this with the timer queue, but that appears to confuse the garbage collector, and is overengineering for simple deferred actions in any case.

Definition at line 248 of file async.py.

10.7.3.2 rpki::async.ExitNow = asyncore.ExitNow

Definition at line 24 of file async.py.

10.8 Package rpki.cli

Classes

- class Cmd

Functions

- def yes_or_no

Variables

- dictionary _yes_or_no_prompts
- have_readline = True

10.8.1 Detailed Description

```
Utilities for writing command line tools.

$Id: cli.py 3191 2010-04-12 23:07:16Z sra $

Copyright (C) 2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

10.8.2 Function Documentation

10.8.2.1 def rpki.cli.yes_or_no (*prompt*, *default* = `None`, *require_full_word* = `False`)

```
Ask a yes-or-no question.
```

Definition at line 157 of file cli.py.

10.8.3 Variable Documentation

10.8.3.1 dictionary rpki::cli._yes_or_no_prompts

Initial value:

```
{
  True  : ' ("yes" or "no" ["yes"]) ',
  False : ' ("yes" or "no" ["no"]) ',
  None  : ' ("yes" or "no") ' }
```

Definition at line 172 of file cli.py.

10.8.3.2 rpki::cli.have_readline = True

Definition at line 25 of file cli.py.

10.9 Package rpki.config

Classes

- class parser

10.9.1 Detailed Description

```
Configuration file parsing utilities, layered on top of stock Python
ConfigParser module.

$Id: config.py 3107 2010-03-16 23:13:08Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
```

PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008 American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

10.10 Package rpki.exceptions

Classes

- class BadClassNameSyntax
- class BadClientURL
- class BadContactURL
- class BadExtension
- class BadIRDBReply
- class BadIssueResponse
- class BadPKCS10
- class BadPublicationReply
- class BadQuery
- class BadSender
- class BadStatusCode
- class BadURISyntax
- class BSCNotFound
- class BSCNotReady
- class ChildNotFound
- class ClassNameMismatch
- class ClassNameUnknown
- class ClientNotFound
- class CMSContentNotSet
- class CMSCRLNotSet
- class CMSVerificationFailed
- class DBConsistancyError
- class DERObjectConversionError
- class DuplicateObject
- class EmptyPEM
- class EmptyROAPrefixList

- class ForbiddenURI
- class HandleTranslationError
- class HTTPRequestFailed
- class HTTPSBadVersion
- class HTTPSClientAborted
- class HTTPSUnexpectedState
- class MissingCMSCRL
- class MissingCMSEEcert
- class MultipleTLSEECert
- class MustBePrefix
- class NoActiveCA
- class NoCoveringCertForROA
- class NoObjectAtURI
- class NotACertificateChain
- class NotFound
- class NotImplementedYet
- class NotInDatabase
- class ReceivedTLSCACert
- class RPKI_Exception
- class ServerShuttingDown
- class SKIMismatch
- class SubprocessError
- class TLSValidationError
- class UnexpectedCMSCerts
- class UnexpectedCMSCRLs
- class UnparsableCMSDER
- class UpstreamError
- class WrongEContentType

10.10.1 Detailed Description

```
Exception definitions for RPKI modules.

$Id: exceptions.py 2907 2009-12-23 20:48:19Z sra $

Copyright (C) 2009  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
```

OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008 American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

10.11 Package rpki.https

Classes

- class caller
- class http_client
- class http_listener
- class http_message
- class http_queue
- class http_request
- class http_response
- class http_server
- class http_stream

Functions

- def build_https_ta_cache
- def client
- def log_method
- def server

Variables

- dictionary client_queues = { }

  Map of (host, port) tuples to http_queue objects.

- debug_http = False

  Verbose chatter about HTTP streams.

- debug_tls_certs = False

  Verbose chatter about TLS certificates.

- tuple default_client_timeout = rpki.sundial.timedelta(minutes = 15)

  Default HTTP client connection timeout.

- tuple default_http_version = (1, 0)

  Preferred HTTP version.

- tuple default_server_timeout = rpki.sundial.timedelta(minutes = 20)

  Default HTTP server connection timeouts.

- string rpki_content_type = "application/x-rpki"

  HTTP content type used for all RPKI messages.

- tuple supported_address_families = (socket.AF_INET, socket.AF_INET6)

  IP address families to support.

- want_persistent_client = False

  Whether we want persistent HTTP client streams, when server also supports them.

- want_persistent_server = False

  Whether we want persistent HTTP server streams, when client also supports them.

10.11.1 Detailed Description

```
HTTPS utilities, both client and server.

$Id: https.py 3191 2010-04-12 23:07:16Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
```

```
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

10.11.2 Function Documentation

10.11.2.1 def rpki.https.build_https_ta_cache (*certs*)

```
Package up a collection of certificates into a form suitable for use
as a dynamic HTTPS trust anchor set.  Precise format of this
collection is an internal conspiracy within the rpki.https module;
at one point it was a POW.X509Store object, at the moment it's a
Python set, what it will be tomorow is nobody else's business.
```

Definition at line 1094 of file https.py.

10.11.2.2 def rpki.https.client (*msg*, *client_key*, *client_cert*, *server_ta*, *url*, *callback*, *errback*)

```
Open client HTTPS connection, send a message, set up callbacks to
handle response.
```

Definition at line 1034 of file https.py.

10.11.2.3 def rpki.https.log_method (*self*, *msg*, *logger* = rpki.log.debug)

```
Logging method used in several different classes.
```

Definition at line 235 of file https.py.

10.11.2.4 def rpki.https.server (*handlers*, *server_key*, *server_cert*, *port*, *host* = `""`, *client_ta* = `()`, *dynamic_https_trust_anchor* = `None`, *address_families* = `supported_address_families`)

```
Run an HTTPS server and wait (forever) for connections.
```

Definition at line 1079 of file https.py.

10.11.3 Variable Documentation

10.11.3.1 rpki::https::client_queues = {}

Map of (host, port) tuples to http_queue objects.

Definition at line 1032 of file https.py.

10.11.3.2 rpki::https::debug_http = False

Verbose chatter about HTTP streams.

Definition at line 45 of file https.py.

10.11.3.3 rpki::https::debug_tls_certs = False

Verbose chatter about TLS certificates.

Definition at line 49 of file https.py.

10.11.3.4 rpki::https::default_client_timeout = rpki.sundial.timedelta(minutes = 15)

Default HTTP client connection timeout.

Definition at line 61 of file https.py.

10.11.3.5 rpki::https::default_http_version = (1, 0)

Preferred HTTP version.

Definition at line 72 of file https.py.

10.11.3.6 rpki::https::default_server_timeout = rpki.sundial.timedelta(minutes = 20)

Default HTTP server connection timeouts.

Given our druthers, we'd prefer that the client close the connection, as this avoids the problem of client starting to reuse connection just as server closes it, so this should be longer than the client timeout.

Definition at line 68 of file https.py.

10.11.3.7 rpki::https::rpki_content_type = "application/x-rpki"

HTTP content type used for all RPKI messages.

Definition at line 41 of file https.py.

10.11.3.8 tuple rpki::https::supported_address_families = (socket.AF_INET, socket.AF_INET6)

IP address families to support.

Almost all the code is in place for IPv6, the missing bits are DNS support that would let us figure out which address family to request, and configuration support to let us figure out which protocols are supported on the local machine. For now, leave code in place but disabled.

Address families on which to listen; first entry is also the default for opening new connections.

Definition at line 85 of file https.py.

10.11.3.9 rpki::https::want_persistent_client = False

Whether we want persistent HTTP client streams, when server also supports them.

Definition at line 53 of file https.py.

10.11.3.10 rpki::https::want_persistent_server = False

Whether we want persistent HTTP server streams, when client also supports them.

Definition at line 57 of file https.py.

10.12 Package rpki.ipaddrs

Classes

- class v4addr
- class v6addr

10.12.1 Detailed Description

```
Classes to represent IP addresses.

Given some of the other operations we need to perform on them, it's
most convenient to represent IP addresses as Python "long" values.
The classes in this module just wrap suitable read/write syntax around
the underlying "long" type.

These classes also supply a "bits" attribute for use by other code
built on these classes; for the most part, IPv6 addresses really are
just IPv4 addresses with more bits, so we supply the number of bits
once, here, thus avoiding a lot of duplicate code elsewhere.

$Id: ipaddrs.py 2424 2009-05-11 06:37:32Z sra $

Copyright (C) 2009  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
```

```
PERFORMANCE OF THIS SOFTWARE.
```

10.13 Package rpki.left_right

Classes

- class bsc_elt
- class child_elt
- class cms_msg
- class data_elt
- class left_right_namespace
- class list_published_objects_elt
- class list_received_resources_elt
- class list_resources_elt
- class list_roa_requests_elt
- class msg
- class parent_elt
- class report_error_elt
- class repository_elt
- class sax_handler
- class self_elt

Variables

- enforce_strict_up_down_xml_sender = False

10.13.1 Detailed Description

```
RPKI "left-right" protocol.

$Id: left_right.py 3191 2010-04-12 23:07:16Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

Portions copyright (C) 2007--2008 American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

10.13.2 Variable Documentation

10.13.2.1 rpki::left_right.enforce_strict_up_down_xml_sender = False

Definition at line 40 of file left_right.py.

10.14 Package rpki.log

Classes

- class logger

Functions

- def init
- def set_trace
- def trace
- def traceback

Variables

- tuple debug = logger(syslog.LOG_DEBUG)
- enable_trace = False

  Whether call tracing is enabled.

- tuple error = logger(syslog.LOG_ERR)
- tuple info = logger(syslog.LOG_INFO)
- tuple note = logger(syslog.LOG_NOTICE)
- int pid = 0

- string tag = ""
- use_syslog = True

  Whether to use syslog.

- tuple warn = logger(syslog.LOG_WARNING)

10.14.1 Detailed Description

```
Logging facilities for RPKI libraries.

$Id: log.py 3107 2010-03-16 23:13:08Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

10.14.2 Function Documentation

10.14.2.1 def rpki.log.init (*ident* = `"rpki"`, *flags* = `syslog.LOG_PID`, *facility* = `syslog.LOG_DAEMON`)

```
Initialize logging system.
```

Definition at line 51 of file log.py.

10.14.2.2 def rpki.log.set_trace (*enable*)

```
Enable or disable call tracing.
```

Definition at line 63 of file log.py.

10.14.2.3 def rpki.log.trace ()

```
Execution trace -- where are we now, and whence came we here?
```

Definition at line 91 of file log.py.

10.14.2.4 def rpki.log.traceback ()

```
Consolidated backtrace facility with a bit of extra info.
```

Definition at line 100 of file log.py.

10.14.3 Variable Documentation

10.14.3.1 tuple rpki::log.debug = logger(syslog.LOG_DEBUG)

Definition at line 89 of file log.py.

10.14.3.2 rpki::log::enable_trace = False

Whether call tracing is enabled.

Definition at line 41 of file log.py.

10.14.3.3 tuple rpki::log.error = logger(syslog.LOG_ERR)

Definition at line 85 of file log.py.

10.14.3.4 tuple rpki::log.info = logger(syslog.LOG_INFO)

Definition at line 88 of file log.py.

10.14.3.5 tuple rpki::log.note = logger(syslog.LOG_NOTICE)

Definition at line 87 of file log.py.

10.14.3.6 int rpki::log.pid = 0

Definition at line 49 of file log.py.

10.14.3.7 string rpki::log.tag = ""

Definition at line 48 of file log.py.

10.14.3.8 rpki::log::use_syslog = True

Whether to use syslog.

Definition at line 46 of file log.py.

10.14.3.9 tuple rpki::log.warn = logger(syslog.LOG_WARNING)

Definition at line 86 of file log.py.

10.15 Package rpki.manifest

Classes

- class FileAndHash
- class FilesAndHashes
- class Manifest

10.15.1 Detailed Description

```
Signed manifests.  This is just the ASN.1 encoder, the rest is in
rpki.x509 with the rest of the DER_object code.

Note that rpki.x509.SignedManifest implements the signed manifest;
the structures here are just the payload of the CMS eContent field.

$Id: manifest.py 2424 2009-05-11 06:37:32Z sra $

Copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

10.16 Package rpki.oids

Variables

- tuple name2oid = dict((v, k) for k, v in oid2name.items())

  Mapping table of string names to OIDs.

- dictionary oid2name

  Mapping table of OIDs to conventional string names.

10.16.1 Detailed Description

```
OID database.

$Id: oids.py 2424 2009-05-11 06:37:32Z sra $

Copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
```

```
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

10.16.2 Variable Documentation

10.16.2.1 rpki::oids::name2oid = dict((v, k) for k, v in oid2name.items())

Mapping table of string names to OIDs.

Definition at line 58 of file oids.py.

10.16.2.2 rpki::oids::oid2name

Initial value:

```
{
  (1, 2, 840, 113549, 1, 1, 11)         : "sha256WithRSAEncryption",
  (1, 2, 840, 113549, 1, 1, 12)         : "sha384WithRSAEncryption",
  (1, 2, 840, 113549, 1, 1, 13)         : "sha512WithRSAEncryption",
  (1, 2, 840, 113549, 1, 7,  1)         : "id-data",
  (1, 2, 840, 113549, 1, 9, 16)         : "id-smime",
  (1, 2, 840, 113549, 1, 9, 16, 1)      : "id-ct",
  (1, 2, 840, 113549, 1, 9, 16, 1, 24)  : "id-ct-routeOriginAttestation",
  (1, 2, 840, 113549, 1, 9, 16, 1, 26)  : "id-ct-rpkiManifest",
  (1, 2, 840, 113549, 1, 9, 16, 1, 28)  : "id-ct-xml",
  (1, 3, 6, 1, 5, 5, 7, 1, 1)           : "authorityInfoAccess",
  (1, 3, 6, 1, 5, 5, 7, 1, 11)          : "subjectInfoAccess",
  (1, 3, 6, 1, 5, 5, 7, 1, 7)           : "sbgp-ipAddrBlock",
  (1, 3, 6, 1, 5, 5, 7, 1, 8)           : "sbgp-autonomousSysNum",
  (1, 3, 6, 1, 5, 5, 7, 14, 2)          : "id-cp-ipAddr-asNumber",
  (1, 3, 6, 1, 5, 5, 7, 48, 2)          : "id-ad-caIssuers",
  (1, 3, 6, 1, 5, 5, 7, 48, 5)          : "id-ad-caRepository",
  (1, 3, 6, 1, 5, 5, 7, 48, 9)          : "id-ad-signedObjectRepository",
  (1, 3, 6, 1, 5, 5, 7, 48, 10)         : "id-ad-rpkiManifest",
  (1, 3, 6, 1, 5, 5, 7, 48, 11)         : "id-ad-signedObject",
  (2, 16, 840, 1, 101, 3, 4, 2, 1)      : "id-sha256",
  (2, 5, 29, 14)                        : "subjectKeyIdentifier",
  (2, 5, 29, 15)                        : "keyUsage",
  (2, 5, 29, 19)                        : "basicConstraints",
  (2, 5, 29, 20)                        : "cRLNumber",
  (2, 5, 29, 31)                        : "cRLDistributionPoints",
  (2, 5, 29, 32)                        : "certificatePolicies",
  (2, 5, 29, 35)                        : "authorityKeyIdentifier",
  (2, 5, 4, 3)                          : "commonName",
}
```

Mapping table of OIDs to conventional string names.

Definition at line 24 of file oids.py.

10.17 Package rpki.publication

Classes

- class certificate_elt
- class client_elt
- class cms_msg
- class config_elt
- class control_elt
- class crl_elt
- class manifest_elt
- class msg
- class publication_namespace
- class publication_object_elt
- class report_error_elt
- class roa_elt
- class sax_handler

10.17.1 Detailed Description

```
RPKI "publication" protocol.

$Id: publication.py 3107 2010-03-16 23:13:08Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

10.18 Package rpki.relaxng

Variables

- tuple left_right

  Parsed RelaxNG left_right schema.

- tuple publication

  Parsed RelaxNG publication schema.

- tuple up_down

  Parsed RelaxNG up_down schema.

10.18.1 Variable Documentation

10.18.1.1 rpki::relaxng::left_right

Parsed RelaxNG left_right schema.

Definition at line 7 of file relaxng.py.

10.18.1.2 rpki::relaxng::publication

Parsed RelaxNG publication schema.

Definition at line 1252 of file relaxng.py.

10.18.1.3 rpki::relaxng::up_down

Parsed RelaxNG up_down schema.

Definition at line 998 of file relaxng.py.

10.19 Package rpki.resource_set

Classes

- class resource_bag

- class resource_range
- class resource_range_as
- class resource_range_ip
- class resource_range_ipv4
- class resource_range_ipv6
- class resource_set
- class resource_set_as
- class resource_set_ip
- class resource_set_ipv4
- class resource_set_ipv6
- class roa_prefix
- class roa_prefix_ipv4
- class roa_prefix_ipv6
- class roa_prefix_set
- class roa_prefix_set_ipv4
- class roa_prefix_set_ipv6

Functions

- def _bs2long
- def _long2bs
- def _rsplit
- def test1
- def test2

Variables

- string inherit_token = "<inherit>"

  Token used to indicate inheritance in read and print syntax.

10.19.1 Detailed Description

```
Classes dealing with sets of resources.

The basic mechanics of a resource set are the same for any of the
resources we handle (ASNs, IPv4 addresses, or IPv6 addresses), so we
can provide the same operations on any of them, even though the
underlying details vary.

We also provide some basic set operations (union, intersection, etc).

$Id: resource_set.py 3107 2010-03-16 23:13:08Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")
```

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008 American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

10.19.2 Function Documentation

10.19.2.1 def rpki.resource_set._bs2long (*bs*, *addrlen*, *fill*) [private]

Utility function to convert a bitstring (POW.pkix tuple
representation) into a Python long.

Definition at line 514 of file resource_set.py.

10.19.2.2 def rpki.resource_set._long2bs (*number*, *addrlen*, *prefixlen* = None, *strip* = None) [private]

Utility function to convert a Python long into a POW.pkix tuple
bitstring. This is a bit complicated because it supports the
fiendishly compact encoding used in RFC 3779.

Definition at line 526 of file resource_set.py.

10.19.2.3 def rpki.resource_set._rsplit (*rset*, *that*) [private]

```
Utility function to split a resource range into two resource ranges.
```

Definition at line 190 of file resource_set.py.

10.19.2.4 def rpki.resource_set.test1 (*t*, *s1*, *s2*)

Definition at line 884 of file resource_set.py.

10.19.2.5 def rpki.resource_set.test2 (*t*, *s1*, *s2*)

Definition at line 917 of file resource_set.py.

10.19.3 Variable Documentation

10.19.3.1 rpki::resource_set::inherit_token = "<inherit>"

Token used to indicate inheritance in read and print syntax.

Definition at line 48 of file resource_set.py.

10.20 Package rpki.roa

Classes

- class ROAIPAddress
- class ROAIPAddresses
- class ROAIPAddressFamilies
- class ROAIPAddressFamily
- class RouteOriginAttestation

10.20.1 Detailed Description

```
ROA (Route Origin Authorization).
```

```
At the moment this is just the ASN.1 encoder.

This corresponds to draft-ietf-sidr-roa-format, which is a work in
progress, so this may need updating later.

$Id: roa.py 2424 2009-05-11 06:37:32Z sra $

Copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

draft-ietf-sidr-roa-format-03 2.1.3.2 specifies:

   RouteOriginAttestation ::= SEQUENCE {
      version [0] INTEGER DEFAULT 0,
      asID  ASID,
      ipAddrBlocks SEQUENCE OF ROAIPAddressFamily }

   ASID ::= INTEGER

   ROAIPAddressFamily ::= SEQUENCE {
      addressFamily OCTET STRING (SIZE (2..3)),
      addresses SEQUENCE OF ROAIPAddress }

   ROAIPAddress ::= SEQUENCE {
      address IPAddress,
      maxLength INTEGER OPTIONAL }

   IPAddress ::= BIT STRING
```

10.21 Package rpki.rpki_engine

Classes

- class ca_detail_obj
- class ca_obj
- class child_cert_obj
- class publication_queue
- class revoked_cert_obj
- class roa_obj
- class rpkid_context

10.21.1 Detailed Description

```
Global context for rpkid.

$Id: rpki_engine.py 3107 2010-03-16 23:13:08Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

10.22 Package rpki.sql

Classes

- class session
- class sql_persistent
- class template

10.22.1 Detailed Description

```
SQL interface code.

$Id: sql.py 2895 2009-12-21 17:17:55Z sra $

Copyright (C) 2009  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
```

copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008 American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

10.23 Package rpki.sundial

Classes

- class datetime
- class timedelta

Functions

- def _cast
- def now
- def test

10.23.1 Detailed Description

Unified RPKI date/time handling, based on the standard Python datetime module.

Module name chosen to sidestep a nightmare of import-related errors
that occur with the more obvious module names.

List of arithmetic methods that require result casting was derived by
inspection of the datetime module, to wit:

```
>>> import datetime
>>> for t in (datetime.datetime, datetime.timedelta):
...  for k in t.__dict__.keys():
```

```
  ...   if k.startswith("__"):
  ...    print "%s.%s()" % (t.__name__, k)
```

```
$Id: sundial.py 3191 2010-04-12 23:07:16Z sra $
```


```
Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```


10.23.2 Function Documentation

10.23.2.1 def rpki.sundial._cast (*x*) [private]

```
Cast result of arithmetic operations back into correct subtype.
```

Definition at line 257 of file sundial.py.

10.23.2.2 def rpki.sundial.now ()

```
Get current timestamp.
```

Definition at line 50 of file sundial.py.

10.23.2.3 def rpki.sundial.test (*t*)

Definition at line 269 of file sundial.py.

10.24 Package rpki.up_down

Classes

- class base_elt
- class certificate_elt
- class class_elt
- class class_response_syntax
- class cms_msg
- class error_response_pdu
- class issue_pdu
- class issue_response_pdu
- class list_pdu
- class list_response_pdu
- class message_pdu
- class multi_uri
- class revoke_pdu
- class revoke_response_pdu
- class revoke_syntax
- class sax_handler

Variables

- dictionary nsmap = { None : xmlns }
- string xmlns = "http://www.apnic.net/specs/rescerts/up-down/"

10.24.1 Detailed Description

```
RPKI "up-down" protocol.

$Id: up_down.py 3162 2010-04-06 18:50:47Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
```

REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008 American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

10.24.2 Variable Documentation

10.24.2.1 dictionary rpki::up_down.nsmap = { None : xmlns }

Definition at line 41 of file up_down.py.

10.24.2.2 string rpki::up_down.xmlns = "http://www.apnic.net/specs/rescerts/up-down/"

Definition at line 39 of file up_down.py.

10.25 Package rpki.x509

Classes

- class CMS_object
- class CRL
- class DeadDrop
- class DER_CMS_object
- class DER_object
- class PEM_converter
- class PKCS10
- class ROA

- class RSA
- class RSApublic
- class SignedManifest
- class X509
- class XML_CMS_object

Functions

- def _find_xia_uri
- def calculate_SKI
- def POWify_OID

10.25.1 Detailed Description

```
One X.509 implementation to rule them all...

...and in the darkness hide the twisty maze of partially overlapping
X.509 support packages in Python.

There are several existing packages, none of which do quite what I
need, due to age, lack of documentation, specialization, or lack of
foresight on somebody's part (perhaps mine).  This module attempts to
bring together the functionality I need in a way that hides at least
some of the nasty details.  This involves a lot of format conversion.

$Id: x509.py 3107 2010-03-16 23:13:08Z sra $


Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.


Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
```

```
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

10.25.2 Function Documentation

10.25.2.1 def rpki.x509._find_xia_uri (*extension*, *name*) [private]

```
Find a rsync URI in an SIA or AIA extension.
Returns the URI if found, otherwise None.
```

Definition at line 105 of file x509.py.

10.25.2.2 def rpki.x509.calculate_SKI (*public_key_der*)

```
Calculate the SKI value given the DER representation of a public
key, which requires first peeling the ASN.1 wrapper off the key.
```

Definition at line 51 of file x509.py.

10.25.2.3 def rpki.x509.POWify_OID (*oid*)

```
Utility function to convert tuple form of an OID to the
dotted-decimal string form that POW uses.
```

Definition at line 725 of file x509.py.

10.26 Package rpki.xml_utils

Classes

- class base_elt
- class data_elt
- class msg
- class sax_handler
- class text_elt

10.26.1 Detailed Description

```
XML utilities.

$Id: xml_utils.py 2836 2009-10-26 22:31:16Z sra $

Copyright (C) 2009  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

10.27 Package rpkid

Functions

- def main

Variables

- string cfg_file = "rpkid.conf"
- profile = None

10.27.1 Detailed Description

```
RPKI engine daemon.  This is still very much a work in progress.

Usage: python rpkid.py [ { -c | --config } configfile ]
                    [ { -h | --help } ]
```

```
                  [ { -p | --profile } outputfile ]

Default configuration file is rpkid.conf, override with --config option.

$Id: rpkid.py 2913 2009-12-28 20:55:38Z sra $

Copyright (C) 2009  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

10.27.2 Function Documentation

10.27.2.1 def rpkid.main ()

Definition at line 68 of file rpkid.py.

10.27.3 Variable Documentation

10.27.3.1 rpkid.cfg_file = "rpkid.conf"

Definition at line 49 of file rpkid.py.

10.27.3.2 rpkid.profile = None

Definition at line 50 of file rpkid.py.

11 Class Documentation

11.1 async_chat Class Reference

Inherited by rpki.https.http_stream.

The documentation for this class was generated from the following file:

- https.py (3191)

11.2 dispatcher Class Reference

Inherited by rpki.https.http_listener.

The documentation for this class was generated from the following file:

- https.py (3191)

11.3 Cmd Class Reference

Inherited by rpki.cli.Cmd.

The documentation for this class was generated from the following file:

- cli.py (3191)

11.4 Exception Class Reference

Inherited by rpki.exceptions.RPKI_Exception.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.5 irbe_cli.bsc_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::bsc_elt.

Collaboration diagram for irbe_cli.bsc_elt:

Public Member Functions

- def client_query_signing_cert
- def client_query_signing_cert_crl
- def client_reply_decode

Public Attributes

- signing_cert
- signing_cert_crl

Static Public Attributes

- tuple excludes = ("pkcs10_request",)

  XML attributes and elements that should not be allowed as command line arguments.

11.5.1 Detailed Description

Definition at line 152 of file irbe_cli.py.

11.5.2 Member Function Documentation

11.5.2.1 def irbe_cli.bsc_elt.client_query_signing_cert (*self*, *arg*)

```
--signing_cert option.
```

Definition at line 156 of file irbe_cli.py.

11.5.2.2 def irbe_cli.bsc_elt.client_query_signing_cert_crl (*self*, *arg*)

```
--signing_cert_crl option.
```

Definition at line 160 of file irbe_cli.py.

11.5.2.3 def irbe_cli.bsc_elt.client_reply_decode (*self*)

Reimplemented from irbe_cli.reply_elt_mixin.

Definition at line 164 of file irbe_cli.py.

11.5.3 Member Data Documentation

11.5.3.1 tuple irbe_cli.bsc_elt.excludes = ("pkcs10_request",) `[static]`

XML attributes and elements that should not be allowed as command line arguments.

Reimplemented from irbe_cli.cmd_elt_mixin.

Definition at line 154 of file irbe_cli.py.

11.5.3.2 irbe_cli.bsc_elt.signing_cert

Reimplemented from rpki.left_right.bsc_elt.

Definition at line 158 of file irbe_cli.py.

11.5.3.3 irbe_cli.bsc_elt.signing_cert_crl

Reimplemented from rpki.left_right.bsc_elt.

Definition at line 162 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.6 irbe_cli.certificate_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::publication::certificate_elt.

Collaboration diagram for irbe_cli.certificate_elt:

11.6.1 Detailed Description

Definition at line 211 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.7 irbe_cli.child_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::child_elt.

Collaboration diagram for irbe_cli.child_elt:

11.7.1 Detailed Description

Definition at line 174 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.8 irbe_cli.client_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::publication::client_elt.

Collaboration diagram for irbe_cli.client_elt:

11.8.1 Detailed Description

Definition at line 208 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.9 irbe_cli.cmd_elt_mixin Class Reference

Inherits irbe_cli::reply_elt_mixin.

Inherited by irbe_cli.bsc_elt, irbe_cli.certificate_elt, irbe_cli.child_elt, irbe_cli.client_elt, irbe_cli.config_elt, irbe_cli.crl_elt, irbe_cli.list_published_objects_elt, irbe_cli.list_received_resources_elt, irbe_cli.manifest_elt, irbe_cli.parent_elt, irbe_cli.repository_elt, irbe_cli.roa_elt, and irbe_cli.self_elt.

Collaboration diagram for irbe_cli.cmd_elt_mixin:

Public Member Functions

- def client_getopt
- def client_query_bpki_cert
- def client_query_bpki_cms_cert
- def client_query_bpki_https_cert
- def client_query_cms_glue

- def client_query_glue
- def client_query_https_glue
- def usage

Public Attributes

- bpki_cert
- bpki_cms_cert
- bpki_cms_glue
- bpki_glue
- bpki_https_cert
- bpki_https_glue

Static Public Attributes

- tuple excludes = ()

  XML attributes and elements that should not be allowed as command line arguments.

- is_cmd = True

11.9.1 Detailed Description

```
Protocol mix-in for command line client element PDUs.
```

Definition at line 68 of file irbe_cli.py.

11.9.2 Member Function Documentation

11.9.2.1 def irbe_cli.cmd_elt_mixin.client_getopt (*self*, *argv*)

```
Parse options for this class.
```

Definition at line 92 of file irbe_cli.py.

11.9.2.2 def irbe_cli.cmd_elt_mixin.client_query_bpki_cert (*self*, *arg*)

```
Special handler for --bpki_cert option.
```

Definition at line 109 of file irbe_cli.py.

11.9.2.3 def irbe_cli.cmd_elt_mixin.client_query_bpki_cms_cert (*self*, *arg*)

```
Special handler for --bpki_cms_cert option.
```

Definition at line 117 of file irbe_cli.py.

11.9.2.4 def irbe_cli.cmd_elt_mixin.client_query_bpki_https_cert (*self*, *arg*)

```
Special handler for --bpki_https_cert option.
```

Definition at line 125 of file irbe_cli.py.

11.9.2.5 def irbe_cli.cmd_elt_mixin.client_query_cms_glue (*self*, *arg*)

```
Special handler for --bpki_cms_glue option.
```

Definition at line 121 of file irbe_cli.py.

11.9.2.6 def irbe_cli.cmd_elt_mixin.client_query_glue (*self*, *arg*)

```
Special handler for --bpki_glue option.
```

Definition at line 113 of file irbe_cli.py.

11.9.2.7 def irbe_cli.cmd_elt_mixin.client_query_https_glue (*self*, *arg*)

```
Special handler for --bpki_https_glue option.
```

Definition at line 129 of file irbe_cli.py.

11.9.2.8 def irbe_cli.cmd_elt_mixin.usage (*cls*)

```
Generate usage message for this PDU.
```

Definition at line 81 of file irbe_cli.py.

11.9.3 Member Data Documentation

11.9.3.1 irbe_cli.cmd_elt_mixin.bpki_cert

Definition at line 111 of file irbe_cli.py.

11.9.3.2 irbe_cli.cmd_elt_mixin.bpki_cms_cert

Definition at line 119 of file irbe_cli.py.

11.9.3.3 irbe_cli.cmd_elt_mixin.bpki_cms_glue

Definition at line 123 of file irbe_cli.py.

11.9.3.4 irbe_cli.cmd_elt_mixin.bpki_glue

Definition at line 115 of file irbe_cli.py.

11.9.3.5 irbe_cli.cmd_elt_mixin.bpki_https_cert

Definition at line 127 of file irbe_cli.py.

11.9.3.6 irbe_cli.cmd_elt_mixin.bpki_https_glue

Definition at line 131 of file irbe_cli.py.

11.9.3.7 irbe_cli.cmd_elt_mixin::excludes = () `[static]`

XML attributes and elements that should not be allowed as command line arguments.

Reimplemented in irbe_cli.bsc_elt, irbe_cli.list_published_objects_elt, and irbe_cli.list_received_resources_elt.

Definition at line 78 of file irbe_cli.py.

11.9.3.8 irbe_cli.cmd_elt_mixin.is_cmd = True [static]

Reimplemented from irbe_cli.reply_elt_mixin.

Definition at line 73 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.10 irbe_cli.cmd_msg_mixin Class Reference

Inherits object.

Inherited by irbe_cli.left_right_msg, and irbe_cli.publication_msg.

Collaboration diagram for irbe_cli.cmd_msg_mixin:

Public Member Functions

- def usage

11.10.1 Detailed Description

```
Protocol mix-in for command line client message PDUs.
```

Definition at line 133 of file irbe_cli.py.

11.10.2 Member Function Documentation

11.10.2.1 def irbe_cli.cmd_msg_mixin.usage (*cls*)

```
Generate usage message for this PDU.
```

Definition at line 139 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.11 irbe_cli.config_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::publication::config_elt.

Collaboration diagram for irbe_cli.config_elt:

Public Member Functions

- def client_query_bpki_crl

Public Attributes

- bpki_crl

11.11.1 Detailed Description

Definition at line 202 of file irbe_cli.py.

11.11.2 Member Function Documentation

11.11.2.1 def irbe_cli.config_elt.client_query_bpki_crl (*self*, *arg*)

```
Special handler for --bpki_crl option.
```

Definition at line 204 of file irbe_cli.py.

11.11.3 Member Data Documentation

11.11.3.1 irbe_cli.config_elt.bpki_crl

Definition at line 206 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.12 irbe_cli.crl_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::publication::crl_elt.

Collaboration diagram for irbe_cli.crl_elt:

11.12.1 Detailed Description

Definition at line 214 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.13 irbe_cli.left_right_cms_msg Class Reference

Inherits rpki::left_right::cms_msg.

Collaboration diagram for irbe_cli.left_right_cms_msg:

Static Public Attributes

- saxify = left_right_sax_handler.saxify

11.13.1 Detailed Description

Definition at line 197 of file irbe_cli.py.

11.13.2 Member Data Documentation

11.13.2.1 irbe_cli.left_right_cms_msg.saxify = left_right_sax_handler.saxify [static]

Reimplemented from rpki.left_right.cms_msg.

Definition at line 198 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.14 irbe_cli.left_right_msg Class Reference

Inherits irbe_cli::cmd_msg_mixin, and rpki::left_right::msg.

Collaboration diagram for irbe_cli.left_right_msg:

Static Public Attributes

- tuple pdus

  Dispatch table of PDUs for this protocol.

11.14.1 Detailed Description

Definition at line 189 of file irbe_cli.py.

11.14.2 Member Data Documentation

11.14.2.1 tuple irbe_cli.left_right_msg.pdus [static]

Initial value:

```
dict((x.element_name, x)
              for x in (self_elt, bsc_elt, parent_elt, child_elt, repository_elt,

                        list_published_objects_elt, list_received_resources_elt,
      report_error_elt))
```

Dispatch table of PDUs for this protocol.

Reimplemented from rpki.left_right.msg.

Definition at line 190 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.15 irbe_cli.left_right_proto Class Reference

Inherits object.

Collaboration diagram for irbe_cli.left_right_proto:

Static Public Attributes

- cms_msg = left_right_cms_msg
- msg = left_right_msg

11.15.1 Detailed Description

Definition at line 302 of file irbe_cli.py.

11.15.2 Member Data Documentation

11.15.2.1 irbe_cli.left_right_proto.cms_msg = left_right_cms_msg [static]

Definition at line 303 of file irbe_cli.py.

11.15.2.2 irbe_cli.left_right_proto.msg = left_right_msg [static]

Definition at line 304 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.16 irbe_cli.left_right_sax_handler Class Reference

Inherits rpki::left_right::sax_handler.

Collaboration diagram for irbe_cli.left_right_sax_handler:

Static Public Attributes

- pdu = left_right_msg

11.16.1 Detailed Description

Definition at line 194 of file irbe_cli.py.

11.16.2 Member Data Documentation

11.16.2.1 irbe_cli.left_right_sax_handler.pdu = left_right_msg [static]

Reimplemented from rpki.left_right.sax_handler.

Definition at line 195 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.17 irbe_cli.list_published_objects_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::list_published_objects_elt.

Collaboration diagram for irbe_cli.list_published_objects_elt:

Static Public Attributes

- tuple excludes = ("uri",)

XML attributes and elements that should not be allowed as command line arguments.

11.17.1 Detailed Description

Definition at line 180 of file irbe_cli.py.

11.17.2 Member Data Documentation

11.17.2.1 tuple irbe_cli.list_published_objects_elt.excludes = ("uri",) [static]

XML attributes and elements that should not be allowed as command line arguments.

Reimplemented from irbe_cli.cmd_elt_mixin.

Definition at line 181 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.18 irbe_cli.list_received_resources_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::list_received_resources_elt.

Collaboration diagram for irbe_cli.list_received_resources_elt:

Static Public Attributes

- tuple excludes = ("notBefore", "notAfter", "uri", "sia_uri", "aia_uri", "asn", "ipv4", "ipv6")

  XML attributes and elements that should not be allowed as command line arguments.

11.18.1 Detailed Description

Definition at line 183 of file irbe_cli.py.

11.18.2 Member Data Documentation

11.18.2.1 tuple irbe_cli.list_received_resources_elt.excludes = ("notBefore", "notAfter", "uri", "sia_uri", "aia_uri", "asn", "ipv4", "ipv6") [static]

XML attributes and elements that should not be allowed as command line arguments.

Reimplemented from irbe_cli.cmd_elt_mixin.

Definition at line 184 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.19 irbe_cli.manifest_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::publication::manifest_elt.

Collaboration diagram for irbe_cli.manifest_elt:

11.19.1 Detailed Description

Definition at line 217 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.20 irbe_cli.parent_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::parent_elt.

Collaboration diagram for irbe_cli.parent_elt:

11.20.1 Detailed Description

Definition at line 171 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.21 irbe_cli.publication_cms_msg Class Reference

Inherits rpki::publication::cms_msg.

Collaboration diagram for irbe_cli.publication_cms_msg:

Static Public Attributes

- saxify = publication_sax_handler.saxify

11.21.1 Detailed Description

Definition at line 233 of file irbe_cli.py.

11.21.2 Member Data Documentation

11.21.2.1 irbe_cli.publication_cms_msg.saxify = publication_sax_handler.saxify [static]

Reimplemented from rpki.publication.cms_msg.

Definition at line 234 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.22 irbe_cli.publication_msg Class Reference

Inherits irbe_cli::cmd_msg_mixin, and rpki::publication::msg.

Collaboration diagram for irbe_cli.publication_msg:

Static Public Attributes

- tuple pdus

  Dispatch table of PDUs for this protocol.

11.22.1 Detailed Description

Definition at line 226 of file irbe_cli.py.

11.22.2 Member Data Documentation

11.22.2.1 tuple irbe_cli.publication_msg.pdus [static]

Initial value:

```
dict((x.element_name, x)
              for x in (config_elt, client_elt, certificate_elt, crl_elt, manifes
      t_elt, roa_elt, report_error_elt))
```

Dispatch table of PDUs for this protocol.

Reimplemented from rpki.publication.msg.

Definition at line 227 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.23 irbe_cli.publication_proto Class Reference

Inherits object.

Collaboration diagram for irbe_cli.publication_proto:

Static Public Attributes

- cms_msg = publication_cms_msg
- msg = publication_msg

11.23.1 Detailed Description

Definition at line 319 of file irbe_cli.py.

11.23.2 Member Data Documentation

11.23.2.1 irbe_cli.publication_proto.cms_msg = publication_cms_msg [static]

Definition at line 321 of file irbe_cli.py.

11.23.2.2 irbe_cli.publication_proto.msg = publication_msg [static]

Definition at line 320 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.24 irbe_cli.publication_sax_handler Class Reference

Inherits rpki::publication::sax_handler.

Collaboration diagram for irbe_cli.publication_sax_handler:

Static Public Attributes

- pdu = publication_msg

11.24.1 Detailed Description

Definition at line 230 of file irbe_cli.py.

11.24.2 Member Data Documentation

11.24.2.1 irbe_cli.publication_sax_handler.pdu = publication_msg [static]

Reimplemented from rpki.publication.sax_handler.

Definition at line 231 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.25 irbe_cli.reply_elt_mixin Class Reference

Inherits object.

Inherited by irbe_cli.cmd_elt_mixin, irbe_cli.report_error_elt, and irbe_cli.report_error_elt.

Collaboration diagram for irbe_cli.reply_elt_mixin:

Public Member Functions

- def client_reply_decode
- def client_reply_show

Static Public Attributes

- is_cmd = False

11.25.1 Detailed Description

```
Protocol mix-in for printout of reply PDUs.
```

Definition at line 52 of file irbe_cli.py.

11.25.2 Member Function Documentation

11.25.2.1 def irbe_cli.reply_elt_mixin.client_reply_decode (*self*)

Reimplemented in irbe_cli.bsc_elt.

Definition at line 59 of file irbe_cli.py.

11.25.2.2 def irbe_cli.reply_elt_mixin.client_reply_show (*self*)

Definition at line 62 of file irbe_cli.py.

11.25.3 Member Data Documentation

11.25.3.1 irbe_cli.reply_elt_mixin.is_cmd = False `[static]`

Reimplemented in irbe_cli.cmd_elt_mixin.

Definition at line 57 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.26 irbe_cli.report_error_elt Class Reference

Inherits irbe_cli::reply_elt_mixin, rpki::publication::report_error_elt, irbe_cli::reply_-elt_mixin, and rpki::left_right::report_error_elt.

Collaboration diagram for irbe_cli.report_error_elt:

11.26.1 Detailed Description

Definition at line 186 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.27 irbe_cli.repository_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::repository_elt.

Collaboration diagram for irbe_cli.repository_elt:

11.27.1 Detailed Description

Definition at line 177 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.28 irbe_cli.roa_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::publication::roa_elt.

Collaboration diagram for irbe_cli.roa_elt:

11.28.1 Detailed Description

Definition at line 220 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.29 irbe_cli.self_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::self_elt.

Collaboration diagram for irbe_cli.self_elt:

11.29.1 Detailed Description

Definition at line 149 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.30 irbe_cli.UsageWrapper Class Reference

Inherits textwrap::TextWrapper.

Collaboration diagram for irbe_cli.UsageWrapper:

Public Member Functions

- def __call__

11.30.1 Detailed Description

```
Call interface around Python textwrap.Textwrapper class.
```

Definition at line 41 of file irbe_cli.py.

11.30.2 Member Function Documentation

11.30.2.1 def irbe_cli.UsageWrapper.__call__ (*self*, *args*)

```
Format arguments, with TextWrapper indentation.
```

Definition at line 46 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.31 long Class Reference

Inherited by rpki.ipaddrs.v4addr, and rpki.ipaddrs.v6addr.

The documentation for this class was generated from the following file:

- ipaddrs.py (2424)

11.32 object Class Reference

Inherited by irbe_cli.cmd_msg_mixin, irbe_cli.left_right_proto, irbe_cli.publication_proto, irbe_cli.reply_elt_mixin, pubd.pubd_context, rpki.async.gc_summary, rpki.async.iterator, rpki.async.sync_wrapper, rpki.async.timer, rpki.config.parser, rpki.https.caller, rpki.https.http_message, rpki.https.http_queue, rpki.left_right.left_right_namespace, rpki.log.logger, rpki.publication.publication_namespace, rpki.resource_set.resource_bag, rpki.resource_set.resource_range, rpki.resource_set.roa_prefix, rpki.rpki_engine.publication_queue, rpki.rpki_engine.rpkid_context, rpki.sql.session, rpki.sql.sql_persistent, rpki.sql.template, rpki.up_down.base_elt, rpki.x509.DeadDrop, rpki.x509.DER_object, rpki.x509.PEM_converter, and rpki.xml_utils.base_elt.

The documentation for this class was generated from the following file:

- x509.py (3107)

11.33 pubd.pubd_context Class Reference

Inherits object.

Collaboration diagram for pubd.pubd_context:

Public Member Functions

- def __init__
- def build_https_ta_cache
- def clear_https_ta_cache

- def client_handler
- def control_handler
- def handler_common

Public Attributes

- bpki_ta
- https_server_host
- https_server_port
- irbe_cert
- pubd_cert
- pubd_key
- publication_base
- publication_multimodule
- sql

Static Public Attributes

- tuple client_url_regexp = re.compile("/client/([-A-Z0-9_/]+)$", re.I)
- https_ta_cache = None

  HTTPS trust anchor cache, to avoid regenerating it for every TLS connection.

11.33.1 Detailed Description

```
A container for various pubd parameters.
```

Definition at line 46 of file pubd.py.

11.33.2 Member Function Documentation

11.33.2.1 def pubd.pubd_context.__init__ (*self*, *cfg*)

Definition at line 51 of file pubd.py.

11.33.2.2 def pubd.pubd_context.build_https_ta_cache (*self*)

```
Build dynamic TLS trust anchors.
```

Definition at line 140 of file pubd.py.

11.33.2.3 def pubd.pubd_context.clear_https_ta_cache (*self*)

```
Clear dynamic TLS trust anchors.
```

Definition at line 132 of file pubd.py.

11.33.2.4 def pubd.pubd_context.client_handler (*self*, *query*, *path*, *cb*)

```
Process one PDU from a client.
```

Definition at line 100 of file pubd.py.

11.33.2.5 def pubd.pubd_context.control_handler (*self*, *query*, *path*, *cb*)

```
Process one PDU from the IRBE.
```

Definition at line 80 of file pubd.py.

11.33.2.6 def pubd.pubd_context.handler_common (*self*, *query*, *client*, *cb*, *certs*, *crl* = `None`)

```
Common PDU handler code.
```

Definition at line 67 of file pubd.py.

11.33.3 Member Data Documentation

11.33.3.1 pubd.pubd_context.bpki_ta

Definition at line 55 of file pubd.py.

11.33.3.2 tuple pubd.pubd_context.client_url_regexp = re.compile("/client/([-A-Z0-9_/]+)$", re.I) [static]

Definition at line 98 of file pubd.py.

11.33.3.3 pubd.pubd_context.https_server_host

Definition at line 60 of file pubd.py.

11.33.3.4 pubd.pubd_context.https_server_port

Definition at line 61 of file pubd.py.

11.33.3.5 pubd.pubd_context::https_ta_cache = None [static]

HTTPS trust anchor cache, to avoid regenerating it for every TLS connection.

Definition at line 130 of file pubd.py.

11.33.3.6 pubd.pubd_context.irbe_cert

Definition at line 56 of file pubd.py.

11.33.3.7 pubd.pubd_context.pubd_cert

Definition at line 57 of file pubd.py.

11.33.3.8 pubd.pubd_context.pubd_key

Definition at line 58 of file pubd.py.

11.33.3.9 pubd.pubd_context.publication_base

Definition at line 63 of file pubd.py.

11.33.3.10 pubd.pubd_context.publication_multimodule

Definition at line 65 of file pubd.py.

11.33.3.11 pubd.pubd_context.sql

Definition at line 53 of file pubd.py.

The documentation for this class was generated from the following file:

- pubd.py (3107)

11.34 datetime Class Reference

Inherited by rpki.sundial.datetime.

The documentation for this class was generated from the following file:

- sundial.py (3191)

11.35 timedelta Class Reference

Inherited by rpki.sundial.timedelta.

The documentation for this class was generated from the following file:

- sundial.py (3191)

11.36 rootd.cms_msg Class Reference

Inherits rpki::up_down::cms_msg.

Collaboration diagram for rootd.cms_msg:

Static Public Attributes

- saxify = sax_handler.saxify

11.36.1 Detailed Description

Definition at line 235 of file rootd.py.

11.36.2 Member Data Documentation

11.36.2.1 rootd.cms_msg.saxify = sax_handler.saxify [static]

Reimplemented from rpki.up_down.cms_msg.

Definition at line 236 of file rootd.py.

The documentation for this class was generated from the following file:

- rootd.py (2913)

11.37 rootd.issue_pdu Class Reference

Inherits rpki::up_down::issue_pdu.

Collaboration diagram for rootd.issue_pdu:

Public Member Functions

- def serve_pdu

11.37.1 Detailed Description

Definition at line 194 of file rootd.py.

11.37.2 Member Function Documentation

11.37.2.1 def rootd.issue_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*, *callback*, *errback*)

```
Serve one issue request PDU.
```

Reimplemented from rpki.up_down.issue_pdu.

Definition at line 195 of file rootd.py.

The documentation for this class was generated from the following file:

- rootd.py (2913)

11.38 rootd.list_pdu Class Reference

Inherits rpki::up_down::list_pdu.

Collaboration diagram for rootd.list_pdu:

Public Member Functions

- def serve_pdu

11.38.1 Detailed Description

Definition at line 188 of file rootd.py.

11.38.2 Member Function Documentation

11.38.2.1 def rootd.list_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*, *callback*, *errback*)

```
Serve one "list" PDU.
```

Reimplemented from rpki.up_down.list_pdu.

Definition at line 189 of file rootd.py.

The documentation for this class was generated from the following file:

- rootd.py (2913)

11.39 rootd.message_pdu Class Reference

Inherits rpki::up_down::message_pdu.

Collaboration diagram for rootd.message_pdu:

Public Member Functions

- def log_query

Static Public Attributes

- dictionary name2type

- tuple type2name = dict((v, k) for k, v in name2type.items())

11.39.1 Detailed Description

Definition at line 213 of file rootd.py.

11.39.2 Member Function Documentation

11.39.2.1 def rootd.message_pdu.log_query (*self*, *child*)

```
Log query we're handling.
```

Reimplemented from rpki.up_down.message_pdu.

Definition at line 226 of file rootd.py.

11.39.3 Member Data Documentation

11.39.3.1 dictionary rootd.message_pdu.name2type [static]

Initial value:

```
{
    "list"            : list_pdu,
    "list_response"   : rpki.up_down.list_response_pdu,
    "issue"           : issue_pdu,
    "issue_response"  : rpki.up_down.issue_response_pdu,
    "revoke"          : revoke_pdu,
    "revoke_response" : rpki.up_down.revoke_response_pdu,
    "error_response"  : rpki.up_down.error_response_pdu }
```

Reimplemented from rpki.up_down.message_pdu.

Definition at line 215 of file rootd.py.

11.39.3.2 tuple rootd.message_pdu.type2name = dict((v, k) for k, v in name2type.items()) [static]

Reimplemented from rpki.up_down.message_pdu.

Definition at line 224 of file rootd.py.

The documentation for this class was generated from the following file:

- rootd.py (2913)

11.40 rootd.revoke_pdu Class Reference

Inherits rpki::up_down::revoke_pdu.

Collaboration diagram for rootd.revoke_pdu:

Public Member Functions

- def serve_pdu

11.40.1 Detailed Description

Definition at line 201 of file rootd.py.

11.40.2 Member Function Documentation

11.40.2.1 def rootd.revoke_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*, *cb*, *eb*)

```
Serve one revoke request PDU.
```

Reimplemented from rpki.up_down.revoke_pdu.

Definition at line 202 of file rootd.py.

The documentation for this class was generated from the following file:

- rootd.py (2913)

11.41 rootd.sax_handler Class Reference

Inherits rpki::up_down::sax_handler.

Collaboration diagram for rootd.sax_handler:

Static Public Attributes

- pdu = message_pdu

11.41.1 Detailed Description

Definition at line 232 of file rootd.py.

11.41.2 Member Data Documentation

11.41.2.1 rootd.sax_handler.pdu = message_pdu [static]

Reimplemented from rpki.up_down.sax_handler.

Definition at line 233 of file rootd.py.

The documentation for this class was generated from the following file:

- rootd.py (2913)

11.42 rpki.async.gc_summary Class Reference

Inherits object.

Collaboration diagram for rpki.async.gc_summary:

Public Member Functions

- def __init__

- def handler

Public Attributes

- interval
- threshold
- timer

11.42.1 Detailed Description

```
Periodic summary of GC state, for tracking down memory bloat.
```

Definition at line 368 of file async.py.

11.42.2 Member Function Documentation

11.42.2.1 def rpki.async.gc_summary.__init__ (*self*, *interval*, *threshold* = 0)

Definition at line 373 of file async.py.

11.42.2.2 def rpki.async.gc_summary.handler (*self*)

```
Collect and log GC state for this period, reset timer.
```

Definition at line 381 of file async.py.

11.42.3 Member Data Documentation

11.42.3.1 rpki.async.gc_summary.interval

Definition at line 376 of file async.py.

11.42.3.2 rpki.async.gc_summary.threshold

Definition at line 377 of file async.py.

11.42.3.3 rpki.async.gc_summary.timer

Definition at line 378 of file async.py.

The documentation for this class was generated from the following file:

- async.py (3191)

11.43 rpki.async.iterator Class Reference

Inherits object.

Collaboration diagram for rpki.async.iterator:

Public Member Functions

- def __call__
- def __init__
- def __repr__
- def doit

Public Attributes

- caller_function
- done_callback
- item_callback
- iterator
- unwind_stack

11.43.1 Detailed Description

```
Iteration construct for event-driven code.  Takes three
arguments:

- Some kind of iterable object

- A callback to call on each item in the iteration

- A callback to call after the iteration terminates.

The item callback receives two arguments: the callable iterator
object and the current value of the iteration.  It should call the
iterator (or arrange for the iterator to be called) when it is time
to continue to the next item in the iteration.

The termination callback receives no arguments.
```

Definition at line 26 of file async.py.

11.43.2 Member Function Documentation

11.43.2.1 def rpki.async.iterator.__call__ (*self*)

Definition at line 64 of file async.py.

11.43.2.2 def rpki.async.iterator.__init__ (*self*, *iterable*, *item_callback*, *done_callback*, *unwind_stack* = `True`)

Definition at line 45 of file async.py.

11.43.2.3 def rpki.async.iterator.__repr__ (*self*)

Definition at line 59 of file async.py.

11.43.2.4 def rpki.async.iterator.doit (*self*)

```
Implement the iterator protocol: attempt to call the item handler
with the next iteration value, call the termination handler if the
iterator signaled StopIteration.
```

Definition at line 70 of file async.py.

11.43.3 Member Data Documentation

11.43.3.1 rpki.async.iterator.caller_function

Definition at line 48 of file async.py.

11.43.3.2 rpki.async.iterator.done_callback

Definition at line 47 of file async.py.

11.43.3.3 rpki.async.iterator.item_callback

Definition at line 46 of file async.py.

11.43.3.4 rpki.async.iterator.iterator

Definition at line 51 of file async.py.

11.43.3.5 rpki.async.iterator.unwind_stack

Definition at line 49 of file async.py.

The documentation for this class was generated from the following file:

- async.py (3191)

11.44 rpki.async.sync_wrapper Class Reference

Inherits object.

Collaboration diagram for rpki.async.sync_wrapper:

Public Member Functions

- def __call__
- def __init__
- def cb
- def eb

Public Attributes

- func

Static Public Attributes

- err = None
- res = None

11.44.1 Detailed Description

```
Synchronous wrapper around asynchronous functions.  Running in
asynchronous mode at all times makes sense for event-driven daemons,
but is kind of tedious for simple scripts, hence this wrapper.

The wrapped function should take at least two arguments: a callback
function and an errback function.  If any arguments are passed to
the wrapper, they will be passed as additional arguments to the
wrapped function.
```

Definition at line 305 of file async.py.

11.44.2 Member Function Documentation

11.44.2.1 def rpki.async.sync_wrapper.__call__ (*self*, *args*, *kwargs*)

Definition at line 340 of file async.py.

11.44.2.2 def rpki.async.sync_wrapper.__init__ (*self*, *func*)

Definition at line 320 of file async.py.

11.44.2.3 def rpki.async.sync_wrapper.cb (*self*, *res* = `None`)

```
Wrapped code has requested normal termination.  Store result, and
exit the event loop.
```

Definition at line 323 of file async.py.

11.44.2.4 def rpki.async.sync_wrapper.eb (*self*, *err*)

```
Wrapped code raised an exception.  Store exception data, then exit
the event loop.
```

Definition at line 331 of file async.py.

11.44.3 Member Data Documentation

11.44.3.1 rpki.async.sync_wrapper.err = None [static]

Definition at line 318 of file async.py.

11.44.3.2 rpki.async.sync_wrapper.func

Definition at line 321 of file async.py.

11.44.3.3 rpki.async.sync_wrapper.res = None [static]

Definition at line 317 of file async.py.

The documentation for this class was generated from the following file:

- async.py (3191)

11.45 rpki.async.timer Class Reference

Inherits object.

Collaboration diagram for rpki.async.timer:

Public Member Functions

- def __cmp__
- def __del__
- def __init__
- def __repr__
- def cancel

- def clear
- def errback
- def handler
- def is_set
- def runq
- def seconds_until_wakeup
- def set
- def set_errback
- def set_handler
- def trace

Public Attributes

- errback
- handler
- when

Static Public Attributes

- gc_debug = False

  Verbose chatter about timers states and garbage collection.

- list queue = [ ]

  Timer queue, shared by all timer instances (there can be only one queue).

- run_debug = False

  Verbose chatter about timers being run.

11.45.1 Detailed Description

```
Timer construct for event-driven code.  It can be used in either of two ways:

- As a virtual class, in which case the subclass should provide a
  handler() method to receive the wakup event when the timer expires; or

- By setting an explicit handler callback, either via the
  constructor or the set_handler() method.

Subclassing is probably more Pythonic, but setting an explict
handler turns out to be very convenient when combined with bound
methods to other objects.
```

Definition at line 82 of file async.py.

11.45.2 Member Function Documentation

11.45.2.1 def rpki.async.timer.__cmp__ (*self*, *other*)

Definition at line 142 of file async.py.

11.45.2.2 def rpki.async.timer.__del__ (*self*)

Definition at line 146 of file async.py.

11.45.2.3 def rpki.async.timer.__init__ (*self*, *handler* = `None`, *errback* = `None`)

Definition at line 109 of file async.py.

11.45.2.4 def rpki.async.timer.__repr__ (*self*)

Definition at line 209 of file async.py.

11.45.2.5 def rpki.async.timer.cancel (*self*)

```
Cancel a timer, if it was set.
```

Definition at line 149 of file async.py.

11.45.2.6 def rpki.async.timer.clear (*cls*)

```
Cancel every timer on the queue.  We could just throw away the
queue content, but this way we can notify subclasses that provide
their own cancel() method.
```

Definition at line 234 of file async.py.

11.45.2.7 def rpki.async.timer.errback (*self*, *e*)

```
Error callback.  May be overridden, or set with set_errback().
```

Definition at line 181 of file async.py.

11.45.2.8 def rpki.async.timer.handler (*self*)

```
Handle a timer that has expired.  This must either be overriden by
a subclass or set dynamically by set_handler().
```

Definition at line 164 of file async.py.

11.45.2.9 def rpki.async.timer.is_set (*self*)

```
Test whether this timer is currently set.
```

Definition at line 160 of file async.py.

11.45.2.10 def rpki.async.timer.runq (*cls*)

```
Run the timer queue: for each timer whose call time has passed,
pull the timer off the queue and call its handler() method.
```

Definition at line 193 of file async.py.

11.45.2.11 def rpki.async.timer.seconds_until_wakeup (*cls*)

```
Calculate delay until next timer expires, or None if no timers are
set and we should wait indefinitely.  Rounds up to avoid spinning
in select() or poll().  We could calculate fractional seconds in
the right units instead, but select() and poll() don't even take
the same units (argh!), and we're not doing anything that
hair-triggered, so rounding up is simplest.
```

Definition at line 213 of file async.py.

11.45.2.12 def rpki.async.timer.set (*self*, *when*)

```
Set a timer.  Argument can be a datetime, to specify an absolute
time, or a timedelta, to specify an offset time.
```

Definition at line 126 of file async.py.

11.45.2.13 def rpki.async.timer.set_errback (*self*, *errback*)

```
Set a timer's errback.  Like set_handler(), for errbacks.
```

Definition at line 188 of file async.py.

11.45.2.14 def rpki.async.timer.set_handler (*self*, *handler*)

```
Set timer's expiration handler.  This is an alternative to
subclassing the timer class, and may be easier to use when
integrating timers into other classes (eg, the handler can be a
bound method to an object in a class representing a network
connection).
```

Definition at line 171 of file async.py.

11.45.2.15 def rpki.async.timer.trace (*self*, *msg*)

```
Debug logging.
```

Definition at line 118 of file async.py.

11.45.3 Member Data Documentation

11.45.3.1 rpki.async.timer.errback

Definition at line 190 of file async.py.

11.45.3.2 rpki::async.timer::gc_debug = False [static]

Verbose chatter about timers states and garbage collection.

Definition at line 99 of file async.py.

11.45.3.3 rpki.async.timer.handler

Definition at line 179 of file async.py.

11.45.3.4 rpki::async.timer::queue = [] [static]

Timer queue, shared by all timer instances (there can be only one queue).

Definition at line 107 of file async.py.

11.45.3.5 rpki::async.timer::run_debug = False [static]

Verbose chatter about timers being run.

Definition at line 103 of file async.py.

11.45.3.6 rpki.async.timer.when

Definition at line 114 of file async.py.

The documentation for this class was generated from the following file:

- async.py (3191)

11.46 rpki.cli.Cmd Class Reference

Inherits cmd::Cmd.

Collaboration diagram for rpki.cli.Cmd:

Public Member Functions

- def __init__
- def cmdloop_with_history
- def complete_help
- def completenames

- def do_EOF
- def do_exit
- def emptyline
- def filename_complete
- def help_help
- def onecmd

Static Public Attributes

- cmdloop_with_history = cmd.Cmd.cmdloop
- do_quit = do_exit
- emptyline_repeats_last_command = False
- EOF_exits_command_loop = True
- histfile = None
- string identchars = "/-."

11.46.1 Detailed Description

```
Customized subclass of Python cmd module.
```

Definition at line 29 of file cli.py.

11.46.2 Member Function Documentation

11.46.2.1 def rpki.cli.Cmd.__init__ (*self*, *argv* = `None`)

Definition at line 42 of file cli.py.

11.46.2.2 def rpki.cli.Cmd.cmdloop_with_history (*self*)

```
Better command loop, with history file and tweaked readline
completion delimiters.
```

Definition at line 132 of file cli.py.

11.46.2.3 def rpki.cli.Cmd.complete_help (*self*, *args*)

```
Better completion function for help command arguments.
```

Definition at line 119 of file cli.py.

11.46.2.4 def rpki.cli.Cmd.completenames (*self*, *text*, *ignored*)

```
Command name completion handler, with hack to restore what I
consider the normal (bash-like) behavior when one hits the
completion key and there's only one match.
```

Definition at line 101 of file cli.py.

11.46.2.5 def rpki.cli.Cmd.do_EOF (*self*, *arg*)

```
Exit program.
```

Definition at line 61 of file cli.py.

11.46.2.6 def rpki.cli.Cmd.do_exit (*self*, *arg*)

```
Exit program.
```

Definition at line 69 of file cli.py.

11.46.2.7 def rpki.cli.Cmd.emptyline (*self*)

```
Handle an empty line.  cmd module default is to repeat the last
command, which I find to be violation of the principal of least
astonishment, so my preference is that an empty line does nothing.
```

Definition at line 77 of file cli.py.

11.46.2.8 def rpki.cli.Cmd.filename_complete (*self*, *text*, *line*, *begidx*, *endidx*)

```
Filename completion handler, with hack to restore what I consider
the normal (bash-like) behavior when one hits the completion key
and there's only one match.
```

Definition at line 86 of file cli.py.

11.46.2.9 def rpki.cli.Cmd.help_help (*self*)

```
Type "help [topic]" for help on a command,
or just "help" for a list of commands.
```

Definition at line 112 of file cli.py.

11.46.2.10 def rpki.cli.Cmd.onecmd (*self*, *line*)

```
Wrap error handling around cmd.Cmd.onecmd().  Might want to do
something kinder than showing a traceback, eventually.
```

Definition at line 49 of file cli.py.

11.46.3 Member Data Documentation

11.46.3.1 rpki.cli.Cmd.cmdloop_with_history = cmd.Cmd.cmdloop [static]

Definition at line 153 of file cli.py.

11.46.3.2 rpki.cli.Cmd.do_quit = do_exit [static]

Definition at line 75 of file cli.py.

11.46.3.3 rpki.cli.Cmd.emptyline_repeats_last_command = False [static]

Definition at line 34 of file cli.py.

11.46.3.4 rpki.cli.Cmd.EOF_exits_command_loop = True [static]

Definition at line 36 of file cli.py.

11.46.3.5 rpki.cli.Cmd.histfile = None [static]

Definition at line 40 of file cli.py.

11.46.3.6 string rpki.cli.Cmd.identchars = "/-." [static]

Definition at line 38 of file cli.py.

The documentation for this class was generated from the following file:

- cli.py (3191)

11.47 rpki.config.parser Class Reference

Inherits object.

Collaboration diagram for rpki.config.parser:

Public Member Functions

- def __init__
- def get
- def getboolean
- def getint

- def getlong
- def has_option
- def has_section
- def multiget
- def set_global_flags

Public Attributes

- cfg
- default_section
- filename

Private Member Functions

- def _repl

Static Private Attributes

- tuple _regexp = re.compile("\\${(.*?)::(.*?)}")

11.47.1 Detailed Description

```
Extensions to stock Python ConfigParser:

Read config file and set default section while initializing parser object.

Support for OpenSSL-style subscripted options and a limited form of
OpenSSL-style indirect variable references (${section::option}).

get-methods with default values and default section name.
```

Definition at line 38 of file config.py.

11.47.2 Member Function Documentation

11.47.2.1 def rpki.config.parser.__init__ (*self*, *filename*, *section* = `None`, *allow_missing* = `False`)

```
Initialize this parser.
```

Definition at line 50 of file config.py.

11.47.2.2 def rpki.config.parser._repl (*self*, *m*) [private]

```
Replacement function for indirect variable substitution.
This is intended for use with re.subn().
```

Definition at line 101 of file config.py.

11.47.2.3 def rpki.config.parser.get (*self*, *option*, *default* = None, *section* = None)

```
Get an option, perhaps with a default value.
```

Definition at line 112 of file config.py.

11.47.2.4 def rpki.config.parser.getboolean (*self*, *option*, *default* = None, *section* = None)

```
Get a boolean option, perhaps with a default value.
```

Definition at line 126 of file config.py.

11.47.2.5 def rpki.config.parser.getint (*self*, *option*, *default* = None, *section* = None)

```
Get an integer option, perhaps with a default value.
```

Definition at line 138 of file config.py.

11.47.2.6 def rpki.config.parser.getlong (*self*, *option*, *default* = None, *section* = None)

```
Get a long integer option, perhaps with a default value.
```

Definition at line 144 of file config.py.

11.47.2.7 def rpki.config.parser.has_option (*self*, *option*, *section* = `None`)

```
Test whether an option exists.
```

Definition at line 71 of file config.py.

11.47.2.8 def rpki.config.parser.has_section (*self*, *section*)

```
Test whether a section exists.
```

Definition at line 64 of file config.py.

11.47.2.9 def rpki.config.parser.multiget (*self*, *option*, *section* = `None`)

```
Parse OpenSSL-style foo.0, foo.1, ... subscripted options.

Returns a list of values matching the specified option name.
```

Definition at line 80 of file config.py.

11.47.2.10 def rpki.config.parser.set_global_flags (*self*)

```
Consolidated control for all the little global control flags
scattered through the libraries.  This isn't a particularly good
place for this function to live, but it has to live somewhere and
making it a method of the config parser from which it gets all of
its data is less silly than the available alternatives.
```

Definition at line 150 of file config.py.

11.47.3 Member Data Documentation

11.47.3.1 tuple rpki.config.parser._regexp = re.compile("\\${(.*?)::(.*?)}") `[static, private]`

Definition at line 99 of file config.py.

11.47.3.2 rpki.config.parser.cfg

Definition at line 56 of file config.py.

11.47.3.3 rpki.config.parser.default_section

Definition at line 62 of file config.py.

11.47.3.4 rpki.config.parser.filename

Definition at line 55 of file config.py.

The documentation for this class was generated from the following file:

- config.py (3107)

11.48 rpki.exceptions.BadClassNameSyntax Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadClassNameSyntax:

11.48.1 Detailed Description

```
Illegal syntax for a class_name.
```

Definition at line 92 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.49 rpki.exceptions.BadClientURL Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadClientURL:

11.49.1 Detailed Description

```
URL given to HTTPS client does not match profile.
```

Definition at line 232 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.50 rpki.exceptions.BadContactURL Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadContactURL:

11.50.1 Detailed Description

```
Error trying to parse contact URL.
```

Definition at line 87 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.51 rpki.exceptions.BadExtension Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadExtension:

11.51.1 Detailed Description

```
Forbidden X.509 extension.
```

Definition at line 242 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.52 rpki.exceptions.BadIRDBReply Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadIRDBReply:

11.52.1 Detailed Description

```
Unexpected reply to IRDB query.
```

Definition at line 152 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.53 rpki.exceptions.BadIssueResponse Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadIssueResponse:

11.53.1 Detailed Description

```
issue_response PDU with wrong number of classes or certificates.
```

Definition at line 97 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.54 rpki.exceptions.BadPKCS10 Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadPKCS10:

11.54.1 Detailed Description

```
Bad PKCS #10 object.
```

Definition at line 107 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.55 rpki.exceptions.BadPublicationReply Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadPublicationReply:

11.55.1 Detailed Description

```
Unexpected reply to publication query.
```

Definition at line 257 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.56 rpki.exceptions.BadQuery Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadQuery:

11.56.1 Detailed Description

```
Unexpected protocol query.
```

Definition at line 55 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.57 rpki.exceptions.BadSender Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadSender:

11.57.1 Detailed Description

```
Unexpected XML sender value.
```

Definition at line 127 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.58 rpki.exceptions.BadStatusCode Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadStatusCode:

11.58.1 Detailed Description

```
Unrecognized protocol status code.
```

Definition at line 50 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.59 rpki.exceptions.BadURISyntax Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadURISyntax:

11.59.1 Detailed Description

```
Illegal syntax for a URI.
```

Definition at line 45 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.60 rpki.exceptions.BSCNotFound Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BSCNotFound:

11.60.1 Detailed Description

```
Could not find specified BSC in database.
```

Definition at line 122 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.61 rpki.exceptions.BSCNotReady Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BSCNotReady:

11.61.1 Detailed Description

```
BSC not yet in a usable state, signing_cert not set.
```

Definition at line 277 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.62 rpki.exceptions.ChildNotFound Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.ChildNotFound:

11.62.1 Detailed Description

```
Could not find specified child in database.
```

Definition at line 117 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.63 rpki.exceptions.ClassNameMismatch Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.ClassNameMismatch:

11.63.1 Detailed Description

```
class_name does not match child context.
```

Definition at line 132 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.64 rpki.exceptions.ClassNameUnknown Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.ClassNameUnknown:

11.64.1 Detailed Description

```
Unknown class_name.
```

Definition at line 137 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.65 rpki.exceptions.ClientNotFound Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.ClientNotFound:

11.65.1 Detailed Description

```
Could not find specified client in database.
```

Definition at line 237 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.66 rpki.exceptions.CMSContentNotSet Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.CMSContentNotSet:

11.66.1 Detailed Description

```
Inner content of a CMS_object has not been set.  If object is known
to be valid, the .extract() method should be able to set the
content; otherwise, only the .verify() method (which checks
signatures) is safe.
```

Definition at line 302 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.67 rpki.exceptions.CMSCRLNotSet Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.CMSCRLNotSet:

11.67.1 Detailed Description

```
CMS CRL has not been configured.
```

Definition at line 217 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.68 rpki.exceptions.CMSVerificationFailed Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.CMSVerificationFailed:

11.68.1 Detailed Description

```
Verification of a CMS message failed.
```

Definition at line 66 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.69 rpki.exceptions.DBConsistancyError Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.DBConsistancyError:

11.69.1 Detailed Description

```
Found multiple matches for a database query that shouldn't ever
return that.
```

Definition at line 60 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.70 rpki.exceptions.DERObjectConversionError Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.DERObjectConversionError:

11.70.1 Detailed Description

```
Error trying to convert a DER-based object from one representation
to another.
```

Definition at line 76 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.71 rpki.exceptions.DuplicateObject Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.DuplicateObject:

11.71.1 Detailed Description

```
Attempt to create an object that already exists.
```

Definition at line 262 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.72 rpki.exceptions.EmptyPEM Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.EmptyPEM:

11.72.1 Detailed Description

```
Couldn't find PEM block to convert.
```

Definition at line 187 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.73 rpki.exceptions.EmptyROAPrefixList Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.EmptyROAPrefixList:

11.73.1 Detailed Description

```
Can't create ROA with an empty prefix list.
```

Definition at line 267 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.74 rpki.exceptions.ForbiddenURI Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.ForbiddenURI:

11.74.1 Detailed Description

```
Forbidden URI, does not start with correct base URI.
```

Definition at line 247 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.75 rpki.exceptions.HandleTranslationError Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.HandleTranslationError:

11.75.1 Detailed Description

```
Internal error translating protocol handle -> SQL id.
```

Definition at line 292 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.76 rpki.exceptions.HTTPRequestFailed Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.HTTPRequestFailed:

11.76.1 Detailed Description

```
HTTP request failed.
```

Definition at line 71 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.77 rpki.exceptions.HTTPSBadVersion Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.HTTPSBadVersion:

11.77.1 Detailed Description

```
HTTPS couldn't parse HTTP version.
```

Definition at line 287 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.78 rpki.exceptions.HTTPSClientAborted Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.HTTPSClientAborted:

11.78.1 Detailed Description

```
HTTPS client connection closed while in request-sent state.
```

Definition at line 252 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.79 rpki.exceptions.HTTPSUnexpectedState Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.HTTPSUnexpectedState:

11.79.1 Detailed Description

```
HTTPS event occurred in an unexpected state.
```

Definition at line 282 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.80 rpki.exceptions.MissingCMSCRL Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.MissingCMSCRL:

11.80.1 Detailed Description

```
Didn't receive CMS CRL when expecting one.
```

Definition at line 207 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.81 rpki.exceptions.MissingCMSEEcert Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.MissingCMSEEcert:

11.81.1 Detailed Description

```
Didn't receive CMS EE cert when expecting one.
```

Definition at line 202 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.82 rpki.exceptions.MultipleTLSEECert Class Reference

Inherits rpki::exceptions::TLSValidationError.

Collaboration diagram for rpki.exceptions.MultipleTLSEECert:

11.82.1 Detailed Description

```
Received more than one TLS EE certificate.
```

Definition at line 172 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.83 rpki.exceptions.MustBePrefix Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.MustBePrefix:

11.83.1 Detailed Description

```
Resource range cannot be expressed as a prefix.
```

Definition at line 162 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.84 rpki.exceptions.NoActiveCA Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.NoActiveCA:

11.84.1 Detailed Description

```
No active ca_detail for specified class.
```

Definition at line 227 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.85 rpki.exceptions.NoCoveringCertForROA Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.NoCoveringCertForROA:

11.85.1 Detailed Description

```
Couldn't find a covering certificate to generate ROA.
```

Definition at line 272 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.86 rpki.exceptions.NoObjectAtURI Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.NoObjectAtURI:

11.86.1 Detailed Description

```
No object published at specified URI.
```

Definition at line 297 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.87 rpki.exceptions.NotACertificateChain Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.NotACertificateChain:

11.87.1 Detailed Description

```
Certificates don't form a proper chain.
```

Definition at line 82 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.88 rpki.exceptions.NotFound Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.NotFound:

11.88.1 Detailed Description

```
Object not found in database.
```

Definition at line 157 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.89 rpki.exceptions.NotImplementedYet Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.NotImplementedYet:

11.89.1 Detailed Description

```
Internal error -- not implemented yet.
```

Definition at line 102 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.90 rpki.exceptions.NotInDatabase Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.NotInDatabase:

11.90.1 Detailed Description

```
Lookup failed for an object expected to be in the database.
```

Definition at line 40 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.91 rpki.exceptions.ReceivedTLSCACert Class Reference

Inherits rpki::exceptions::TLSValidationError.

Collaboration diagram for rpki.exceptions.ReceivedTLSCACert:

11.91.1 Detailed Description

`Received CA certificate via TLS.`

Definition at line 177 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.92 rpki.exceptions.RPKI_Exception Class Reference

Inherits Exception.

Inherited by rpki.exceptions.BadClassNameSyntax, rpki.exceptions.BadClientURL, rpki.exceptions.BadContactURL, rpki.exceptions.BadExtension, rpki.exceptions.BadIRDBReply, rpki.exceptions.BadIssueResponse, rpki.exceptions.BadPKCS10, rpki.exceptions.BadPublicationReply, rpki.exceptions.BadQuery, rpki.exceptions.BadSender, rpki.exceptions.BadStatusCode, rpki.exceptions.BadURISyntax, rpki.exceptions.BSCNotFound, rpki.exceptions.BSCNotReady, rpki.exceptions.ChildNotFound, rpki.exceptions.ClassNameMismatch, rpki.exceptions.ClassNameUnknown, rpki.exceptions.ClientNotFound, rpki.exceptions.CMSContentNotSet, rpki.exceptions.CMSCRLNotSet, rpki.exceptions.CMSVerificationFailed, rpki.exceptions.DBConsistancyError, rpki.exceptions.DERObjectConversionError, rpki.exceptions.DuplicateObject, rpki.exceptions.EmptyPEM, rpki.exceptions.EmptyROAPrefixList, rpki.exceptions.ForbiddenURI, rpki.exceptions.HandleTranslationError, rpki.exceptions.HTTPRequestFailed, rpki.exceptions.HTTPSBadVersion, rpki.exceptions.HTTPSClientAborted, rpki.exceptions.HTTPSUnexpectedState, rpki.exceptions.MissingCMSCRL, rpki.exceptions.MissingCMSEEcert, rpki.exceptions.MustBePrefix, rpki.exceptions.NoActiveCA, rpki.exceptions.NoCoveringCertForROA, rpki.exceptions.NoObjectAtURI, rpki.exceptions.NotACertificateChain, rpki.exceptions.NotFound, rpki.exceptions.NotImplementedYet, rpki.exceptions.NotInDatabase, rpki.exceptions.ServerShuttingDown, rpki.exceptions.SKIMismatch, rpki.exceptions.SubprocessError, rpki.exceptions.TLSValidationError, rpki.exceptions.UnexpectedCMSCerts, rpki.exceptions.UnexpectedCMSCRLs, rpki.exceptions.UnparsableCMSDER, rpki.exceptions.UpstreamError, and rpki.exceptions.WrongEContentType.

Collaboration diagram for rpki.exceptions.RPKI_Exception:

11.92.1 Detailed Description

```
Base class for RPKI exceptions.
```

Definition at line 35 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.93 rpki.exceptions.ServerShuttingDown Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.ServerShuttingDown:

11.93.1 Detailed Description

```
Server is shutting down.
```

Definition at line 222 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.94 rpki.exceptions.SKIMismatch Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.SKIMismatch:

11.94.1 Detailed Description

```
SKI value in response does not match request.
```

Definition at line 142 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.95 rpki.exceptions.SubprocessError Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.SubprocessError:

11.95.1 Detailed Description

```
Subprocess returned unexpected error.
```

Definition at line 147 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.96 rpki.exceptions.TLSValidationError Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Inherited by rpki.exceptions.MultipleTLSEECert, and rpki.exceptions.ReceivedTLSCACert.

Collaboration diagram for rpki.exceptions.TLSValidationError:

11.96.1 Detailed Description

```
TLS certificate validation error.
```

Definition at line 167 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.97 rpki.exceptions.UnexpectedCMSCerts Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.UnexpectedCMSCerts:

11.97.1 Detailed Description

```
Received CMS certs when not expecting any.
```

Definition at line 192 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.98 rpki.exceptions.UnexpectedCMSCRLs Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.UnexpectedCMSCRLs:

11.98.1 Detailed Description

```
Received CMS CRLs when not expecting any.
```

Definition at line 197 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.99 rpki.exceptions.UnparsableCMSDER Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.UnparsableCMSDER:

11.99.1 Detailed Description

```
Alleged CMS DER wasn't parsable.
```

Definition at line 212 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.100 rpki.exceptions.UpstreamError Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.UpstreamError:

11.100.1 Detailed Description

```
Received an error from upstream.
```

Definition at line 112 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.101 rpki.exceptions.WrongEContentType Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.WrongEContentType:

11.101.1 Detailed Description

`Received wrong CMS eContentType.`

Definition at line 182 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

11.102 rpki.https.caller Class Reference

Inherits object.

Collaboration diagram for rpki.https.caller:

Public Member Functions

- def __call__
- def __init__

Public Attributes

- client_cert

- client_key
- proto
- server_cert
- server_ta
- url

Static Public Attributes

- debug = False

11.102.1 Detailed Description

```
Handle client-side mechanics for protocols based on HTTPS, CMS, and
rpki.xml_utils.  Calling sequence is intended to nest within
rpki.async.sync_wrapper.
```

Definition at line 1105 of file https.py.

11.102.2 Member Function Documentation

11.102.2.1 def rpki.https.caller.__call__ (*self*, *cb*, *eb*, *pdus*)

Definition at line 1124 of file https.py.

11.102.2.2 def rpki.https.caller.__init__ (*self*, *proto*, *client_key*, *client_cert*, *server_ta*, *server_cert*, *url*, *debug* = `None`)

Definition at line 1114 of file https.py.

11.102.3 Member Data Documentation

11.102.3.1 rpki.https.caller.client_cert

Definition at line 1117 of file https.py.

11.102.3.2 rpki.https.caller.client_key

Definition at line 1116 of file https.py.

11.102.3.3 rpki.https.caller.debug = False [static]

Definition at line 1112 of file https.py.

11.102.3.4 rpki.https.caller.proto

Definition at line 1115 of file https.py.

11.102.3.5 rpki.https.caller.server_cert

Definition at line 1119 of file https.py.

11.102.3.6 rpki.https.caller.server_ta

Definition at line 1118 of file https.py.

11.102.3.7 rpki.https.caller.url

Definition at line 1120 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

11.103 rpki.https.http_client Class Reference

Inherits rpki::https::http_stream.

Collaboration diagram for rpki.https.http_client:

Public Member Functions

- def __init__
- def handle_close
- def handle_connect
- def handle_error
- def handle_message

- def handle_no_content_length
- def handle_timeout
- def send_request
- def set_state
- def start
- def tls_connect

Public Attributes

- af
- cert
- expect_close
- hostport
- key
- queue
- retry_read
- retry_write
- state
- ta
- tls

Static Public Attributes

- parse_type = http_response

  Stream parser should look for incoming HTTP response messages.

- timeout = default_client_timeout

  Use the default client timeout value set in the module header.

11.103.1 Detailed Description

```
HTTP(S) client stream.
```

Definition at line 759 of file https.py.

11.103.2 Member Function Documentation

11.103.2.1 def rpki.https.http_client.__init__ (*self*, *queue*, *hostport*, *cert* = `None`, *key* = `None`, *ta* = `()`, *af* = supported_address_families`[0]`)

Definition at line 772 of file https.py.

11.103.2.2 def rpki.https.http_client.handle_close (*self*)

```
Asyncore signaled connection close.  If we were waiting for that
to find the end of a response message, process the resulting
message now; if we were waiting for the response to a request we
sent, signal the error.
```

Reimplemented from rpki.https.http_stream.

Definition at line 892 of file https.py.

11.103.2.3 def rpki.https.http_client.handle_connect (*self*)

```
Asyncore says socket has connected, configure TLS junk.
```

Definition at line 797 of file https.py.

11.103.2.4 def rpki.https.http_client.handle_error (*self*)

```
Asyncore says something threw an exception.  Log it, then shut
down the connection and pass back the exception.
```

Reimplemented from rpki.https.http_stream.

Definition at line 918 of file https.py.

11.103.2.5 def rpki.https.http_client.handle_message (*self*)

```
Handle incoming HTTP response message.  Make sure we're in a state
where we expect to see such a message (and allow the mysterious
empty messages that Apache sends during connection close, no idea
what that is supposed to be about).  If everybody agrees that the
connection should stay open, put it into an idle state; otherwise,
arrange for the stream to shut down.
```

Definition at line 856 of file https.py.

11.103.2.6 def rpki.https.http_client.handle_no_content_length (*self*)

```
Handle response message that used neither chunking nor a
Content-Length header (that is: this message will be the last one
in this server stream).  In this case we want to read until we
reach the end of the data stream.
```

Definition at line 836 of file https.py.

11.103.2.7 def rpki.https.http_client.handle_timeout (*self*)

```
Connection idle timer has expired.  If we weren't idle, log that
something bad has happened, then shut down the connection in any
case.
```

Reimplemented from rpki.https.http_stream.

Definition at line 907 of file https.py.

11.103.2.8 def rpki.https.http_client.send_request (*self*, *msg*)

```
Queue up request message and kickstart connection.
```

Definition at line 845 of file https.py.

11.103.2.9 def rpki.https.http_client.set_state (*self*, *state*)

```
Set HTTP client connection state.
```

Definition at line 829 of file https.py.

11.103.2.10 def rpki.https.http_client.start (*self*)

```
Create socket and request a connection.
```

Definition at line 785 of file https.py.

11.103.2.11 def rpki.https.http_client.tls_connect (*self*)

```
Initialize client side of TLS.
```

Definition at line 814 of file https.py.

11.103.3 Member Data Documentation

11.103.3.1 rpki.https.http_client.af

Definition at line 783 of file https.py.

11.103.3.2 rpki.https.http_client.cert

Definition at line 780 of file https.py.

11.103.3.3 rpki.https.http_client.expect_close

Definition at line 779 of file https.py.

11.103.3.4 rpki.https.http_client.hostport

Definition at line 777 of file https.py.

11.103.3.5 rpki.https.http_client.key

Definition at line 781 of file https.py.

11.103.3.6 rpki::https.http_client::parse_type = http_response [static]

Stream parser should look for incoming HTTP response messages.

Definition at line 766 of file https.py.

11.103.3.7 rpki.https.http_client.queue

Definition at line 776 of file https.py.

11.103.3.8 rpki.https.http_client.retry_read

Reimplemented from rpki.https.http_stream.

Definition at line 821 of file https.py.

11.103.3.9 rpki.https.http_client.retry_write

Reimplemented from rpki.https.http_stream.

Definition at line 823 of file https.py.

11.103.3.10 rpki.https.http_client.state

Definition at line 778 of file https.py.

11.103.3.11 rpki.https.http_client.ta

Definition at line 782 of file https.py.

11.103.3.12 rpki::https.http_client::timeout = default_client_timeout [static]

Use the default client timeout value set in the module header.

Definition at line 770 of file https.py.

11.103.3.13 rpki.https.http_client.tls

Reimplemented from rpki.https.http_stream.

Definition at line 802 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

11.104 rpki.https.http_listener Class Reference

Inherits asyncore::dispatcher.

Collaboration diagram for rpki.https.http_listener:

Public Member Functions

- def __init__
- def handle_accept
- def handle_error

Public Attributes

- cert
- dynamic_ta
- handlers
- key
- ta

Static Public Attributes

- log = log_method

11.104.1 Detailed Description

```
Listener for incoming HTTP(S) connections.
```

Definition at line 707 of file https.py.

11.104.2 Member Function Documentation

11.104.2.1 def rpki.https.http_listener.__init__ (*self*, *handlers*, *port* = `80`, *host* = `""`, *cert* = `None`, *key* = `None`, *ta* = `None`, *dynamic_ta* = `None`, *af* = supported_address_families`[0]`)

Definition at line 714 of file https.py.

11.104.2.2 def rpki.https.http_listener.handle_accept (*self*)

```
Asyncore says we have an incoming connection, spawn an http_server
stream for it and pass along all of our handler and TLS data.
```

Definition at line 735 of file https.py.

11.104.2.3 def rpki.https.http_listener.handle_error (*self*)

```
Asyncore signaled an error, pass it along or log it.
```

Definition at line 748 of file https.py.

11.104.3 Member Data Documentation

11.104.3.1 rpki.https.http_listener.cert

Definition at line 718 of file https.py.

11.104.3.2 rpki.https.http_listener.dynamic_ta

Definition at line 721 of file https.py.

11.104.3.3 rpki.https.http_listener.handlers

Definition at line 717 of file https.py.

11.104.3.4 rpki.https.http_listener.key

Definition at line 719 of file https.py.

11.104.3.5 rpki.https.http_listener.log = log_method [static]

Definition at line 712 of file https.py.

11.104.3.6 rpki.https.http_listener.ta

Definition at line 720 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

11.105 rpki.https.http_message Class Reference

Inherits object.

Inherited by rpki.https.http_request, and rpki.https.http_response.

Collaboration diagram for rpki.https.http_message:

Public Member Functions

- def __init__
- def __str__
- def format
- def normalize_headers
- def parse_from_wire
- def parse_version
- def persistent

Public Attributes

- body
- headers
- version

Static Public Attributes

- string software_name = "ISC RPKI library"

11.105.1 Detailed Description

```
Virtual class representing of one HTTP message.
```

Definition at line 90 of file https.py.

11.105.2 Member Function Documentation

11.105.2.1 def rpki.https.http_message.__init__ (*self*, *version* = `None`, *body* = `None`, *headers* = `None`)

Definition at line 97 of file https.py.

11.105.2.2 def rpki.https.http_message.__str__ (*self*)

Definition at line 155 of file https.py.

11.105.2.3 def rpki.https.http_message.format (*self*)

```
Format an outgoing HTTP message.
```

Definition at line 140 of file https.py.

11.105.2.4 def rpki.https.http_message.normalize_headers (*self*, *headers* = None)

```
Clean up (some of) the horrible messes that HTTP allows in its
headers.
```

Definition at line 103 of file https.py.

11.105.2.5 def rpki.https.http_message.parse_from_wire (*cls*, *headers*)

```
Parse and normalize an incoming HTTP message.
```

Definition at line 126 of file https.py.

11.105.2.6 def rpki.https.http_message.parse_version (*self*, *version*)

```
Parse HTTP version, raise an exception if we can't.
```

Definition at line 158 of file https.py.

11.105.2.7 def rpki.https.http_message.persistent (*self*)

```
Figure out whether this HTTP message encourages a persistent connection.
```

Definition at line 166 of file https.py.

11.105.3 Member Data Documentation

11.105.3.1 rpki.https.http_message.body

Definition at line 99 of file https.py.

11.105.3.2 rpki.https.http_message.headers

Definition at line 100 of file https.py.

11.105.3.3 string rpki.https.http_message.software_name = "ISC RPKI library" [static]

Definition at line 95 of file https.py.

11.105.3.4 rpki.https.http_message.version

Definition at line 98 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

11.106 rpki.https.http_queue Class Reference

Inherits object.

Collaboration diagram for rpki.https.http_queue:

Public Member Functions

- def __init__
- def detach
- def request
- def restart
- def return_result
- def send_request

Public Attributes

- cert
- client
- hostport
- key
- queue
- ta

Static Public Attributes

- log = log_method

11.106.1 Detailed Description

```
Queue of pending HTTP requests for a single destination.  This class
is very tightly coupled to http_client; http_client handles the HTTP
stream itself, this class provides a slightly higher-level API.
```

Definition at line 929 of file https.py.

11.106.2 Member Function Documentation

11.106.2.1 def rpki.https.http_queue.__init__ (*self*, *hostport*, *cert* = `None`, *key* = `None`, *ta* = `()`)

Definition at line 938 of file https.py.

11.106.2.2 def rpki.https.http_queue.detach (*self*, *client_*)

```
Detatch a client from this queue.  Silently ignores attempting to
detach a client that is not attached to this queue, to simplify
handling of what otherwise would be a nasty set of race
conditions.
```

Definition at line 986 of file https.py.

11.106.2.3 def rpki.https.http_queue.request (*self*, *requests*)

```
Append http_request object(s) to this queue.
```

Definition at line 948 of file https.py.

11.106.2.4 def rpki.https.http_queue.restart (*self*)

```
Send next request for this queue, if we can.  This may involve
starting a new http_client stream, reusing an existing idle
stream, or just ignoring this request if there's an active client
stream already; in the last case, handling of the response (or
exception, or timeout) for the query currently in progress will
call this method when it's time to kick out the next query.
```

Definition at line 955 of file https.py.

11.106.2.5 def rpki.https.http_queue.return_result (*self*, *result*)

```
Client stream has returned a result, which we need to pass along
to the original caller.  Result may be either an HTTP response
message or an exception.  In either case, once we're done
processing this result, kick off next message in the queue, if any.
```

Definition at line 997 of file https.py.

11.106.2.6 def rpki.https.http_queue.send_request (*self*)

```
Kick out the next query in this queue, if any.
```

Definition at line 979 of file https.py.

11.106.3 Member Data Documentation

11.106.3.1 rpki.https.http_queue.cert

Definition at line 944 of file https.py.

11.106.3.2 rpki.https.http_queue.client

Definition at line 942 of file https.py.

11.106.3.3 rpki.https.http_queue.hostport

Definition at line 941 of file https.py.

11.106.3.4 rpki.https.http_queue.key

Definition at line 945 of file https.py.

11.106.3.5 rpki.https.http_queue.log = log_method [static]

Definition at line 936 of file https.py.

11.106.3.6 rpki.https.http_queue.queue

Definition at line 943 of file https.py.

11.106.3.7 rpki.https.http_queue.ta

Definition at line 946 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

11.107 rpki.https.http_request Class Reference

Inherits rpki::https::http_message.

Collaboration diagram for rpki.https.http_request:

Public Member Functions

- def __init__
- def format_first_line
- def parse_first_line

Public Attributes

- callback
- cmd
- errback
- path
- retried

11.107.1 Detailed Description

```
HTTP request message.
```

Definition at line 178 of file https.py.

11.107.2 Member Function Documentation

11.107.2.1 def rpki.https.http_request.__init__ (*self*, *cmd* = `None`, *path* = `None`, *version* = default_http_version, *body* = `None`, *callback* = `None`, *errback* = `None`, *headers*)

Definition at line 183 of file https.py.

11.107.2.2 def rpki.https.http_request.format_first_line (*self*)

```
Format first line of HTTP request message, and set up the
User-Agent header.
```

Definition at line 200 of file https.py.

11.107.2.3 def rpki.https.http_request.parse_first_line (*self*, *cmd*, *path*, *version*)

```
Parse first line of HTTP request message.
```

Definition at line 192 of file https.py.

11.107.3 Member Data Documentation

11.107.3.1 rpki.https.http_request.callback

Definition at line 188 of file https.py.

11.107.3.2 rpki.https.http_request.cmd

Definition at line 186 of file https.py.

11.107.3.3 rpki.https.http_request.errback

Definition at line 189 of file https.py.

11.107.3.4 rpki.https.http_request.path

Definition at line 187 of file https.py.

11.107.3.5 rpki.https.http_request.retried

Definition at line 190 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

11.108 rpki.https.http_response Class Reference

Inherits rpki::https::http_message.

Collaboration diagram for rpki.https.http_response:

Public Member Functions

- def __init__
- def format_first_line
- def parse_first_line

Public Attributes

- code
- reason

11.108.1 Detailed Description

```
HTTP response message.
```

Definition at line 208 of file https.py.

11.108.2 Member Function Documentation

11.108.2.1 def rpki.https.http_response.__init__ (*self*, *code* = `None`, *reason* = `None`, *version* = default_http_version, *body* = `None`, *headers*)

Definition at line 213 of file https.py.

11.108.2.2 def rpki.https.http_response.format_first_line (*self*)

```
Format first line of HTTP response message, and set up Date and
Server headers.
```

Definition at line 226 of file https.py.

11.108.2.3 def rpki.https.http_response.parse_first_line (*self*, *version*, *code*, *reason*)

```
Parse first line of HTTP response message.
```

Definition at line 218 of file https.py.

11.108.3 Member Data Documentation

11.108.3.1 rpki.https.http_response.code

Definition at line 215 of file https.py.

11.108.3.2 rpki.https.http_response.reason

Definition at line 216 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

11.109 rpki.https.http_server Class Reference

Inherits rpki::https::http_stream.

Collaboration diagram for rpki.https.http_server:

Public Member Functions

- def __init__
- def find_handler
- def handle_message
- def handle_no_content_length
- def send_error

- def send_message
- def send_reply
- def tls_accept

Public Attributes

- expect_close
- handlers
- retry_read
- retry_write
- tls

Static Public Attributes

- parse_type = http_request

  Stream parser should look for incoming HTTP request messages.

- timeout = default_server_timeout

  Use the default server timeout value set in the module header.

11.109.1 Detailed Description

```
HTTP(S) server stream.
```

Definition at line 561 of file https.py.

11.109.2 Member Function Documentation

11.109.2.1 def rpki.https.http_server.__init__ (*self*, *sock*, *handlers*, *cert* = `None`, *key* = `None`, *ta* = `()`, *dynamic_ta* = `None`)

Definition at line 574 of file https.py.

11.109.2.2 def rpki.https.http_server.find_handler (*self*, *path*)

```
Helper method to search self.handlers.
```

Definition at line 635 of file https.py.

11.109.2.3 def rpki.https.http_server.handle_message (*self*)

```
TLS and HTTP layers managed to deliver a complete HTTP request to
us, figure out what to do with it.  Check the command and
Content-Type, look for a handler, and if everything looks right,
pass the message body, path, and a reply callback to the handler.
```

Definition at line 644 of file https.py.

11.109.2.4 def rpki.https.http_server.handle_no_content_length (*self*)

```
Handle an incoming message that used neither chunking nor a
Content-Length header (that is: this message will be the last one
in this server stream).  No special action required.
```

Definition at line 627 of file https.py.

11.109.2.5 def rpki.https.http_server.send_error (*self*, *code*, *reason*)

```
Send an error response to this request.
```

Definition at line 673 of file https.py.

11.109.2.6 def rpki.https.http_server.send_message (*self*, *code*, *reason* = "OK", *body* = None)

```
Queue up reply message.  If both parties agree that connection is
persistant, and if no error occurred, restart this stream to
listen for next message; otherwise, queue up a close event for
this stream so it will shut down once the reply has been sent.
```

Definition at line 685 of file https.py.

11.109.2.7 def rpki.https.http_server.send_reply (*self*, *code*, *body*)

```
Send a reply to this request.
```

Definition at line 679 of file https.py.

11.109.2.8 def rpki.https.http_server.tls_accept (*self*)

```
Set up TLS for server side connection, handling all the whacky
OpenSSL exceptions from TLS.

SSLErrorSSLError exceptions are particularly nasty, because all
too often they indicate a certificate lookup failure deep within
the guts of OpenSSL's TLS connection setup logic.  Extracting
anything resembling a Python data structure from a handler called
that deep inside the OpenSSL TLS library, while theoretically
possible, runs a high risk of triggering some kind of memory leak
or corruption.  So, for now, we just get back a long text string,
which we break up and log but don't attempt to process further.
```

Definition at line 596 of file https.py.

11.109.3 Member Data Documentation

11.109.3.1 rpki.https.http_server.expect_close

Definition at line 578 of file https.py.

11.109.3.2 rpki.https.http_server.handlers

Definition at line 576 of file https.py.

11.109.3.3 rpki::https.http_server::parse_type = http_request [static]

Stream parser should look for incoming HTTP request messages.

Definition at line 568 of file https.py.

11.109.3.4 rpki.https.http_server.retry_read

Reimplemented from rpki.https.http_stream.

Definition at line 613 of file https.py.

11.109.3.5 rpki.https.http_server.retry_write

Reimplemented from rpki.https.http_stream.

Definition at line 615 of file https.py.

11.109.3.6 rpki::https.http_server::timeout = default_server_timeout [static]

Use the default server timeout value set in the module header.

Definition at line 572 of file https.py.

11.109.3.7 rpki.https.http_server.tls

Reimplemented from rpki.https.http_stream.

Definition at line 582 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

11.110 rpki.https.http_stream Class Reference

Inherits asynchat::async_chat.

Inherited by rpki.https.http_client, and rpki.https.http_server.

Collaboration diagram for rpki.https.http_stream:

Public Member Functions

- def __init__
- def chunk_body
- def chunk_discard_crlf
- def chunk_discard_trailer
- def chunk_header

- def close
- def collect_incoming_data
- def found_terminator
- def get_buffer
- def handle_body
- def handle_close
- def handle_error
- def handle_read
- def handle_timeout
- def handle_write
- def initiate_send
- def log_cert
- def readable
- def recv
- def restart
- def send
- def update_timeout
- def writeable

Public Attributes

- buffer
- chunk_handler
- msg
- timer

Static Public Attributes

- log = log_method
- retry_read = None
- retry_write = None
- tls = None

11.110.1 Detailed Description

```
Virtual class representing an HTTP message stream.
```

Definition at line 243 of file https.py.

11.110.2 Member Function Documentation

11.110.2.1 def rpki.https.http_stream.__init__ (*self*, *sock* = None)

Definition at line 253 of file https.py.

11.110.2.2 def rpki.https.http_stream.chunk_body (*self*)

```
Asynchat just handed us what should be the body of a chunk of the
body of a chunked message (sic).  Save it, and prepare to move on
to the next chunk.
```

Definition at line 343 of file https.py.

11.110.2.3 def rpki.https.http_stream.chunk_discard_crlf (*self*)

```
Consume the CRLF that terminates a chunk, reinitialize chunk
decoder to be ready for the next chunk.
```

Definition at line 355 of file https.py.

11.110.2.4 def rpki.https.http_stream.chunk_discard_trailer (*self*)

```
Consume chunk trailer, which should be empty, then (finally!) exit
the chunk decoder and hand complete message off to the application.
```

Definition at line 365 of file https.py.

11.110.2.5 def rpki.https.http_stream.chunk_header (*self*)

```
Asynchat just handed us what should be the header of one chunk of
a chunked encoding stream.  If this chunk has a body, set the
stream up to read it; otherwise, this is the last chunk, so start
the process of exiting the chunk decoder.
```

Definition at line 327 of file https.py.

11.110.2.6 def rpki.https.http_stream.close (*self*, *force* = `False`)

```
Close the stream.

Graceful shutdown of a TLS connection requires multiple calls to
the underlying TLS code.  If the connection should be closed right
now without waiting (perhaps because it's already dead and we're
just cleaning up), call with force = True.
```

Definition at line 521 of file https.py.

11.110.2.7 def rpki.https.http_stream.collect_incoming_data (*self*, *data*)

```
Buffer incoming data from asynchat.
```

Definition at line 279 of file https.py.

11.110.2.8 def rpki.https.http_stream.found_terminator (*self*)

```
Asynchat reported that it found whatever terminator we set, so
figure out what to do next.  This can be messy, because we can be
in any of several different states:

@li We might be handling chunked HTTP, in which case we have to
initialize the chunk decoder;

@li We might have found the end of the message body, in which case
we can (finally) process it; or

@li We might have just gotten to the end of the message headers,
in which case we have to parse them to figure out which of three
separate mechanisms (chunked, content-length, TCP close) is going
to tell us how to find the end of the message body.
```

Definition at line 294 of file https.py.

11.110.2.9 def rpki.https.http_stream.get_buffer (*self*)

```
Consume data buffered from asynchat.
```

Definition at line 286 of file https.py.

11.110.2.10 def rpki.https.http_stream.handle_body (*self*)

```
Hand normal (not chunked) message off to the application.
```

Definition at line 376 of file https.py.

11.110.2.11 def rpki.https.http_stream.handle_close (*self*)

```
Wrapper around asynchat connection close handler, so that we can
log the event.
```

Reimplemented in rpki.https.http_client.

Definition at line 406 of file https.py.

11.110.2.12 def rpki.https.http_stream.handle_error (*self*)

```
Asynchat (or asyncore, or somebody) raised an exception.  See
whether it's one we should just pass along, otherwise log a stack
trace and close the stream.
```

Reimplemented in rpki.https.http_client.

Definition at line 383 of file https.py.

11.110.2.13 def rpki.https.http_stream.handle_read (*self*)

```
Asyncore says socket is readable.  Make sure there's no TLS write
already in progress, retry previous read operation if we had one
that was waiting for more input, otherwise try to read some data,
and handle all the weird OpenSSL exceptions that the TLS code
throws.
```

Definition at line 450 of file https.py.

11.110.2.14 def rpki.https.http_stream.handle_timeout (*self*)

```
Inactivity timer expired, close connection with prejudice.
```

Reimplemented in rpki.https.http_client.

Definition at line 399 of file https.py.

11.110.2.15 def rpki.https.http_stream.handle_write (*self*)

```
Asyncore says socket is writeable.  Make sure there's no TLS read
already in progress, retry previous write operation if we had one
that was blocked on the socket, otherwise try to write some data.
Handling all the weird OpenSSL exceptions that TLS throws is our
caller's problem.
```

Definition at line 478 of file https.py.

11.110.2.16 def rpki.https.http_stream.initiate_send (*self*)

```
Initiate a write operation.  This is just a wrapper around the
asynchat method, to handle all the whacky TLS exceptions.
```

Definition at line 502 of file https.py.

11.110.2.17 def rpki.https.http_stream.log_cert (*self*, *tag*, *x*)

```
Log HTTPS certificates, if certificate debugging is enabled.
```

Definition at line 554 of file https.py.

11.110.2.18 def rpki.https.http_stream.readable (*self*)

```
TLS replacement for normal asynchat .readable() method.  A TLS
connection that's blocked waiting for TLS write is considered not
readable even if the underlying socket is.
```

Definition at line 434 of file https.py.

11.110.2.19 def rpki.https.http_stream.recv (*self*, *buffer_size*)

```
TLS replacement for normal asyncore .recv() method.  Throw an
exception if TLS hasn't been started or if TLS I/O was already in
progress, otherwise hand off to the TLS code.
```

Definition at line 424 of file https.py.

11.110.2.20 def rpki.https.http_stream.restart (*self*)

```
(Re)start HTTP message parser, reset timer.
```

Definition at line 259 of file https.py.

11.110.2.21 def rpki.https.http_stream.send (*self*, *data*)

```
TLS replacement for normal asyncore .send() method.  Throw an
exception if TLS hasn't been started or if TLS I/O was already in
progress, otherwise hand off to the TLS code.
```

Definition at line 414 of file https.py.

11.110.2.22 def rpki.https.http_stream.update_timeout (*self*)

```
Put this stream's timer in known good state: set it to the
stream's timeout value if we're doing timeouts, otherwise clear
it.
```

Definition at line 268 of file https.py.

11.110.2.23 def rpki.https.http_stream.writeable (*self*)

```
TLS replacement for normal asynchat .writeable() method.  A TLS
connection that's blocked waiting for TLS read is considered not
writeable even if the underlying socket is.
```

Definition at line 442 of file https.py.

11.110.3 Member Data Documentation

11.110.3.1 rpki.https.http_stream.buffer

Definition at line 255 of file https.py.

11.110.3.2 rpki.https.http_stream.chunk_handler

Definition at line 264 of file https.py.

11.110.3.3 rpki.https.http_stream.log = log_method [static]

Definition at line 248 of file https.py.

11.110.3.4 rpki.https.http_stream.msg

Definition at line 317 of file https.py.

11.110.3.5 rpki.https.http_stream.retry_read = None [static]

Reimplemented in rpki.https.http_server, and rpki.https.http_client.

Definition at line 250 of file https.py.

11.110.3.6 rpki.https.http_stream.retry_write = None [static]

Reimplemented in rpki.https.http_server, and rpki.https.http_client.

Definition at line 251 of file https.py.

11.110.3.7 rpki.https.http_stream.timer

Definition at line 256 of file https.py.

11.110.3.8 rpki.https.http_stream.tls = None [static]

Reimplemented in rpki.https.http_server, and rpki.https.http_client.

Definition at line 249 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

11.111 rpki.ipaddrs.v4addr Class Reference

Inherits long.

Collaboration diagram for rpki.ipaddrs.v4addr:

Public Member Functions

- def __new__
- def __str__
- def from_bytes
- def to_bytes

Static Public Attributes

- int bits = 32

11.111.1 Detailed Description

```
IPv4 address.

Derived from long, but supports IPv4 print syntax.
```

Definition at line 47 of file ipaddrs.py.

11.111.2 Member Function Documentation

11.111.2.1 def rpki.ipaddrs.v4addr.__new__ (*cls*, *x*)

```
Construct a v4addr object.
```

Definition at line 56 of file ipaddrs.py.

11.111.2.2 def rpki.ipaddrs.v4addr.__str__ (*self*)

```
Convert a v4addr object to string format.
```

Definition at line 74 of file ipaddrs.py.

11.111.2.3 def rpki.ipaddrs.v4addr.from_bytes (*cls*, *x*)

```
Convert from a raw byte string to a v4addr object.
```

Definition at line 70 of file ipaddrs.py.

11.111.2.4 def rpki.ipaddrs.v4addr.to_bytes (*self*)

```
Convert a v4addr object to a raw byte string.
```

Definition at line 65 of file ipaddrs.py.

11.111.3 Member Data Documentation

11.111.3.1 int rpki.ipaddrs.v4addr.bits = 32 [static]

Definition at line 54 of file ipaddrs.py.

The documentation for this class was generated from the following file:

- ipaddrs.py (2424)

11.112 rpki.ipaddrs.v6addr Class Reference

Inherits long.

Collaboration diagram for rpki.ipaddrs.v6addr:

Public Member Functions

- def __new__
- def __str__
- def from_bytes
- def to_bytes

Static Public Attributes

- int bits = 128

11.112.1 Detailed Description

```
IPv6 address.

Derived from long, but supports IPv6 print syntax.
```

Definition at line 78 of file ipaddrs.py.

11.112.2 Member Function Documentation

11.112.2.1 def rpki.ipaddrs.v6addr.__new__ (*cls*, *x*)

```
Construct a v6addr object.
```

Definition at line 87 of file ipaddrs.py.

11.112.2.2 def rpki.ipaddrs.v6addr.__str__ (*self*)

```
Convert a v6addr object to string format.
```

Definition at line 104 of file ipaddrs.py.

11.112.2.3 def rpki.ipaddrs.v6addr.from_bytes (*cls*, *x*)

```
Convert from a raw byte string to a v6addr object.
```

Definition at line 99 of file ipaddrs.py.

11.112.2.4 def rpki.ipaddrs.v6addr.to_bytes (*self*)

```
Convert a v6addr object to a raw byte string.
```

Definition at line 94 of file ipaddrs.py.

11.112.3 Member Data Documentation

11.112.3.1 int rpki.ipaddrs.v6addr.bits = 128 [static]

Definition at line 85 of file ipaddrs.py.

The documentation for this class was generated from the following file:

- ipaddrs.py (2424)

11.113 rpki.left_right.bsc_elt Class Reference

Inherits rpki::left_right::data_elt.

Inherited by irbe_cli.bsc_elt.

Collaboration diagram for rpki.left_right.bsc_elt:

Public Member Functions

- def children
- def parents
- def repositories
- def serve_pre_save_hook

Static Public Attributes

- tuple attributes = ("action", "tag", "self_handle", "bsc_handle", "key_type", "hash_alg", "key_length")

  XML attributes for this element.

- tuple booleans = ("generate_keypair",)

  Boolean attributes (value "yes" or "no") for this element.

- string element_name = "bsc"
- tuple elements = ("signing_cert", "signing_cert_crl", "pkcs10_request")

  XML elements contained by this element.

- tuple handles = (("self", self_elt),)
- pkcs10_request = None
- private_key_id = None
- signing_cert = None
- signing_cert_crl = None
- tuple sql_template

11.113.1 Detailed Description

```
<bsc/> (Business Signing Context) element.
```

Definition at line 526 of file left_right.py.

11.113.2 Member Function Documentation

11.113.2.1 def rpki.left_right.bsc_elt.children (*self*)

```
Fetch all child objects that link to this BSC object.
```

Definition at line 557 of file left_right.py.

11.113.2.2 def rpki.left_right.bsc_elt.parents (*self*)

```
Fetch all parent objects that link to this BSC object.
```

Definition at line 553 of file left_right.py.

11.113.2.3 def rpki.left_right.bsc_elt.repositories (*self*)

```
Fetch all repository objects that link to this BSC object.
```

Definition at line 549 of file left_right.py.

11.113.2.4 def rpki.left_right.bsc_elt.serve_pre_save_hook (*self*, *q_pdu*, *r_pdu*, *cb*, *eb*)

```
Extra server actions for bsc_elt -- handle key generation.  For
now this only allows RSA with SHA-256.
```

Reimplemented from rpki.left_right.data_elt.

Definition at line 561 of file left_right.py.

11.113.3 Member Data Documentation

11.113.3.1 tuple rpki.left_right.bsc_elt.attributes = ("action", "tag", "self_handle", "bsc_handle", "key_type", "hash_alg", "key_length") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 532 of file left_right.py.

11.113.3.2 tuple rpki.left_right.bsc_elt.booleans = ("generate_keypair",) [static]

Boolean attributes (value "yes" or "no") for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 534 of file left_right.py.

11.113.3.3 string rpki.left_right.bsc_elt.element_name = "bsc" [static]

Definition at line 531 of file left_right.py.

11.113.3.4 tuple rpki.left_right.bsc_elt.elements = ("signing_cert", "signing_cert_crl", "pkcs10_request") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 533 of file left_right.py.

11.113.3.5 tuple rpki.left_right.bsc_elt.handles = (("self", self_elt),) [static]

Reimplemented from rpki.left_right.data_elt.

Definition at line 542 of file left_right.py.

11.113.3.6 rpki.left_right.bsc_elt.pkcs10_request = None [static]

Definition at line 545 of file left_right.py.

11.113.3.7 rpki.left_right.bsc_elt.private_key_id = None [static]

Definition at line 544 of file left_right.py.

11.113.3.8 rpki.left_right.bsc_elt.signing_cert = None [static]

Reimplemented in irbe_cli.bsc_elt.

Definition at line 546 of file left_right.py.

11.113.3.9 rpki.left_right.bsc_elt.signing_cert_crl = None [static]

Reimplemented in irbe_cli.bsc_elt.

Definition at line 547 of file left_right.py.

11.113.3.10 tuple rpki.left_right.bsc_elt.sql_template [static]

Initial value:

```
rpki.sql.template("bsc", "bsc_id", "bsc_handle",
                                   "self_id", "hash_alg",
                                   ("private_key_id", rpki.x509.RSA),
                                   ("pkcs10_request", rpki.x509.PKCS10),
                                   ("signing_cert", rpki.x509.X509),
                                   ("signing_cert_crl", rpki.x509.CRL))
```

Definition at line 536 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

11.114 rpki.left_right.child_elt Class Reference

Inherits rpki::left_right::data_elt.

Inherited by irbe_cli.child_elt.

Collaboration diagram for rpki.left_right.child_elt:

Public Member Functions

- def ca_from_class_name
- def child_certs
- def endElement
- def parents
- def serve_destroy_hook
- def serve_post_save_hook
- def serve_up_down

Static Public Attributes

- tuple attributes = ("action", "tag", "self_handle", "child_handle", "bsc_-handle")

  XML attributes for this element.

- tuple booleans = ("reissue",)

  Boolean attributes (value "yes" or "no") for this element.

- bpki_cert = None
- bpki_glue = None
- clear_https_ta_cache = False
- string element_name = "child"
- tuple elements = ("bpki_cert", "bpki_glue")

  XML elements contained by this element.

- tuple handles = (("self", self_elt), ("bsc", bsc_elt))
- tuple sql_template

11.114.1 Detailed Description

```
<child/> element.
```

Definition at line 805 of file left_right.py.

11.114.2 Member Function Documentation

11.114.2.1 def rpki.left_right.child_elt.ca_from_class_name (*self*, *class_name*)

```
Fetch the CA corresponding to an up-down class_name.
```

Definition at line 834 of file left_right.py.

11.114.2.2 def rpki.left_right.child_elt.child_certs (*self*, *ca_detail* = `None`, *ski* = `None`, *unique* = `False`)

```
Fetch all child_cert objects that link to this child object.
```

Definition at line 826 of file left_right.py.

11.114.2.3 def rpki.left_right.child_elt.endElement (*self*, *stack*, *name*, *text*)

```
Handle subelements of <child/> element.  These require special
handling because modifying them invalidates the HTTPS trust anchor
cache.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 866 of file left_right.py.

11.114.2.4 def rpki.left_right.child_elt.parents (*self*)

```
Fetch all parent objects that link to self object to which this child object links.
```

Definition at line 830 of file left_right.py.

11.114.2.5 def rpki.left_right.child_elt.serve_destroy_hook (*self*, *cb*, *eb*)

```
Extra server actions when destroying a child_elt.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 858 of file left_right.py.

11.114.2.6 def rpki.left_right.child_elt.serve_post_save_hook (*self*, *q_pdu*, *r_pdu*, *cb*, *eb*)

```
Extra server actions for child_elt.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 848 of file left_right.py.

11.114.2.7 def rpki.left_right.child_elt.serve_up_down (*self*, *query*, *callback*)

```
Outer layer of server handling for one up-down PDU from this child.
```

Definition at line 876 of file left_right.py.

11.114.3 Member Data Documentation

11.114.3.1 tuple rpki.left_right.child_elt.attributes = ("action", "tag", "self_handle", "child_handle", "bsc_handle") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 811 of file left_right.py.

11.114.3.2 tuple rpki.left_right.child_elt.booleans = ("reissue",) [static]

Boolean attributes (value "yes" or "no") for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 813 of file left_right.py.

11.114.3.3 rpki.left_right.child_elt.bpki_cert = None [static]

Definition at line 822 of file left_right.py.

11.114.3.4 rpki.left_right.child_elt.bpki_glue = None [static]

Definition at line 823 of file left_right.py.

11.114.3.5 rpki.left_right.child_elt.clear_https_ta_cache = False [static]

Definition at line 824 of file left_right.py.

11.114.3.6 string rpki.left_right.child_elt.element_name = "child" [static]

Definition at line 810 of file left_right.py.

11.114.3.7 tuple rpki.left_right.child_elt.elements = ("bpki_cert", "bpki_glue") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 812 of file left_right.py.

11.114.3.8 tuple rpki.left_right.child_elt.handles = (("self", self_elt), ("bsc", bsc_elt)) [static]

Reimplemented from rpki.left_right.data_elt.

Definition at line 820 of file left_right.py.

11.114.3.9 tuple rpki.left_right.child_elt.sql_template [static]

Initial value:

```
rpki.sql.template("child", "child_id", "child_handle",
                                  "self_id", "bsc_id",
                                  ("bpki_cert", rpki.x509.X509),
                                  ("bpki_glue", rpki.x509.X509))
```

Definition at line 815 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

11.115 rpki.left_right.cms_msg Class Reference

Inherits rpki::x509::XML_CMS_object.

Inherited by irbe_cli.left_right_cms_msg.

Collaboration diagram for rpki.left_right.cms_msg:

Static Public Attributes

- string encoding = "us-ascii"
- saxify = sax_handler.saxify
- schema = rpki.relaxng.left_right

11.115.1 Detailed Description

```
Class to hold a CMS-signed left-right PDU.
```

Definition at line 1120 of file left_right.py.

11.115.2 Member Data Documentation

11.115.2.1 string rpki.left_right.cms_msg.encoding = "us-ascii" [static]

Definition at line 1125 of file left_right.py.

11.115.2.2 rpki.left_right.cms_msg.saxify = sax_handler.saxify [static]

Reimplemented in irbe_cli.left_right_cms_msg.

Definition at line 1127 of file left_right.py.

11.115.2.3 rpki.left_right.cms_msg.schema = rpki.relaxng.left_right [static]

Definition at line 1126 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

11.116 rpki.left_right.data_elt Class Reference

Inherits rpki::xml_utils::data_elt, rpki::sql::sql_persistent, and rpki::left_right::left_-right_namespace.

Inherited by rpki.left_right.bsc_elt, rpki.left_right.child_elt, rpki.left_right.parent_elt, rpki.left_right.repository_elt, and rpki.left_right.self_elt.

Collaboration diagram for rpki.left_right.data_elt:

Public Member Functions

- def bsc
- def make_reply_clone_hook
- def self
- def serve_fetch_all
- def serve_fetch_handle
- def serve_fetch_one_maybe
- def serve_pre_save_hook

Static Public Attributes

- tuple handles = ()
- self_handle = None
- self_id = None

11.116.1 Detailed Description

```
Virtual class for top-level left-right protocol data elements.
```

Definition at line 50 of file left_right.py.

11.116.2 Member Function Documentation

11.116.2.1 def rpki.left_right.data_elt.bsc (*self*)

```
Return BSC object to which this object links.
```

Definition at line 64 of file left_right.py.

11.116.2.2 def rpki.left_right.data_elt.make_reply_clone_hook (*self*, *r_pdu*)

```
Set handles when cloning, including _id -> _handle translation.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 68 of file left_right.py.

11.116.2.3 def rpki.left_right.data_elt.self (*self*)

```
Fetch self object to which this object links.
```

Definition at line 60 of file left_right.py.

11.116.2.4 def rpki.left_right.data_elt.serve_fetch_all (*self*)

```
Find the objects on which a list method should operate.
```

Reimplemented in rpki.left_right.self_elt.

Definition at line 99 of file left_right.py.

11.116.2.5 def rpki.left_right.data_elt.serve_fetch_handle (*cls*, *gctx*, *self_id*, *handle*)

```
Find an object based on its handle.
```

Reimplemented in rpki.left_right.self_elt.

Definition at line 84 of file left_right.py.

11.116.2.6 def rpki.left_right.data_elt.serve_fetch_one_maybe (*self*)

```
Find the object on which a get, set, or destroy method should
operate, or which would conflict with a create method.
```

Reimplemented in rpki.left_right.self_elt.

Definition at line 90 of file left_right.py.

11.116.2.7 def rpki.left_right.data_elt.serve_pre_save_hook (*self*, *q_pdu*, *r_pdu*, *cb*, *eb*)

```
Hook to do _handle => _id translation before saving.

self is always the object to be saved to SQL.  For create
operations, self and q_pdu are be the same object; for set
operations, self is the pre-existing object from SQL and q_pdu is
the set request received from the the IRBE.
```

Reimplemented from rpki.xml_utils.data_elt.

Reimplemented in rpki.left_right.bsc_elt.

Definition at line 106 of file left_right.py.

11.116.3 Member Data Documentation

11.116.3.1 tuple rpki.left_right.data_elt.handles = () [static]

Reimplemented in rpki.left_right.self_elt, rpki.left_right.bsc_elt, rpki.left_right.repository_elt, rpki.left_right.parent_elt, and rpki.left_right.child_elt.

Definition at line 55 of file left_right.py.

11.116.3.2 rpki.left_right.data_elt.self_handle = None [static]

Definition at line 58 of file left_right.py.

11.116.3.3 rpki.left_right.data_elt.self_id = None [static]

Definition at line 57 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

11.117 rpki.left_right.left_right_namespace Class Reference

Inherits object.

Inherited by rpki.left_right.data_elt, rpki.left_right.list_published_objects_elt, rpki.left_right.list_received_resources_elt, rpki.left_right.list_resources_elt, rpki.left_right.list_roa_requests_elt, rpki.left_right.msg, and rpki.left_right.report_error_elt.

Collaboration diagram for rpki.left_right.left_right_namespace:

Static Public Attributes

- dictionary nsmap = { None : xmlns }
- string xmlns = "http://www.hactrn.net/uris/rpki/left-right-spec/"

11.117.1 Detailed Description

```
XML namespace parameters for left-right protocol.
```

Definition at line 42 of file left_right.py.

11.117.2 Member Data Documentation

11.117.2.1 dictionary rpki.left_right.left_right_namespace.nsmap = { None : xmlns } [static]

Definition at line 48 of file left_right.py.

11.117.2.2 string rpki.left_right.left_right_namespace.xmlns = "http://www.hactrn.net/uris/rpki/left-right-spec/" [static]

Definition at line 47 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

11.118 rpki.left_right.list_published_objects_elt Class Reference

Inherits rpki::xml_utils::text_elt, and rpki::left_right::left_right_namespace.

Inherited by irbe_cli.list_published_objects_elt.

Collaboration diagram for rpki.left_right.list_published_objects_elt:

Public Member Functions

- def make_reply
- def serve_dispatch

Static Public Attributes

- tuple attributes = ("self_handle", "tag", "uri")

  XML attributes for this element.

- string element_name = "list_published_objects"
- obj = None
- string text_attribute = "obj"

  Name of the class attribute that holds the text value.

11.118.1 Detailed Description

```
<list_published_objects/> element.
```

Definition at line 968 of file left_right.py.

11.118.2 Member Function Documentation

11.118.2.1 def rpki.left_right.list_published_objects_elt.make_reply (*self*, *uri*, *obj*)

```
Generate one reply PDU.
```

Definition at line 995 of file left_right.py.

11.118.2.2 def rpki.left_right.list_published_objects_elt.serve_dispatch (*self*, *r_msg*, *cb*, *eb*)

```
Handle a <list_published_objects/> query.  The method name is a
misnomer here, there's no action attribute and no dispatch, we
just dump every published object for the specified <self/> and return.
```

Definition at line 979 of file left_right.py.

11.118.3 Member Data Documentation

11.118.3.1 tuple rpki.left_right.list_published_objects_elt.attributes = ("self_handle", "tag", "uri") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 974 of file left_right.py.

11.118.3.2 string rpki.left_right.list_published_objects_elt.element_name = "list_published_objects" [static]

Definition at line 973 of file left_right.py.

11.118.3.3 rpki.left_right.list_published_objects_elt.obj = None [static]

Definition at line 977 of file left_right.py.

11.118.3.4 string rpki.left_right.list_published_objects_elt.text_attribute = "obj" [static]

Name of the class attribute that holds the text value.

Reimplemented from rpki.xml_utils.text_elt.

Definition at line 975 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

11.119 rpki.left_right.list_received_resources_elt Class Reference

Inherits rpki::xml_utils::base_elt, and rpki::left_right::left_right_namespace.

Inherited by irbe_cli.list_received_resources_elt.

Collaboration diagram for rpki.left_right.list_received_resources_elt:

Public Member Functions

- def make_reply
- def serve_dispatch

Static Public Attributes

- tuple attributes

  XML attributes for this element.

- string element_name = "list_received_resources"

11.119.1 Detailed Description

```
<list_received_resources/> element.
```

Definition at line 1003 of file left_right.py.

11.119.2 Member Function Documentation

11.119.2.1 def rpki.left_right.list_received_resources_elt.make_reply (*self*, *uri*, *cert*)

```
Generate one reply PDU.
```

Definition at line 1026 of file left_right.py.

11.119.2.2 def rpki.left_right.list_received_resources_elt.serve_dispatch (*self*, *r_msg*, *cb*, *eb*)

```
Handle a <list_received_resources/> query.  The method name is a
misnomer here, there's no action attribute and no dispatch, we
just dump a bunch of data about every certificate issued to us by
one of our parents, then return.
```

Definition at line 1012 of file left_right.py.

11.119.3 Member Data Documentation

11.119.3.1 tuple rpki.left_right.list_received_resources_elt.attributes [static]

Initial value:

```
("self_handle", "tag",
                "notBefore", "notAfter", "uri", "sia_uri", "aia_uri", "asn", "ipv
      4", "ipv6")
```

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 1009 of file left_right.py.

11.119.3.2 string rpki.left_right.list_received_resources_elt.element_name = "list_received_resources" [static]

Definition at line 1008 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

11.120 rpki.left_right.list_resources_elt Class Reference

Inherits rpki::xml_utils::base_elt, and rpki::left_right::left_right_namespace.

Collaboration diagram for rpki.left_right.list_resources_elt:

Public Member Functions

- def startElement
- def toXML

Public Attributes

- asn

- ipv4
- ipv6

Static Public Attributes

- tuple attributes = ("self_handle", "tag", "child_handle", "valid_until", "asn", "ipv4", "ipv6")

  XML attributes for this element.

- string element_name = "list_resources"
- valid_until = None

11.120.1 Detailed Description

```
<list_resources/> element.
```

Definition at line 913 of file left_right.py.

11.120.2 Member Function Documentation

11.120.2.1 def rpki.left_right.list_resources_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle <list_resources/> element.  This requires special handling
due to the data types of some of the attributes.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 922 of file left_right.py.

11.120.2.2 def rpki.left_right.list_resources_elt.toXML (*self*)

```
Generate <list_resources/> element.  This requires special
handling due to the data types of some of the attributes.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 938 of file left_right.py.

11.120.3 Member Data Documentation

11.120.3.1 rpki.left_right.list_resources_elt.asn

Definition at line 932 of file left_right.py.

11.120.3.2 tuple rpki.left_right.list_resources_elt.attributes = ("self_handle", "tag", "child_handle", "valid_until", "asn", "ipv4", "ipv6") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 919 of file left_right.py.

11.120.3.3 string rpki.left_right.list_resources_elt.element_name = "list_resources" [static]

Definition at line 918 of file left_right.py.

11.120.3.4 rpki.left_right.list_resources_elt.ipv4

Definition at line 934 of file left_right.py.

11.120.3.5 rpki.left_right.list_resources_elt.ipv6

Definition at line 936 of file left_right.py.

11.120.3.6 rpki.left_right.list_resources_elt.valid_until = None [static]

Definition at line 920 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

11.121 rpki.left_right.list_roa_requests_elt Class Reference

Inherits rpki::xml_utils::base_elt, and rpki::left_right::left_right_namespace.

Collaboration diagram for rpki.left_right.list_roa_requests_elt:

Public Member Functions

- def startElement

Public Attributes

- ipv4
- ipv6

Static Public Attributes

- tuple attributes = ("self_handle", "tag", "asn", "ipv4", "ipv6")

  XML attributes for this element.

- string element_name = "list_roa_requests"

11.121.1 Detailed Description

```
<list_roa_requests/> element.
```

Definition at line 948 of file left_right.py.

11.121.2 Member Function Documentation

11.121.2.1 def rpki.left_right.list_roa_requests_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle <list_roa_requests/> element.  This requires special handling
due to the data types of some of the attributes.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 956 of file left_right.py.

11.121.3 Member Data Documentation

11.121.3.1 tuple rpki.left_right.list_roa_requests_elt.attributes = ("self_handle", "tag", "asn", "ipv4", "ipv6") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 954 of file left_right.py.

11.121.3.2 string rpki.left_right.list_roa_requests_elt.element_name = "list_roa_requests" [static]

Definition at line 953 of file left_right.py.

11.121.3.3 rpki.left_right.list_roa_requests_elt.ipv4

Definition at line 964 of file left_right.py.

11.121.3.4 rpki.left_right.list_roa_requests_elt.ipv6

Definition at line 966 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

11.122 rpki.left_right.msg Class Reference

Inherits rpki::xml_utils::msg, and rpki::left_right::left_right_namespace.

Inherited by irbe_cli.left_right_msg.

Collaboration diagram for rpki.left_right.msg:

Public Member Functions

- def serve_top_level

Static Public Attributes

- tuple pdus

Dispatch table of PDUs for this protocol.

- int version = 1

  Protocol version.

11.122.1 Detailed Description

```
Left-right PDU.
```

Definition at line 1066 of file left_right.py.

11.122.2 Member Function Documentation

11.122.2.1 def rpki.left_right.msg.serve_top_level (*self*, *gctx*, *cb*)

```
Serve one msg PDU.
```

Definition at line 1083 of file left_right.py.

11.122.3 Member Data Documentation

11.122.3.1 rpki::left_right.msg::pdus [static]

Initial value:

```
dict((x.element_name, x)
              for x in (self_elt, child_elt, parent_elt, bsc_elt, repository_elt,

                        list_resources_elt, list_roa_requests_elt,
                        list_published_objects_elt, list_received_resources_elt,
                        report_error_elt))
```

Dispatch table of PDUs for this protocol.

Reimplemented in irbe_cli.left_right_msg.

Definition at line 1077 of file left_right.py.

11.122.3.2 rpki::left_right.msg::version = 1 [static]

Protocol version.

Reimplemented from rpki.xml_utils.msg.

Definition at line 1073 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

11.123 rpki.left_right.parent_elt Class Reference

Inherits rpki::left_right::data_elt.

Inherited by irbe_cli.parent_elt.

Collaboration diagram for rpki.left_right.parent_elt:

Public Member Functions

- def cas
- def query_up_down
- def repository
- def serve_post_save_hook
- def serve_rekey
- def serve_revoke
- def serve_revoke_forgotten

Static Public Attributes

- tuple attributes

  XML attributes for this element.

- tuple booleans = ("rekey", "reissue", "revoke", "revoke_forgotten")

  Boolean attributes (value "yes" or "no") for this element.

- bpki_cms_cert = None
- bpki_cms_glue = None
- bpki_https_cert = None
- bpki_https_glue = None
- string element_name = "parent"
- tuple elements = ("bpki_cms_cert", "bpki_cms_glue", "bpki_https_cert", "bpki_https_glue")

  XML elements contained by this element.

- tuple handles = (("self", self_elt), ("bsc", bsc_elt), ("repository", repository_elt))
- tuple sql_template

11.123.1 Detailed Description

```
<parent/> element.
```

Definition at line 656 of file left_right.py.

11.123.2 Member Function Documentation

11.123.2.1 def rpki.left_right.parent_elt.cas (*self*)

```
Fetch all CA objects that link to this parent object.
```

Definition at line 683 of file left_right.py.

11.123.2.2 def rpki.left_right.parent_elt.query_up_down (*self*, *q_pdu*, *cb*, *eb*)

```
Client code for sending one up-down query PDU to this parent.
```

Definition at line 759 of file left_right.py.

11.123.2.3 def rpki.left_right.parent_elt.repository (*self*)

```
Fetch repository object to which this parent object links.
```

Definition at line 679 of file left_right.py.

11.123.2.4 def rpki.left_right.parent_elt.serve_post_save_hook (*self*, *q_pdu*, *r_pdu*, *cb*, *eb*)

```
Extra server actions for parent_elt.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 687 of file left_right.py.

11.123.2.5 def rpki.left_right.parent_elt.serve_rekey (*self*, *cb*, *eb*)

```
Handle a left-right rekey action for this parent.
```

Definition at line 703 of file left_right.py.

11.123.2.6 def rpki.left_right.parent_elt.serve_revoke (*self*, *cb*, *eb*)

```
Handle a left-right revoke action for this parent.
```

Definition at line 711 of file left_right.py.

11.123.2.7 def rpki.left_right.parent_elt.serve_revoke_forgotten (*self*, *cb*, *eb*)

```
Handle a left-right revoke_forgotten action for this parent.

This is a bit fiddly: we have to compare the result of an up-down
list query with what we have locally and identify the SKIs of any
certificates that have gone missing.  This should never happen in
ordinary operation, but can arise if we have somehow lost a
private key, in which case there is nothing more we can do with
the issued cert, so we have to clear it.  As this really is not
supposed to happen, we don't clear it automatically, instead we
require an explicit trigger.
```

Definition at line 719 of file left_right.py.

11.123.3 Member Data Documentation

11.123.3.1 tuple rpki.left_right.parent_elt.attributes [static]

Initial value:

```
("action", "tag", "self_handle", "parent_handle", "bsc_handle", "repository_handl
      e",
                "peer_contact_uri", "sia_base", "sender_name", "recipient_name")
```

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 662 of file left_right.py.

11.123.3.2 tuple rpki.left_right.parent_elt.booleans = ("rekey", "reissue", "revoke", "revoke_forgotten") [static]

Boolean attributes (value "yes" or "no") for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 665 of file left_right.py.

11.123.3.3 rpki.left_right.parent_elt.bpki_cms_cert = None [static]

Definition at line 674 of file left_right.py.

11.123.3.4 rpki.left_right.parent_elt.bpki_cms_glue = None [static]

Definition at line 675 of file left_right.py.

11.123.3.5 rpki.left_right.parent_elt.bpki_https_cert = None [static]

Definition at line 676 of file left_right.py.

11.123.3.6 rpki.left_right.parent_elt.bpki_https_glue = None [static]

Definition at line 677 of file left_right.py.

11.123.3.7 string rpki.left_right.parent_elt.element_name = "parent" [static]

Definition at line 661 of file left_right.py.

11.123.3.8 tuple rpki.left_right.parent_elt.elements = ("bpki_cms_cert", "bpki_cms_glue", "bpki_https_cert", "bpki_https_glue") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 664 of file left_right.py.

11.123.3.9 tuple rpki.left_right.parent_elt.handles = (("self", self_elt), ("bsc", bsc_elt), ("repository", repository_elt)) [static]

Reimplemented from rpki.left_right.data_elt.

Definition at line 672 of file left_right.py.

11.123.3.10 tuple rpki.left_right.parent_elt.sql_template [static]

Initial value:

```
rpki.sql.template("parent", "parent_id", "parent_handle",
                                  "self_id", "bsc_id", "repository_id",
                                  ("bpki_cms_cert", rpki.x509.X509), ("bpki_cms_
      glue", rpki.x509.X509),
                                  ("bpki_https_cert", rpki.x509.X509), ("bpki_ht
      tps_glue", rpki.x509.X509),
                                  "peer_contact_uri", "sia_base", "sender_name",
       "recipient_name")
```

Definition at line 667 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

11.124 rpki.left_right.report_error_elt Class Reference

Inherits rpki::xml_utils::text_elt, and rpki::left_right::left_right_namespace.

Inherited by irbe_cli.report_error_elt.

Collaboration diagram for rpki.left_right.report_error_elt:

Public Member Functions

- def from_exception

Public Attributes

- error_code
- self_handle
- tag

Static Public Attributes

- tuple attributes = ("tag", "self_handle", "error_code")

  XML attributes for this element.

- string element_name = "report_error"
- error_text = None
- string text_attribute = "error_text"

  Name of the class attribute that holds the text value.

11.124.1 Detailed Description

```
<report_error/> element.
```

Definition at line 1043 of file left_right.py.

11.124.2 Member Function Documentation

11.124.2.1 def rpki.left_right.report_error_elt.from_exception (*cls*, *e*, *self_handle* = `None`, *tag* = `None`)

```
Generate a <report_error/> element from an exception.
```

Definition at line 1055 of file left_right.py.

11.124.3 Member Data Documentation

11.124.3.1 tuple rpki.left_right.report_error_elt.attributes = ("tag", "self_handle", "error_code") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 1049 of file left_right.py.

11.124.3.2 string rpki.left_right.report_error_elt.element_name = "report_error" [static]

Definition at line 1048 of file left_right.py.

11.124.3.3 rpki.left_right.report_error_elt.error_code

Definition at line 1062 of file left_right.py.

11.124.3.4 rpki.left_right.report_error_elt.error_text = None [static]

Definition at line 1052 of file left_right.py.

11.124.3.5 rpki.left_right.report_error_elt.self_handle

Definition at line 1060 of file left_right.py.

11.124.3.6 rpki.left_right.report_error_elt.tag

Definition at line 1061 of file left_right.py.

11.124.3.7 string rpki.left_right.report_error_elt.text_attribute = "error_text" [static]

Name of the class attribute that holds the text value.

Reimplemented from rpki.xml_utils.text_elt.

Definition at line 1050 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

11.125 rpki.left_right.repository_elt Class Reference

Inherits rpki::left_right::data_elt.

Inherited by irbe_cli.repository_elt.

Collaboration diagram for rpki.left_right.repository_elt:

Public Member Functions

- def call_pubd
- def default_pubd_handler
- def parents

Static Public Attributes

- tuple attributes = ("action", "tag", "self_handle", "repository_handle", "bsc_-handle", "peer_contact_uri")

  XML attributes for this element.

- bpki_cert = None
- bpki_glue = None
- string element_name = "repository"
- tuple elements = ("bpki_cert", "bpki_glue")

  XML elements contained by this element.

- tuple handles = (("self", self_elt), ("bsc", bsc_elt))
- tuple sql_template

11.125.1 Detailed Description

```
<repository/> element.
```

Definition at line 573 of file left_right.py.

11.125.2 Member Function Documentation

11.125.2.1 def rpki.left_right.repository_elt.call_pubd (*self*, *callback*, *errback*, *q_msg*, *handlers* = `None`)

```
Send a message to publication daemon and return the response.

As a convenience, attempting to send an empty message returns
immediate success without sending anything.

Handlers is a dict of handler functions to process the response
PDUs.  If the tag value in the response PDU appears in the dict,
the associated handler is called to process the PDU.  If no tag
matches, default_pubd_handler() is called.  A handler value of
False suppresses calling of the default handler.
```

Definition at line 601 of file left_right.py.

11.125.2.2 def rpki.left_right.repository_elt.default_pubd_handler (*pdu*)

```
Default handler for publication response PDUs.
```

Definition at line 595 of file left_right.py.

11.125.2.3 def rpki.left_right.repository_elt.parents (*self*)

```
Fetch all parent objects that link to this repository object.
```

Definition at line 590 of file left_right.py.

11.125.3 Member Data Documentation

11.125.3.1 tuple rpki.left_right.repository_elt.attributes = ("action", "tag", "self_handle", "repository_handle", "bsc_handle", "peer_contact_uri") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 579 of file left_right.py.

11.125.3.2 rpki.left_right.repository_elt.bpki_cert = None [static]

Definition at line 587 of file left_right.py.

11.125.3.3 rpki.left_right.repository_elt.bpki_glue = None [static]

Definition at line 588 of file left_right.py.

11.125.3.4 string rpki.left_right.repository_elt.element_name = "repository" [static]

Definition at line 578 of file left_right.py.

11.125.3.5 tuple rpki.left_right.repository_elt.elements = ("bpki_cert", "bpki_glue") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 580 of file left_right.py.

11.125.3.6 tuple rpki.left_right.repository_elt.handles = (("self", self_elt), ("bsc", bsc_elt)) [static]

Reimplemented from rpki.left_right.data_elt.

Definition at line 585 of file left_right.py.

11.125.3.7 tuple rpki.left_right.repository_elt.sql_template [static]

Initial value:

```
rpki.sql.template("repository", "repository_id", "repository_handle",
                                  "self_id", "bsc_id", "peer_contact_uri",
                                  ("bpki_cert", rpki.x509.X509), ("bpki_glue", r
      pki.x509.X509))
```

Definition at line 582 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

11.126 rpki.left_right.sax_handler Class Reference

Inherits rpki::xml_utils::sax_handler.

Inherited by irbe_cli.left_right_sax_handler.

Collaboration diagram for rpki.left_right.sax_handler:

Static Public Attributes

- string name = "msg"
- pdu = msg
- string version = "1"

11.126.1 Detailed Description

```
SAX handler for Left-Right protocol.
```

Definition at line 1111 of file left_right.py.

11.126.2 Member Data Documentation

11.126.2.1 string rpki.left_right.sax_handler.name = "msg" [static]

Definition at line 1117 of file left_right.py.

11.126.2.2 rpki.left_right.sax_handler.pdu = msg [static]

Reimplemented in irbe_cli.left_right_sax_handler.

Definition at line 1116 of file left_right.py.

11.126.2.3 string rpki.left_right.sax_handler.version = "1" [static]

Definition at line 1118 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

11.127 rpki.left_right.self_elt Class Reference

Inherits rpki::left_right::data_elt.

Inherited by irbe_cli.self_elt.

Collaboration diagram for rpki.left_right.self_elt:

Public Member Functions

- def bscs
- def children
- def client_poll
- def cron
- def parents
- def regenerate_crls_and_manifests
- def repositories
- def roas
- def serve_fetch_all
- def serve_fetch_handle
- def serve_fetch_one_maybe
- def serve_post_save_hook
- def serve_publish_world_now
- def serve_rekey
- def serve_revoke
- def serve_revoke_forgotten
- def serve_run_now
- def update_children
- def update_roas

Static Public Attributes

- tuple attributes = ("action", "tag", "self_handle", "crl_interval", "regen_-margin")

  XML attributes for this element.

- tuple booleans = ("rekey", "reissue", "revoke", "run_now", "publish_world_-now", "revoke_forgotten")

  Boolean attributes (value "yes" or "no") for this element.

- bpki_cert = None
- bpki_glue = None
- crl_interval = None
- string element_name = "self"
- tuple elements = ("bpki_cert", "bpki_glue")

  XML elements contained by this element.

- tuple handles = ()
- regen_margin = None
- tuple sql_template
- use_hsm = False

11.127.1 Detailed Description

```
<self/> element.
```

Definition at line 124 of file left_right.py.

11.127.2 Member Function Documentation

11.127.2.1 def rpki.left_right.self_elt.bscs (*self*)

```
Fetch all BSC objects that link to this self object.
```

Definition at line 145 of file left_right.py.

11.127.2.2 def rpki.left_right.self_elt.children (*self*)

```
Fetch all child objects that link to this self object.
```

Definition at line 157 of file left_right.py.

11.127.2.3 def rpki.left_right.self_elt.client_poll (*self*, *callback*)

```
Run the regular client poll cycle with each of this self's parents
in turn.
```

Definition at line 302 of file left_right.py.

11.127.2.4 def rpki.left_right.self_elt.cron (*self*, *cb*)

```
Periodic tasks.
```

Definition at line 274 of file left_right.py.

11.127.2.5 def rpki.left_right.self_elt.parents (*self*)

```
Fetch all parent objects that link to this self object.
```

Definition at line 153 of file left_right.py.

11.127.2.6 def rpki.left_right.self_elt.regenerate_crls_and_manifests (*self*, *cb*)

```
Generate new CRLs and manifests as necessary for all of this
self's CAs.  Extracting nextUpdate from a manifest is hard at the
moment due to implementation silliness, so for now we generate a
new manifest whenever we generate a new CRL

This method also cleans up tombstones left behind by revoked
ca_detail objects, since we're walking through the relevant
portions of the database anyway.
```

Definition at line 428 of file left_right.py.

11.127.2.7 def rpki.left_right.self_elt.repositories (*self*)

```
Fetch all repository objects that link to this self object.
```

Definition at line 149 of file left_right.py.

11.127.2.8 def rpki.left_right.self_elt.roas (*self*)

```
Fetch all ROA objects that link to this self object.
```

Definition at line 161 of file left_right.py.

11.127.2.9 def rpki.left_right.self_elt.serve_fetch_all (*self*)

```
Find the self objects upon which a list action should operate.
This is different from the list action for all other objects,
where list only works within a given self_id context.
```

Reimplemented from rpki.left_right.data_elt.

Definition at line 266 of file left_right.py.

11.127.2.10 def rpki.left_right.self_elt.serve_fetch_handle (*cls*, *gctx*, *self_id*, *self_handle*)

```
Find a self object based on its self_handle.
```

Reimplemented from rpki.left_right.data_elt.

Definition at line 260 of file left_right.py.

11.127.2.11 def rpki.left_right.self_elt.serve_fetch_one_maybe (*self*)

```
Find the self object upon which a get, set, or destroy action
should operate, or which would conflict with a create method.
```

Reimplemented from rpki.left_right.data_elt.

Definition at line 252 of file left_right.py.

11.127.2.12 def rpki.left_right.self_elt.serve_post_save_hook (*self*, *q_pdu*, *r_pdu*, *cb*, *eb*)

```
Extra server actions for self_elt.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 165 of file left_right.py.

11.127.2.13 def rpki.left_right.self_elt.serve_publish_world_now (*self*, *cb*, *eb*)

```
Handle a left-right publish_world_now action for this self.

The publication stuff needs refactoring, right now publication is
interleaved with local operations in a way that forces far too
many bounces through the task system for any complex update.  The
whole thing ought to be rewritten to queue up outgoing publication
```

```
PDUs and only send them when we're all done or when we need to
force publication at a particular point in a multi-phase operation.

Once that reorganization has been done, this method should be
rewritten to reuse the low-level publish() methods that each
object will have...but we're not there yet.  So, for now, we just
do this via brute force.  Think of it as a trial version to see
whether we've identified everything that needs to be republished
for this operation.
```

Definition at line 213 of file left_right.py.

11.127.2.14 def rpki.left_right.self_elt.serve_rekey (*self*, *cb*, *eb*)

```
Handle a left-right rekey action for this self.
```

Definition at line 186 of file left_right.py.

11.127.2.15 def rpki.left_right.self_elt.serve_revoke (*self*, *cb*, *eb*)

```
Handle a left-right revoke action for this self.
```

Definition at line 195 of file left_right.py.

11.127.2.16 def rpki.left_right.self_elt.serve_revoke_forgotten (*self*, *cb*, *eb*)

```
Handle a left-right revoke_forgotten action for this self.
```

Definition at line 204 of file left_right.py.

11.127.2.17 def rpki.left_right.self_elt.serve_run_now (*self*, *cb*, *eb*)

```
Handle a left-right run_now action for this self.
```

Definition at line 245 of file left_right.py.

11.127.2.18 def rpki.left_right.self_elt.update_children (*self*, *cb*)

```
Check for updated IRDB data for all of this self's children and
issue new certs as necessary.  Must handle changes both in
resources and in expiration date.
```

Definition at line 361 of file left_right.py.

11.127.2.19 def rpki.left_right.self_elt.update_roas (*self*, *cb*)

```
Generate or update ROAs for this self.
```

Definition at line 470 of file left_right.py.

11.127.3 Member Data Documentation

11.127.3.1 tuple rpki.left_right.self_elt.attributes = ("action", "tag", "self_handle", "crl_interval", "regen_margin") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 130 of file left_right.py.

11.127.3.2 tuple rpki.left_right.self_elt.booleans = ("rekey", "reissue", "revoke", "run_now", "publish_world_now", "revoke_forgotten") [static]

Boolean attributes (value "yes" or "no") for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 132 of file left_right.py.

11.127.3.3 rpki.left_right.self_elt.bpki_cert = None [static]

Definition at line 142 of file left_right.py.

11.127.3.4 rpki.left_right.self_elt.bpki_glue = None [static]

Definition at line 143 of file left_right.py.

11.127.3.5 rpki.left_right.self_elt.crl_interval = None [static]

Definition at line 140 of file left_right.py.

11.127.3.6 string rpki.left_right.self_elt.element_name = "self" [static]

Definition at line 129 of file left_right.py.

11.127.3.7 tuple rpki.left_right.self_elt.elements = ("bpki_cert", "bpki_glue") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 131 of file left_right.py.

11.127.3.8 tuple rpki.left_right.self_elt.handles = () [static]

Reimplemented from rpki.left_right.data_elt.

Definition at line 137 of file left_right.py.

11.127.3.9 rpki.left_right.self_elt.regen_margin = None [static]

Definition at line 141 of file left_right.py.

11.127.3.10 tuple rpki.left_right.self_elt.sql_template [static]

Initial value:

```
rpki.sql.template("self", "self_id", "self_handle",
                                  "use_hsm", "crl_interval", "regen_margin",
                                  ("bpki_cert", rpki.x509.X509), ("bpki_glue", r
      pki.x509.X509))
```

Definition at line 134 of file left_right.py.

11.127.3.11 rpki.left_right.self_elt.use_hsm = False [static]

Definition at line 139 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

11.128 rpki.log.logger Class Reference

Inherits object.

Collaboration diagram for rpki.log.logger:

Public Member Functions

- def __call__
- def __init__

Public Attributes

- priority

11.128.1 Detailed Description

```
Closure for logging.
```

Definition at line 71 of file log.py.

11.128.2 Member Function Documentation

11.128.2.1 def rpki.log.logger.__call__ (*self*, *message*)

Definition at line 79 of file log.py.

11.128.2.2 def rpki.log.logger.__init__ (*self*, *priority*)

Definition at line 76 of file log.py.

11.128.3 Member Data Documentation

11.128.3.1 rpki.log.logger.priority

Definition at line 77 of file log.py.

The documentation for this class was generated from the following file:

- log.py (3107)

11.129 rpki.manifest.FileAndHash Class Reference

Inherits Sequence.

Collaboration diagram for rpki.manifest.FileAndHash:

Public Member Functions

- def __init__

Public Attributes

- file
- hash

11.129.1 Detailed Description

Definition at line 27 of file manifest.py.

11.129.2 Member Function Documentation

11.129.2.1 def rpki.manifest.FileAndHash.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 28 of file manifest.py.

11.129.3 Member Data Documentation

11.129.3.1 rpki.manifest.FileAndHash.file

Definition at line 29 of file manifest.py.

11.129.3.2 rpki.manifest.FileAndHash.hash

Definition at line 30 of file manifest.py.

The documentation for this class was generated from the following file:

- manifest.py (2424)

11.130 rpki.manifest.FilesAndHashes Class Reference

Inherits SequenceOf.

Collaboration diagram for rpki.manifest.FilesAndHashes:

Public Member Functions

- def __init__

11.130.1 Detailed Description

Definition at line 34 of file manifest.py.

11.130.2 Member Function Documentation

11.130.2.1 def rpki.manifest.FilesAndHashes.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 35 of file manifest.py.

The documentation for this class was generated from the following file:

- manifest.py (2424)

11.131 rpki.manifest.Manifest Class Reference

Inherits Sequence.

Collaboration diagram for rpki.manifest.Manifest:

Public Member Functions

- def __init__

Public Attributes

- explicitVersion
- fileHashAlg
- fileList
- manifestNumber
- nextUpdate

- thisUpdate
- version

11.131.1 Detailed Description

Definition at line 38 of file manifest.py.

11.131.2 Member Function Documentation

11.131.2.1 def rpki.manifest.Manifest.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 39 of file manifest.py.

11.131.3 Member Data Documentation

11.131.3.1 rpki.manifest.Manifest.explicitVersion

Definition at line 41 of file manifest.py.

11.131.3.2 rpki.manifest.Manifest.fileHashAlg

Definition at line 45 of file manifest.py.

11.131.3.3 rpki.manifest.Manifest.fileList

Definition at line 46 of file manifest.py.

11.131.3.4 rpki.manifest.Manifest.manifestNumber

Definition at line 42 of file manifest.py.

11.131.3.5 rpki.manifest.Manifest.nextUpdate

Definition at line 44 of file manifest.py.

11.131.3.6 rpki.manifest.Manifest.thisUpdate

Definition at line 43 of file manifest.py.

11.131.3.7 rpki.manifest.Manifest.version

Definition at line 40 of file manifest.py.

The documentation for this class was generated from the following file:

- manifest.py (2424)

11.132 rpki.publication.certificate_elt Class Reference

Inherits rpki::publication::publication_object_elt.

Inherited by irbe_cli.certificate_elt.

Collaboration diagram for rpki.publication.certificate_elt:

Static Public Attributes

- string element_name = "certificate"
- payload_type = rpki.x509.X509

11.132.1 Detailed Description

`<certificate/> element.`

Definition at line 287 of file publication.py.

11.132.2 Member Data Documentation

11.132.2.1 string rpki.publication.certificate_elt.element_name = "certificate" [static]

Definition at line 292 of file publication.py.

11.132.2.2 rpki.publication.certificate_elt.payload_type = rpki.x509.X509 [static]

Reimplemented from rpki.publication.publication_object_elt.

Definition at line 293 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

11.133 rpki.publication.client_elt Class Reference

Inherits rpki::publication::control_elt.

Inherited by irbe_cli.client_elt.

Collaboration diagram for rpki.publication.client_elt:

Public Member Functions

- def check_allowed_uri
- def endElement
- def serve_fetch_all
- def serve_fetch_one_maybe
- def serve_post_save_hook

Static Public Attributes

- tuple attributes = ("action", "tag", "client_handle", "base_uri")

  XML attributes for this element.

- base_uri = None
- bpki_cert = None
- bpki_glue = None
- clear_https_ta_cache = False
- string element_name = "client"
- tuple elements = ("bpki_cert", "bpki_glue")

  XML elements contained by this element.

- tuple sql_template = rpki.sql.template("client", "client_id", "client_handle", "base_uri", ("bpki_cert", rpki.x509.X509), ("bpki_glue", rpki.x509.X509))

11.133.1 Detailed Description

```
<client/> element.
```

Definition at line 113 of file publication.py.

11.133.2 Member Function Documentation

11.133.2.1 def rpki.publication.client_elt.check_allowed_uri (*self*, *uri*)

Definition at line 160 of file publication.py.

11.133.2.2 def rpki.publication.client_elt.endElement (*self*, *stack*, *name*, *text*)

```
Handle subelements of <client/> element.  These require special
handling because modifying them invalidates the HTTPS trust anchor
cache.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 130 of file publication.py.

11.133.2.3 def rpki.publication.client_elt.serve_fetch_all (*self*)

```
Find client objects on which a list method should operate.
```

Definition at line 156 of file publication.py.

11.133.2.4 def rpki.publication.client_elt.serve_fetch_one_maybe (*self*)

```
Find the client object on which a get, set, or destroy method
should operate, or which would conflict with a create method.
```

Definition at line 149 of file publication.py.

11.133.2.5 def rpki.publication.client_elt.serve_post_save_hook (*self*, *q_pdu*, *r_pdu*, *cb*, *eb*)

```
Extra server actions for client_elt.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 140 of file publication.py.

11.133.3 Member Data Documentation

11.133.3.1 tuple rpki.publication.client_elt.attributes = ("action", "tag", "client_handle", "base_uri") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 119 of file publication.py.

11.133.3.2 rpki.publication.client_elt.base_uri = None [static]

Definition at line 124 of file publication.py.

11.133.3.3 rpki.publication.client_elt.bpki_cert = None [static]

Definition at line 125 of file publication.py.

11.133.3.4 rpki.publication.client_elt.bpki_glue = None [static]

Definition at line 126 of file publication.py.

11.133.3.5 rpki.publication.client_elt.clear_https_ta_cache = False [static]

Definition at line 128 of file publication.py.

11.133.3.6 string rpki.publication.client_elt.element_name = "client" [static]

Definition at line 118 of file publication.py.

11.133.3.7 tuple rpki.publication.client_elt.elements = ("bpki_cert", "bpki_glue") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 120 of file publication.py.

11.133.3.8 tuple rpki.publication.client_elt.sql_template = rpki.sql.template("client", "client_id", "client_handle", "base_uri", ("bpki_cert", rpki.x509.X509), ("bpki_glue", rpki.x509.X509)) [static]

Definition at line 122 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

11.134 rpki.publication.cms_msg Class Reference

Inherits rpki::x509::XML_CMS_object.

Inherited by irbe_cli.publication_cms_msg.

Collaboration diagram for rpki.publication.cms_msg:

Static Public Attributes

- string encoding = "us-ascii"
- saxify = sax_handler.saxify
- schema = rpki.relaxng.publication

11.134.1 Detailed Description

```
Class to hold a CMS-signed publication PDU.
```

Definition at line 415 of file publication.py.

11.134.2 Member Data Documentation

11.134.2.1 string rpki.publication.cms_msg.encoding = "us-ascii" [static]

Definition at line 420 of file publication.py.

11.134.2.2 rpki.publication.cms_msg.saxify = sax_handler.saxify [static]

Reimplemented in irbe_cli.publication_cms_msg.

Definition at line 422 of file publication.py.

11.134.2.3 rpki.publication.cms_msg.schema = rpki.relaxng.publication [static]

Definition at line 421 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

11.135 rpki.publication.config_elt Class Reference

Inherits rpki::publication::control_elt.

Inherited by irbe_cli.config_elt.

Collaboration diagram for rpki.publication.config_elt:

Public Member Functions

- def fetch
- def serve_fetch_one_maybe
- def serve_set
- def startElement

Public Attributes

- config_id

Static Public Attributes

- tuple attributes = ("action", "tag")

  XML attributes for this element.

- string element_name = "config"
- tuple elements = ("bpki_crl",)

  XML elements contained by this element.

- tuple sql_template = rpki.sql.template("config", "config_id", ("bpki_crl", rpki.x509.CRL))
- int wired_in_config_id = 1

11.135.1 Detailed Description

```
<config/> element.  This is a little weird because there should
never be more than one row in the SQL config table, but we have to
put the BPKI CRL somewhere and SQL is the least bad place available.

So we reuse a lot of the SQL machinery, but we nail config_id at 1,
we don't expose it in the XML protocol, and we only support the get
and set actions.
```

Definition at line 61 of file publication.py.

11.135.2 Member Function Documentation

11.135.2.1 def rpki.publication.config_elt.fetch (*cls*, *gctx*)

```
Fetch the config object from SQL.  This requires special handling
because of the weird way we treat config_id.
```

Definition at line 89 of file publication.py.

11.135.2.2 def rpki.publication.config_elt.serve_fetch_one_maybe (*self*)

```
Find the config object on which a get or set method should
operate.
```

Definition at line 106 of file publication.py.

11.135.2.3 def rpki.publication.config_elt.serve_set (*self*, *r_msg*, *cb*, *eb*)

```
Handle a set action.  This requires special handling because
config doesn't support the create method.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 96 of file publication.py.

11.135.2.4 def rpki.publication.config_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
StartElement() handler for config object.  This requires special
handling because of the weird way we treat config_id.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 80 of file publication.py.

11.135.3 Member Data Documentation

11.135.3.1 tuple rpki.publication.config_elt.attributes = ("action", "tag") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 72 of file publication.py.

11.135.3.2 rpki.publication.config_elt.config_id

Definition at line 86 of file publication.py.

11.135.3.3 string rpki.publication.config_elt.element_name = "config" [static]

Definition at line 73 of file publication.py.

11.135.3.4 tuple rpki.publication.config_elt.elements = ("bpki_crl",) [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 74 of file publication.py.

11.135.3.5 tuple rpki.publication.config_elt.sql_template = rpki.sql.template("config", "config_id", ("bpki_crl", rpki.x509.CRL)) [static]

Definition at line 76 of file publication.py.

11.135.3.6 int rpki.publication.config_elt.wired_in_config_id = 1 [static]

Definition at line 78 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

11.136 rpki.publication.control_elt Class Reference

Inherits rpki::xml_utils::data_elt, rpki::sql::sql_persistent, and rpki::publication::publication_namespace.

Inherited by rpki.publication.client_elt, and rpki.publication.config_elt.

Collaboration diagram for rpki.publication.control_elt:

Public Member Functions

- def serve_dispatch

11.136.1 Detailed Description

```
Virtual class for control channel objects.
```

Definition at line 47 of file publication.py.

11.136.2 Member Function Documentation

11.136.2.1 def rpki.publication.control_elt.serve_dispatch (*self*, *r_msg*, *cb*, *eb*)

```
Action dispatch handler.  This needs special handling because we
need to make sure that this PDU arrived via the control channel.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 52 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

11.137 rpki.publication.crl_elt Class Reference

Inherits rpki::publication::publication_object_elt.

Inherited by irbe_cli.crl_elt.

Collaboration diagram for rpki.publication.crl_elt:

Static Public Attributes

- string element_name = "crl"
- payload_type = rpki.x509.CRL

11.137.1 Detailed Description

`<crl/> element.`

Definition at line 295 of file publication.py.

11.137.2 Member Data Documentation

11.137.2.1 string rpki.publication.crl_elt.element_name = "crl" [static]

Definition at line 300 of file publication.py.

11.137.2.2 rpki.publication.crl_elt.payload_type = rpki.x509.CRL [static]

Reimplemented from rpki.publication.publication_object_elt.

Definition at line 301 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

11.138 rpki.publication.manifest_elt Class Reference

Inherits rpki::publication::publication_object_elt.

Inherited by irbe_cli.manifest_elt.

Collaboration diagram for rpki.publication.manifest_elt:

Static Public Attributes

- string element_name = "manifest"
- payload_type = rpki.x509.SignedManifest

11.138.1 Detailed Description

```
<manifest/> element.
```

Definition at line 303 of file publication.py.

11.138.2 Member Data Documentation

11.138.2.1 string rpki.publication.manifest_elt.element_name = "manifest" [static]

Definition at line 308 of file publication.py.

11.138.2.2 rpki.publication.manifest_elt.payload_type = rpki.x509.SignedManifest [static]

Reimplemented from rpki.publication.publication_object_elt.

Definition at line 309 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

11.139 rpki.publication.msg Class Reference

Inherits rpki::xml_utils::msg, and rpki::publication::publication_namespace.

Inherited by irbe_cli.publication_msg.

Collaboration diagram for rpki.publication.msg:

Public Member Functions

- def serve_top_level

Static Public Attributes

- tuple pdus

  Dispatch table of PDUs for this protocol.

- int version = 1

  Protocol version.

11.139.1 Detailed Description

```
Publication PDU.
```

Definition at line 362 of file publication.py.

11.139.2 Member Function Documentation

11.139.2.1 def rpki.publication.msg.serve_top_level (*self*, *gctx*, *client*, *cb*)

```
Serve one msg PDU.
```

Definition at line 376 of file publication.py.

11.139.3 Member Data Documentation

11.139.3.1 rpki::publication.msg::pdus [static]

Initial value:

```
dict((x.element_name, x)
              for x in (config_elt, client_elt, certificate_elt, crl_elt, manifes
      t_elt, roa_elt, report_error_elt))
```

Dispatch table of PDUs for this protocol.

Reimplemented in irbe_cli.publication_msg.

Definition at line 373 of file publication.py.

11.139.3.2 rpki::publication.msg::version = 1 [static]

Protocol version.

Reimplemented from rpki.xml_utils.msg.

Definition at line 369 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

11.140 rpki.publication.publication_namespace Class Reference

Inherits object.

Inherited by rpki.publication.control_elt, rpki.publication.msg, rpki.publication.publication_object_elt, and rpki.publication.report_error_elt.

Collaboration diagram for rpki.publication.publication_namespace:

Static Public Attributes

- dictionary nsmap = { None : xmlns }
- string xmlns = "http://www.hactrn.net/uris/rpki/publication-spec/"

11.140.1 Detailed Description

```
XML namespace parameters for publication protocol.
```

Definition at line 39 of file publication.py.

11.140.2 Member Data Documentation

11.140.2.1 dictionary rpki.publication.publication_namespace.nsmap = { None : xmlns } [static]

Definition at line 45 of file publication.py.

11.140.2.2 string rpki.publication.publication_namespace.xmlns = "http://www.hactrn.net/uris/rpki/publication-spec/" [static]

Definition at line 44 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

11.141 rpki.publication.publication_object_elt Class Reference

Inherits rpki::xml_utils::base_elt, and rpki::publication::publication_namespace.

Inherited by rpki.publication.certificate_elt, rpki.publication.crl_elt, rpki.publication.manifest_elt, and rpki.publication.roa_elt.

Collaboration diagram for rpki.publication.publication_object_elt:

Public Member Functions

- def endElement
- def make_publish
- def make_withdraw
- def raise_if_error
- def serve_dispatch
- def serve_publish
- def serve_withdraw
- def toXML
- def uri_to_filename

Static Public Attributes

- tuple attributes = ("action", "tag", "client_handle", "uri")

  XML attributes for this element.

- payload = None
- payload_type = None

11.141.1 Detailed Description

```
Virtual class for publishable objects.  These have very similar
syntax, differences lie in underlying datatype and methods.  XML
methods are a little different from the pattern used for objects
that support the create/set/get/list/destroy actions, but
publishable objects don't go in SQL either so these classes would be
different in any case.
```

Definition at line 164 of file publication.py.

11.141.2 Member Function Documentation

11.141.2.1 def rpki.publication.publication_object_elt.endElement (*self*, *stack*, *name*, *text*)

```
Handle a publishable element element.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 178 of file publication.py.

11.141.2.2 def rpki.publication.publication_object_elt.make_publish (*cls*, *uri*, *obj*, *tag* = `None`)

```
Construct a publication PDU.
```

Definition at line 266 of file publication.py.

11.141.2.3 def rpki.publication.publication_object_elt.make_withdraw (*cls*, *uri*, *obj*, *tag* = `None`)

```
Construct a withdrawal PDU.
```

Definition at line 274 of file publication.py.

11.141.2.4 def rpki.publication.publication_object_elt.raise_if_error (*self*)

```
No-op, since this is not a <report_error/> PDU.
```

Definition at line 281 of file publication.py.

11.141.2.5 def rpki.publication.publication_object_elt.serve_dispatch (*self*, *r_msg*, *cb*, *eb*)

```
Action dispatch handler.
```

Definition at line 196 of file publication.py.

11.141.2.6 def rpki.publication.publication_object_elt.serve_publish (*self*)

```
Publish an object.
```

Definition at line 221 of file publication.py.

11.141.2.7 def rpki.publication.publication_object_elt.serve_withdraw (*self*)

```
Withdraw an object.
```

Definition at line 236 of file publication.py.

11.141.2.8 def rpki.publication.publication_object_elt.toXML (*self*)

```
Generate XML element for publishable object.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 187 of file publication.py.

11.141.2.9 def rpki.publication.publication_object_elt.uri_to_filename (*self*)

```
Convert a URI to a local filename.
```

Definition at line 250 of file publication.py.

11.141.3 Member Data Documentation

11.141.3.1 tuple rpki.publication.publication_object_elt.attributes = ("action", "tag", "client_handle", "uri") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 174 of file publication.py.

11.141.3.2 rpki.publication.publication_object_elt.payload = None [static]

Definition at line 176 of file publication.py.

11.141.3.3 rpki.publication.publication_object_elt.payload_type = None [static]

Reimplemented in rpki.publication.certificate_elt, rpki.publication.crl_elt, rpki.publication.manifest_elt, and rpki.publication.roa_elt.

Definition at line 175 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

11.142 rpki.publication.report_error_elt Class Reference

Inherits rpki::xml_utils::text_elt, and rpki::publication::publication_namespace.

Inherited by irbe_cli.report_error_elt.

Collaboration diagram for rpki.publication.report_error_elt:

Public Member Functions

- def __str__
- def from_exception
- def raise_if_error

Public Attributes

- error_code
- tag

Static Public Attributes

- tuple attributes = ("tag", "error_code")

  XML attributes for this element.

- string element_name = "report_error"
- error_text = None
- string text_attribute = "error_text"

  Name of the class attribute that holds the text value.

11.142.1 Detailed Description

```
<report_error/> element.
```

Definition at line 321 of file publication.py.

11.142.2 Member Function Documentation

11.142.2.1 def rpki.publication.report_error_elt.__str__ (*self*)

```
Convert a base_elt object to string format.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 343 of file publication.py.

11.142.2.2 def rpki.publication.report_error_elt.from_exception (*cls*, *e*, *tag* = None)

```
Generate a <report_error/> element from an exception.
```

Definition at line 333 of file publication.py.

11.142.2.3 def rpki.publication.report_error_elt.raise_if_error (*self*)

```
Raise exception associated with this <report_error/> PDU.
```

Definition at line 352 of file publication.py.

11.142.3 Member Data Documentation

11.142.3.1 tuple rpki.publication.report_error_elt.attributes = ("tag", "error_code") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 327 of file publication.py.

11.142.3.2 string rpki.publication.report_error_elt.element_name = "report_error" [static]

Definition at line 326 of file publication.py.

11.142.3.3 rpki.publication.report_error_elt.error_code

Definition at line 339 of file publication.py.

11.142.3.4 rpki.publication.report_error_elt.error_text = None [static]

Definition at line 330 of file publication.py.

11.142.3.5 rpki.publication.report_error_elt.tag

Definition at line 338 of file publication.py.

11.142.3.6 string rpki.publication.report_error_elt.text_attribute = "error_text" [static]

Name of the class attribute that holds the text value.

Reimplemented from rpki.xml_utils.text_elt.

Definition at line 328 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

11.143 rpki.publication.roa_elt Class Reference

Inherits rpki::publication::publication_object_elt.

Inherited by irbe_cli.roa_elt.

Collaboration diagram for rpki.publication.roa_elt:

Static Public Attributes

- string element_name = "roa"
- payload_type = rpki.x509.ROA

11.143.1 Detailed Description

`<roa/> element.`

Definition at line 311 of file publication.py.

11.143.2 Member Data Documentation

11.143.2.1 string rpki.publication.roa_elt.element_name = "roa" [static]

Definition at line 316 of file publication.py.

11.143.2.2 rpki.publication.roa_elt.payload_type = rpki.x509.ROA [static]

Reimplemented from rpki.publication.publication_object_elt.

Definition at line 317 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

11.144 rpki.publication.sax_handler Class Reference

Inherits rpki::xml_utils::sax_handler.

Inherited by irbe_cli.publication_sax_handler.

Collaboration diagram for rpki.publication.sax_handler:

Static Public Attributes

- string name = "msg"
- pdu = msg
- string version = "1"

11.144.1 Detailed Description

```
SAX handler for publication protocol.
```

Definition at line 406 of file publication.py.

11.144.2 Member Data Documentation

11.144.2.1 string rpki.publication.sax_handler.name = "msg" [static]

Definition at line 412 of file publication.py.

11.144.2.2 rpki.publication.sax_handler.pdu = msg [static]

Reimplemented in irbe_cli.publication_sax_handler.

Definition at line 411 of file publication.py.

11.144.2.3 string rpki.publication.sax_handler.version = "1" [static]

Definition at line 413 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

11.145 rpki.resource_set.resource_bag Class Reference

Inherits object.

Collaboration diagram for rpki.resource_set.resource_bag:

Public Member Functions

- def __eq__
- def __init__
- def __ne__
- def __str__
- def empty
- def from_rfc3779_tuples
- def intersection

- def oversized
- def undersized
- def union

Public Attributes

- asn

  Set of Autonomous System Number resources.

- v4

  Set of IPv4 resources.

- v6

  Set of IPv6 resources.

- valid_until

  Expiration date of resources, for setting certificate notAfter field.

11.145.1 Detailed Description

```
Container to simplify passing around the usual triple of ASN, IPv4,
and IPv6 resource sets.
```

Definition at line 547 of file resource_set.py.

11.145.2 Member Function Documentation

11.145.2.1 def rpki.resource_set.resource_bag.__eq__ (*self*, *other*)

Definition at line 615 of file resource_set.py.

11.145.2.2 def rpki.resource_set.resource_bag.__init__ (*self*, *asn* = `None`, *v4* = `None`, *v6* = `None`, *valid_until* = `None`)

Definition at line 565 of file resource_set.py.

11.145.2.3 def rpki.resource_set.resource_bag.__ne__ (*self*, *other*)

Definition at line 621 of file resource_set.py.

11.145.2.4 def rpki.resource_set.resource_bag.__str__ (*self*)

Definition at line 644 of file resource_set.py.

11.145.2.5 def rpki.resource_set.resource_bag.empty (*self*)

```
True iff all resource sets in this bag are empty.
```

Definition at line 611 of file resource_set.py.

11.145.2.6 def rpki.resource_set.resource_bag.from_rfc3779_tuples (*cls*, *exts*)

```
Build a resource_bag from intermediate form generated by RFC 3779
ASN.1 decoder.
```

Definition at line 588 of file resource_set.py.

11.145.2.7 def rpki.resource_set.resource_bag.intersection (*self*, *other*)

```
Compute intersection with another resource_bag.  valid_until
attribute (if any) inherits from self.
```

Definition at line 624 of file resource_set.py.

11.145.2.8 def rpki.resource_set.resource_bag.oversized (*self*, *other*)

```
True iff self is oversized with respect to other.
```

Definition at line 571 of file resource_set.py.

11.145.2.9 def rpki.resource_set.resource_bag.undersized (*self*, *other*)

```
True iff self is undersized with respect to other.
```

Definition at line 579 of file resource_set.py.

11.145.2.10 def rpki.resource_set.resource_bag.union (*self*, *other*)

```
Compute union with another resource_bag.  valid_until attribute
(if any) inherits from self.
```

Definition at line 634 of file resource_set.py.

11.145.3 Member Data Documentation

11.145.3.1 rpki::resource_set.resource_bag::asn

Set of Autonomous System Number resources.

Definition at line 566 of file resource_set.py.

11.145.3.2 rpki::resource_set.resource_bag::v4

Set of IPv4 resources.

Definition at line 567 of file resource_set.py.

11.145.3.3 rpki::resource_set.resource_bag::v6

Set of IPv6 resources.

Definition at line 568 of file resource_set.py.

11.145.3.4 rpki::resource_set.resource_bag::valid_until

Expiration date of resources, for setting certificate notAfter field.

Definition at line 569 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

11.146 rpki.resource_set.resource_range Class Reference

Inherits object.

Inherited by rpki.resource_set.resource_range_as, and rpki.resource_set.resource_-range_ip.

Collaboration diagram for rpki.resource_set.resource_range:

Public Member Functions

- def __cmp__
- def __init__

Public Attributes

- max

- min

11.146.1 Detailed Description

```
Generic resource range type.  Assumes underlying type is some kind
of integer.

This is a virtual class.  You probably don't want to use this type
directly.
```

Definition at line 50 of file resource_set.py.

11.146.2 Member Function Documentation

11.146.2.1 def rpki.resource_set.resource_range.__cmp__ (*self*, *other*)

```
Compare two resource_range objects.
```

Definition at line 67 of file resource_set.py.

11.146.2.2 def rpki.resource_set.resource_range.__init__ (*self*, *min*, *max*)

```
Initialize and sanity check a resource_range.
```

Definition at line 59 of file resource_set.py.

11.146.3 Member Data Documentation

11.146.3.1 rpki.resource_set.resource_range.max

Definition at line 65 of file resource_set.py.

11.146.3.2 rpki.resource_set.resource_range.min

Reimplemented in rpki.resource_set.resource_range_as.

Definition at line 64 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

11.147 rpki.resource_set.resource_range_as Class Reference

Inherits rpki::resource_set::resource_range.

Collaboration diagram for rpki.resource_set.resource_range_as:

Public Member Functions

- def __str__
- def to_rfc3779_tuple

Public Attributes

- min

Static Public Attributes

- datum_type = long

  Type of underlying data (min and max).

11.147.1 Detailed Description

```
Range of Autonomous System Numbers.

Denotes a single ASN by a range whose min and max values are
identical.
```

Definition at line 78 of file resource_set.py.

11.147.2 Member Function Documentation

11.147.2.1 def rpki.resource_set.resource_range_as.__str__ (*self*)

```
Convert a resource_range_as to string format.
```

Definition at line 91 of file resource_set.py.

11.147.2.2 def rpki.resource_set.resource_range_as.to_rfc3779_tuple (*self*)

```
Convert a resource_range_as to tuple format for RFC 3779 ASN.1 encoding.
```

Definition at line 100 of file resource_set.py.

11.147.3 Member Data Documentation

11.147.3.1 rpki::resource_set.resource_range_as::datum_type = long [static]

Type of underlying data (min and max).

Definition at line 89 of file resource_set.py.

11.147.3.2 rpki.resource_set.resource_range_as.min

Reimplemented from rpki.resource_set.resource_range.

Definition at line 95 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

11.148 rpki.resource_set.resource_range_ip Class Reference

Inherits rpki::resource_set::resource_range.

Inherited by rpki.resource_set.resource_range_ipv4, and rpki.resource_set.resource_-range_ipv6.

Collaboration diagram for rpki.resource_set.resource_range_ip:

Public Member Functions

- def __str__
- def make_prefix
- def to_rfc3779_tuple

Private Member Functions

- def _prefixlen

11.148.1 Detailed Description

```
Range of (generic) IP addresses.

Prefixes are converted to ranges on input, and ranges that can be
represented as prefixes are written as prefixes on output.

This is a virtual class.  You probably don't want to use it
directly.
```

Definition at line 109 of file resource_set.py.

11.148.2 Member Function Documentation

11.148.2.1 def rpki.resource_set.resource_range_ip.__str__ (*self*)

```
Convert a resource_range_ip to string format.
```

Definition at line 137 of file resource_set.py.

11.148.2.2 def rpki.resource_set.resource_range_ip._prefixlen (*self*) [private]

```
Determine whether a resource_range_ip can be expressed as a
prefix.
```

Definition at line 120 of file resource_set.py.

11.148.2.3 def rpki.resource_set.resource_range_ip.make_prefix (*cls*, *prefix*, *prefixlen*)

```
Construct a resource range corresponding to a prefix.
```

Definition at line 160 of file resource_set.py.

11.148.2.4 def rpki.resource_set.resource_range_ip.to_rfc3779_tuple (*self*)

```
Convert a resource_range_ip to tuple format for RFC 3779 ASN.1
encoding.
```

Definition at line 147 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

11.149 rpki.resource_set.resource_range_ipv4 Class Reference

Inherits rpki::resource_set::resource_range_ip.

Collaboration diagram for rpki.resource_set.resource_range_ipv4:

Static Public Attributes

- datum_type = rpki.ipaddrs.v4addr

  Type of underlying data (min and max).

11.149.1 Detailed Description

```
Range of IPv4 addresses.
```

Definition at line 170 of file resource_set.py.

11.149.2 Member Data Documentation

11.149.2.1 rpki::resource_set.resource_range_ipv4::datum_type = rpki.ipaddrs.v4addr [static]

Type of underlying data (min and max).

Definition at line 178 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

11.150 rpki.resource_set.resource_range_ipv6 Class Reference

Inherits rpki::resource_set::resource_range_ip.

Collaboration diagram for rpki.resource_set.resource_range_ipv6:

Static Public Attributes

- datum_type = rpki.ipaddrs.v6addr

  Type of underlying data (min and max).

11.150.1 Detailed Description

```
Range of IPv6 addresses.
```

Definition at line 180 of file resource_set.py.

11.150.2 Member Data Documentation

11.150.2.1 rpki::resource_set.resource_range_ipv6::datum_type = rpki.ipaddrs.v6addr [static]

Type of underlying data (min and max).

Definition at line 188 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

11.151 rpki.resource_set.resource_set Class Reference

Inherits list.

Inherited by rpki.resource_set.resource_set_as, and rpki.resource_set.resource_set_ip.

Collaboration diagram for rpki.resource_set.resource_set:

Public Member Functions

- def __init__
- def __str__
- def contains
- def difference
- def from_sql
- def intersection
- def issubset
- def issuperset
- def symmetric_difference
- def union

Static Public Attributes

- inherit = False

  Boolean indicating whether this resource_set uses RFC 3779 inheritance.

Private Member Functions

- def _comm

11.151.1 Detailed Description

```
Generic resource set, a list subclass containing resource ranges.

This is a virtual class.  You probably don't want to use it
directly.
```

Definition at line 206 of file resource_set.py.

11.151.2 Member Function Documentation

11.151.2.1 def rpki.resource_set.resource_set.__init__ (*self*, *ini* = `None`)

```
Initialize a resource_set.
```

Definition at line 219 of file resource_set.py.

11.151.2.2 def rpki.resource_set.resource_set.__str__ (*self*)

```
Convert a resource_set to string format.
```

Definition at line 246 of file resource_set.py.

11.151.2.3 def rpki.resource_set.resource_set._comm (*self*, *other*) `[private]`

```
Like comm(1), sort of.

Returns a tuple of three resource sets: resources only in self,
resources only in other, and resources in both.  Used (not very
efficiently) as the basis for most set operations on resource
sets.
```

Definition at line 255 of file resource_set.py.

11.151.2.4 def rpki.resource_set.resource_set.contains (*self*, *item*)

```
Set membership test for resource sets.
```

Definition at line 332 of file resource_set.py.

11.151.2.5 def rpki.resource_set.resource_set.difference (*self*, *other*)

```
Set difference for resource sets.
```

Definition at line 323 of file resource_set.py.

11.151.2.6 def rpki.resource_set.resource_set.from_sql (*cls*, *sql*, *query*, *args* = **None**)

```
Create resource set from an SQL query.

sql is an object that supports execute() and fetchall() methods
like a DB API 2.0 cursor object.

query is an SQL query that returns a sequence of (min, max) pairs.
```

Definition at line 369 of file resource_set.py.

11.151.2.7 def rpki.resource_set.resource_set.intersection (*self*, *other*)

```
Set intersection for resource sets.
```

Definition at line 319 of file resource_set.py.

11.151.2.8 def rpki.resource_set.resource_set.issubset (*self*, *other*)

```
Test whether self is a subset (possibly improper) of other.
```

Definition at line 355 of file resource_set.py.

11.151.2.9 def rpki.resource_set.resource_set.issuperset (*self*, *other*)

```
Test whether self is a superset (possibly improper) of other.
```

Definition at line 364 of file resource_set.py.

11.151.2.10 def rpki.resource_set.resource_set.symmetric_difference (*self*, *other*)

```
Set symmetric difference (XOR) for resource sets.
```

Definition at line 327 of file resource_set.py.

11.151.2.11 def rpki.resource_set.resource_set.union (*self*, *other*)

```
Set union for resource sets.
```

Definition at line 288 of file resource_set.py.

11.151.3 Member Data Documentation

11.151.3.1 rpki::resource_set.resource_set::inherit = False [static]

Boolean indicating whether this resource_set uses RFC 3779 inheritance.

Reimplemented in rpki.resource_set.resource_set_as, and rpki.resource_set.resource_set_ip.

Definition at line 217 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

11.152 rpki.resource_set.resource_set_as Class Reference

Inherits rpki::resource_set::resource_set.

Collaboration diagram for rpki.resource_set.resource_set_as:

Public Member Functions

- def parse_rfc3779_tuple
- def parse_str
- def to_rfc3779_tuple

Public Attributes

- inherit

  Boolean indicating whether this resource_set uses RFC 3779 inheritance.

Static Public Attributes

- range_type = resource_range_as

  Type of range underlying this type of resource_set.

11.152.1 Detailed Description

```
Autonomous System Number resource set.
```

Definition at line 384 of file resource_set.py.

11.152.2 Member Function Documentation

11.152.2.1 def rpki.resource_set.resource_set_as.parse_rfc3779_tuple (*self*, *x*)

```
Parse ASN resource from tuple format generated by RFC 3779 ASN.1
decoder.
```

Definition at line 404 of file resource_set.py.

11.152.2.2 def rpki.resource_set.resource_set_as.parse_str (*self*, *x*)

```
Parse ASN resource sets from text (eg, XML attributes).
```

Definition at line 394 of file resource_set.py.

11.152.2.3 def rpki.resource_set.resource_set_as.to_rfc3779_tuple (*self*)

```
Convert ASN resource set into tuple format used for RFC 3779 ASN.1
encoding.
```

Definition at line 422 of file resource_set.py.

11.152.3 Member Data Documentation

11.152.3.1 rpki.resource_set.resource_set_as.inherit

Boolean indicating whether this resource_set uses RFC 3779 inheritance.

Reimplemented from rpki.resource_set.resource_set.

Definition at line 420 of file resource_set.py.

11.152.3.2 rpki::resource_set.resource_set_as::range_type = resource_range_as [static]

Type of range underlying this type of resource_set.

Definition at line 392 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

11.153 rpki.resource_set.resource_set_ip Class Reference

Inherits rpki::resource_set::resource_set.

Inherited by rpki.resource_set.resource_set_ipv4, and rpki.resource_set.resource_set_-ipv6.

Collaboration diagram for rpki.resource_set.resource_set_ip:

Public Member Functions

- def parse_rfc3779_tuple
- def parse_str
- def to_rfc3779_tuple

Public Attributes

- inherit

  Boolean indicating whether this resource_set uses RFC 3779 inheritance.

11.153.1 Detailed Description

```
(Generic) IP address resource set.

This is a virtual class.  You probably don't want to use it
directly.
```

Definition at line 434 of file resource_set.py.

11.153.2 Member Function Documentation

11.153.2.1 def rpki.resource_set.resource_set_ip.parse_rfc3779_tuple (*self*, *x*)

```
Parse IP address resource sets from tuple format generated by RFC
3779 ASN.1 decoder.
```

Definition at line 454 of file resource_set.py.

11.153.2.2 def rpki.resource_set.resource_set_ip.parse_str (*self*, *x*)

```
Parse IP address resource sets from text (eg, XML attributes).
```

Definition at line 442 of file resource_set.py.

11.153.2.3 def rpki.resource_set.resource_set_ip.to_rfc3779_tuple (*self*)

```
Convert IP resource set into tuple format used by RFC 3779 ASN.1
encoder.
```

Definition at line 472 of file resource_set.py.

11.153.3 Member Data Documentation

11.153.3.1 rpki.resource_set.resource_set_ip.inherit

Boolean indicating whether this resource_set uses RFC 3779 inheritance.

Reimplemented from rpki.resource_set.resource_set.

Definition at line 470 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

11.154 rpki.resource_set.resource_set_ipv4 Class Reference

Inherits rpki::resource_set::resource_set_ip.

Collaboration diagram for rpki.resource_set.resource_set_ipv4:

Static Public Attributes

- string afi = "\x00\x01"

  Address Family Identifier value for IPv4.

- range_type = resource_range_ipv4

  Type of range underlying this type of resource_set.

11.154.1 Detailed Description

```
IPv4 address resource set.
```

Definition at line 484 of file resource_set.py.

11.154.2 Member Data Documentation

11.154.2.1 rpki::resource_set.resource_set_ipv4::afi = "\x00\x01" [static]

Address Family Identifier value for IPv4.

Definition at line 497 of file resource_set.py.

11.154.2.2 rpki::resource_set.resource_set_ipv4::range_type = resource_range_ipv4 [static]

Type of range underlying this type of resource_set.

Definition at line 492 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

11.155 rpki.resource_set.resource_set_ipv6 Class Reference

Inherits rpki::resource_set::resource_set_ip.

Collaboration diagram for rpki.resource_set.resource_set_ipv6:

Static Public Attributes

- string afi = "\x00\x02"

  Address Family Identifier value for IPv6.

- range_type = resource_range_ipv6

  Type of range underlying this type of resource_set.

11.155.1 Detailed Description

```
IPv6 address resource set.
```

Definition at line 499 of file resource_set.py.

11.155.2 Member Data Documentation

11.155.2.1 rpki::resource_set.resource_set_ipv6::afi = "\x00\x02" [static]

Address Family Identifier value for IPv6.

Definition at line 512 of file resource_set.py.

11.155.2.2 rpki::resource_set.resource_set_ipv6::range_type = resource_range_ipv6 [static]

Type of range underlying this type of resource_set.

Definition at line 507 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

11.156 rpki.resource_set.roa_prefix Class Reference

Inherits object.

Inherited by rpki.resource_set.roa_prefix_ipv4, and rpki.resource_set.roa_prefix_ipv6.

Collaboration diagram for rpki.resource_set.roa_prefix:

Public Member Functions

- def __cmp__
- def __init__
- def __str__
- def max
- def min
- def to_resource_range
- def to_roa_tuple

Public Attributes

- max_prefixlen

Maxmimum prefix length.

- prefix

  The prefix itself, an IP address with bits beyond the prefix length zeroed.

- prefixlen

  (Minimum) prefix length.

11.156.1 Detailed Description

```
ROA prefix.  This is similar to the resource_range_ip class, but
differs in that it only represents prefixes, never ranges, and
includes the maximum prefix length as an additional value.

This is a virtual class, you probably don't want to use it directly.
```

Definition at line 666 of file resource_set.py.

11.156.2 Member Function Documentation

11.156.2.1 def rpki.resource_set.roa_prefix.__cmp__ (*self*, *other*)

```
Compare two ROA prefix objects.  Comparision is based on prefix,
prefixlen, and max_prefixlen, in that order.
```

Definition at line 697 of file resource_set.py.

11.156.2.2 def rpki.resource_set.roa_prefix.__init__ (*self*, *prefix*, *prefixlen*, *max_prefixlen* = `None`)

```
Initialize a ROA prefix.  max_prefixlen is optional and defaults
to prefixlen.  max_prefixlen must not be smaller than prefixlen.
```

Definition at line 685 of file resource_set.py.

11.156.2.3 def rpki.resource_set.roa_prefix.__str__ (*self*)

```
Convert a ROA prefix to string format.
```

Definition at line 710 of file resource_set.py.

11.156.2.4 def rpki.resource_set.roa_prefix.max (*self*)

```
Return highest address covered by prefix.
```

Definition at line 731 of file resource_set.py.

11.156.2.5 def rpki.resource_set.roa_prefix.min (*self*)

```
Return lowest address covered by prefix.
```

Definition at line 727 of file resource_set.py.

11.156.2.6 def rpki.resource_set.roa_prefix.to_resource_range (*self*)

```
Convert this ROA prefix to the equivilent resource_range_ip
object.  This is an irreversable transformation because it loses
the max_prefixlen attribute, nothing we can do about that.
```

Definition at line 719 of file resource_set.py.

11.156.2.7 def rpki.resource_set.roa_prefix.to_roa_tuple (*self*)

```
Convert a resource_range_ip to tuple format for ROA ASN.1
encoding.
```

Definition at line 738 of file resource_set.py.

11.156.3 Member Data Documentation

11.156.3.1 rpki::resource_set.roa_prefix::max_prefixlen

Maxmimum prefix length.

Definition at line 695 of file resource_set.py.

11.156.3.2 rpki::resource_set.roa_prefix::prefix

The prefix itself, an IP address with bits beyond the prefix length zeroed.

Definition at line 693 of file resource_set.py.

11.156.3.3 rpki::resource_set.roa_prefix::prefixlen

(Minimum) prefix length.

Definition at line 694 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

11.157 rpki.resource_set.roa_prefix_ipv4 Class Reference

Inherits rpki::resource_set::roa_prefix.

Collaboration diagram for rpki.resource_set.roa_prefix_ipv4:

Static Public Attributes

- range_type = resource_range_ipv4

  Type of corresponding resource_range_ip.

11.157.1 Detailed Description

```
IPv4 ROA prefix.
```

Definition at line 746 of file resource_set.py.

11.157.2 Member Data Documentation

11.157.2.1 rpki::resource_set.roa_prefix_ipv4::range_type = resource_range_ipv4 [static]

Type of corresponding resource_range_ip.

Definition at line 754 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

11.158 rpki.resource_set.roa_prefix_ipv6 Class Reference

Inherits rpki::resource_set::roa_prefix.

Collaboration diagram for rpki.resource_set.roa_prefix_ipv6:

Static Public Attributes

- range_type = resource_range_ipv6

  Type of corresponding resource_range_ip.

11.158.1 Detailed Description

```
IPv6 ROA prefix.
```

Definition at line 756 of file resource_set.py.

11.158.2 Member Data Documentation

11.158.2.1 rpki::resource_set.roa_prefix_ipv6::range_type = resource_range_ipv6 [static]

Type of corresponding resource_range_ip.

Definition at line 764 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

11.159 rpki.resource_set.roa_prefix_set Class Reference

Inherits list.

Inherited by rpki.resource_set.roa_prefix_set_ipv4, and rpki.resource_set.roa_prefix_-set_ipv6.

Collaboration diagram for rpki.resource_set.roa_prefix_set:

Public Member Functions

- def __init__
- def __str__
- def from_sql
- def parse_str
- def to_resource_set
- def to_roa_tuple

11.159.1 Detailed Description

```
Set of ROA prefixes, analogous to the resource_set_ip class.
```

Definition at line 766 of file resource_set.py.

11.159.2 Member Function Documentation

11.159.2.1 def rpki.resource_set.roa_prefix_set.__init__ (*self*, *ini* = `None`)

```
Initialize a ROA prefix set.
```

Definition at line 771 of file resource_set.py.

11.159.2.2 def rpki.resource_set.roa_prefix_set.__str__ (*self*)

```
Convert a ROA prefix set to string format.
```

Definition at line 791 of file resource_set.py.

11.159.2.3 def rpki.resource_set.roa_prefix_set.from_sql (*cls*, *sql*, *query*, *args* = `None`)

```
Create ROA prefix set from an SQL query.

sql is an object that supports execute() and fetchall() methods
like a DB API 2.0 cursor object.

query is an SQL query that returns a sequence of (prefix,
prefixlen, max_prefixlen) triples.
```

Definition at line 825 of file resource_set.py.

11.159.2.4 def rpki.resource_set.roa_prefix_set.parse_str (*self*, *x*)

```
Parse ROA prefix from text (eg, an XML attribute).
```

Definition at line 795 of file resource_set.py.

11.159.2.5 def rpki.resource_set.roa_prefix_set.to_resource_set (*self*)

```
Convert a ROA prefix set to a resource set.  This is an
irreversable transformation.  We have to compute a union here
because ROA prefix sets can include overlaps, while RFC 3779
resource sets cannot.  This is ugly, and there is almost certainly
a more efficient way to do this, but start by getting the output
right before worrying about making it fast or pretty.
```

Definition at line 807 of file resource_set.py.

11.159.2.6 def rpki.resource_set.roa_prefix_set.to_roa_tuple (*self*)

```
Convert ROA prefix set into tuple format used by ROA ASN.1
encoder.  This is a variation on the format used in RFC 3779.
```

Definition at line 840 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

11.160 rpki.resource_set.roa_prefix_set_ipv4 Class Reference

Inherits rpki::resource_set::roa_prefix_set.

Collaboration diagram for rpki.resource_set.roa_prefix_set_ipv4:

Static Public Attributes

- prefix_type = roa_prefix_ipv4

  Type of underlying roa_prefix.

- resource_set_type = resource_set_ipv4

  Type of corresponding resource_set_ip class.

11.160.1 Detailed Description

```
Set of IPv4 ROA prefixes.
```

Definition at line 850 of file resource_set.py.

11.160.2 Member Data Documentation

11.160.2.1 rpki::resource_set.roa_prefix_set_ipv4::prefix_type = roa_prefix_ipv4 [static]

Type of underlying roa_prefix.

Definition at line 858 of file resource_set.py.

11.160.2.2 rpki::resource_set.roa_prefix_set_ipv4::resource_set_type = resource_set_ipv4 [static]

Type of corresponding resource_set_ip class.

Definition at line 863 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

11.161 rpki.resource_set.roa_prefix_set_ipv6 Class Reference

Inherits rpki::resource_set::roa_prefix_set.

Collaboration diagram for rpki.resource_set.roa_prefix_set_ipv6:

Static Public Attributes

- prefix_type = roa_prefix_ipv6

  Type of underlying roa_prefix.

- resource_set_type = resource_set_ipv6

  Type of corresponding resource_set_ip class.

11.161.1 Detailed Description

```
Set of IPv6 ROA prefixes.
```

Definition at line 865 of file resource_set.py.

11.161.2 Member Data Documentation

11.161.2.1 rpki::resource_set.roa_prefix_set_ipv6::prefix_type = roa_prefix_ipv6 [static]

Type of underlying roa_prefix.

Definition at line 873 of file resource_set.py.

11.161.2.2 rpki::resource_set.roa_prefix_set_ipv6::resource_set_type = resource_set_ipv6 [static]

Type of corresponding resource_set_ip class.

Definition at line 878 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

11.162 rpki.roa.ROAIPAddress Class Reference

Inherits Sequence.

Collaboration diagram for rpki.roa.ROAIPAddress:

Public Member Functions

- def __init__

Public Attributes

- address
- maxLength

11.162.1 Detailed Description

Definition at line 47 of file roa.py.

11.162.2 Member Function Documentation

11.162.2.1 def rpki.roa.ROAIPAddress.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 48 of file roa.py.

11.162.3 Member Data Documentation

11.162.3.1 rpki.roa.ROAIPAddress.address

Definition at line 49 of file roa.py.

11.162.3.2 rpki.roa.ROAIPAddress.maxLength

Definition at line 50 of file roa.py.

The documentation for this class was generated from the following file:

- roa.py (2424)

11.163 rpki.roa.ROAIPAddresses Class Reference

Inherits SequenceOf.

Collaboration diagram for rpki.roa.ROAIPAddresses:

Public Member Functions

- def __init__

11.163.1 Detailed Description

Definition at line 54 of file roa.py.

11.163.2 Member Function Documentation

11.163.2.1 def rpki.roa.ROAIPAddresses.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 55 of file roa.py.

The documentation for this class was generated from the following file:

- roa.py (2424)

11.164 rpki.roa.ROAIPAddressFamilies Class Reference

Inherits SequenceOf.

Collaboration diagram for rpki.roa.ROAIPAddressFamilies:

Public Member Functions

- def __init__

11.164.1 Detailed Description

Definition at line 65 of file roa.py.

11.164.2 Member Function Documentation

11.164.2.1 def rpki.roa.ROAIPAddressFamilies.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 66 of file roa.py.

The documentation for this class was generated from the following file:

- roa.py (2424)

11.165 rpki.roa.ROAIPAddressFamily Class Reference

Inherits Sequence.

Collaboration diagram for rpki.roa.ROAIPAddressFamily:

Public Member Functions

- def __init__

Public Attributes

- addresses
- addressFamily

11.165.1 Detailed Description

Definition at line 58 of file roa.py.

11.165.2 Member Function Documentation

11.165.2.1 def rpki.roa.ROAIPAddressFamily.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 59 of file roa.py.

11.165.3 Member Data Documentation

11.165.3.1 rpki.roa.ROAIPAddressFamily.addresses

Definition at line 61 of file roa.py.

11.165.3.2 rpki.roa.ROAIPAddressFamily.addressFamily

Definition at line 60 of file roa.py.

The documentation for this class was generated from the following file:

- roa.py (2424)

11.166 rpki.roa.RouteOriginAttestation Class Reference

Inherits Sequence.

Collaboration diagram for rpki.roa.RouteOriginAttestation:

Public Member Functions

- def __init__

Public Attributes

- asID
- explicitVersion
- ipAddrBlocks
- version

11.166.1 Detailed Description

Definition at line 69 of file roa.py.

11.166.2 Member Function Documentation

11.166.2.1 def rpki.roa.RouteOriginAttestation.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 70 of file roa.py.

11.166.3 Member Data Documentation

11.166.3.1 rpki.roa.RouteOriginAttestation.asID

Definition at line 73 of file roa.py.

11.166.3.2 rpki.roa.RouteOriginAttestation.explicitVersion

Definition at line 72 of file roa.py.

11.166.3.3 rpki.roa.RouteOriginAttestation.ipAddrBlocks

Definition at line 74 of file roa.py.

11.166.3.4 rpki.roa.RouteOriginAttestation.version

Definition at line 71 of file roa.py.

The documentation for this class was generated from the following file:

- roa.py (2424)

11.167 rpki.rpki_engine.ca_detail_obj Class Reference

Inherits rpki::sql::sql_persistent.

Collaboration diagram for rpki.rpki_engine.ca_detail_obj:

Public Member Functions

- def activate
- def ca
- def child_certs
- def create
- def crl_published_callback

- def crl_uri
- def crl_uri_tail
- def delete
- def generate_crl
- def generate_manifest
- def generate_manifest_cert
- def issue
- def issue_ee
- def manifest_published_callback
- def manifest_uri
- def revoke
- def revoked_certs
- def roas
- def sql_decode
- def update

Public Attributes

- ca_cert_uri
- ca_id
- gctx
- latest_crl
- latest_manifest
- latest_manifest_cert
- manifest_private_key_id
- manifest_public_key
- nextUpdate
- private_key_id
- public_key
- state

Static Public Attributes

- crl_published = None
- latest_ca_cert = None
- manifest_published = None
- tuple sql_template

11.167.1 Detailed Description

```
Internal CA detail object.
```

Definition at line 562 of file rpki_engine.py.

11.167.2 Member Function Documentation

11.167.2.1 def rpki.rpki_engine.ca_detail_obj.activate (*self*, *ca*, *cert*, *uri*, *callback*, *errback*, *predecessor* = `None`)

```
Activate this ca_detail.
```

Definition at line 624 of file rpki_engine.py.

11.167.2.2 def rpki.rpki_engine.ca_detail_obj.ca (*self*)

```
Fetch CA object to which this ca_detail links.
```

Definition at line 596 of file rpki_engine.py.

11.167.2.3 def rpki.rpki_engine.ca_detail_obj.child_certs (*self*, *child* = `None`, *ski* = `None`, *unique* = `False`)

```
Fetch all child_cert objects that link to this ca_detail.
```

Definition at line 600 of file rpki_engine.py.

11.167.2.4 def rpki.rpki_engine.ca_detail_obj.create (*cls*, *ca*)

```
Create a new ca_detail object for a specified CA.
```

Definition at line 762 of file rpki_engine.py.

11.167.2.5 def rpki.rpki_engine.ca_detail_obj.crl_published_callback (*self*, *pdu*)

```
Check result of CRL publication.
```

Definition at line 885 of file rpki_engine.py.

11.167.2.6 def rpki.rpki_engine.ca_detail_obj.crl_uri (*self*, *ca*)

```
Return publication URI for this ca_detail's CRL.
```

Definition at line 612 of file rpki_engine.py.

11.167.2.7 def rpki.rpki_engine.ca_detail_obj.crl_uri_tail (*self*)

```
Return tail (filename portion) of publication URI for this ca_detail's CRL.
```

Definition at line 616 of file rpki_engine.py.

11.167.2.8 def rpki.rpki_engine.ca_detail_obj.delete (*self*, *ca*, *publisher*, *allow_failure* = `False`)

```
Delete this ca_detail and all of the certs it issued.

If allow_failure is true, we clean up as much as we can but don't
raise an exception.
```

Definition at line 649 of file rpki_engine.py.

11.167.2.9 def rpki.rpki_engine.ca_detail_obj.generate_crl (*self*, *publisher*, *nextUpdate* = `None`)

```
Generate a new CRL for this ca_detail.  At the moment this is
unconditional, that is, it is up to the caller to decide whether a
new CRL is needed.
```

Definition at line 849 of file rpki_engine.py.

11.167.2.10 def rpki.rpki_engine.ca_detail_obj.generate_manifest (*self*, *publisher*, *nextUpdate* = `None`)

```
Generate a new manifest for this ca_detail.
```

Definition at line 893 of file rpki_engine.py.

11.167.2.11 def rpki.rpki_engine.ca_detail_obj.generate_manifest_cert (*self*, *ca*)

```
Generate a new manifest certificate for this ca_detail.
```

Definition at line 797 of file rpki_engine.py.

11.167.2.12 def rpki.rpki_engine.ca_detail_obj.issue (*self*, *ca*, *child*, *subject_key*, *sia*, *resources*, *publisher*, *child_cert* = `None`)

```
Issue a new certificate to a child.  Optional child_cert argument
specifies an existing child_cert object to update in place; if not
specified, we create a new one.  Returns the child_cert object
containing the newly issued cert.
```

Definition at line 809 of file rpki_engine.py.

11.167.2.13 def rpki.rpki_engine.ca_detail_obj.issue_ee (*self*, *ca*, *resources*, *subject_key*, *sia* = `None`)

```
Issue a new EE certificate.
```

Definition at line 780 of file rpki_engine.py.

11.167.2.14 def rpki.rpki_engine.ca_detail_obj.manifest_published_callback (*self*, *pdu*)

```
Check result of manifest publication.
```

Definition at line 927 of file rpki_engine.py.

11.167.2.15 def rpki.rpki_engine.ca_detail_obj.manifest_uri (*self*, *ca*)

```
Return publication URI for this ca_detail's manifest.
```

Definition at line 620 of file rpki_engine.py.

11.167.2.16 def rpki.rpki_engine.ca_detail_obj.revoke (*self*, *cb*, *eb*)

```
Request revocation of all certificates whose SKI matches the key
for this ca_detail.

Tasks:

- Request revocation of old keypair by parent.

- Revoke all child certs issued by the old keypair.

- Generate a final CRL, signed with the old keypair, listing all
  the revoked certs, with a next CRL time after the last cert or
  CRL signed by the old keypair will have expired.

- Generate a corresponding final manifest.

- Destroy old keypairs.

- Leave final CRL and manifest in place until their nextupdate
  time has passed.
```

Definition at line 673 of file rpki_engine.py.

11.167.2.17 def rpki.rpki_engine.ca_detail_obj.revoked_certs (*self*)

```
Fetch all revoked_cert objects that link to this ca_detail.
```

Definition at line 604 of file rpki_engine.py.

11.167.2.18 def rpki.rpki_engine.ca_detail_obj.roas (*self*)

```
Fetch all ROA objects that link to this ca_detail.
```

Definition at line 608 of file rpki_engine.py.

11.167.2.19 def rpki.rpki_engine.ca_detail_obj.sql_decode (*self*, *vals*)

```
Extra assertions for SQL decode of a ca_detail_obj.
```

Reimplemented from rpki.sql.sql_persistent.

Definition at line 588 of file rpki_engine.py.

11.167.2.20 def rpki.rpki_engine.ca_detail_obj.update (*self*, *parent*, *ca*, *rc*, *sia_uri_changed*, *old_resources*, *callback*, *errback*)

```
Need to get a new certificate for this ca_detail and perhaps frob
children of this ca_detail.
```

Definition at line 737 of file rpki_engine.py.

11.167.3 Member Data Documentation

11.167.3.1 rpki.rpki_engine.ca_detail_obj.ca_cert_uri

Definition at line 632 of file rpki_engine.py.

11.167.3.2 rpki.rpki_engine.ca_detail_obj.ca_id

Definition at line 768 of file rpki_engine.py.

11.167.3.3 rpki.rpki_engine.ca_detail_obj.crl_published = None [static]

Definition at line 584 of file rpki_engine.py.

11.167.3.4 rpki.rpki_engine.ca_detail_obj.gctx

Reimplemented from rpki.sql.sql_persistent.

Definition at line 767 of file rpki_engine.py.

11.167.3.5 rpki.rpki_engine.ca_detail_obj.latest_ca_cert = None [static]

Definition at line 586 of file rpki_engine.py.

11.167.3.6 rpki.rpki_engine.ca_detail_obj.latest_crl

Definition at line 872 of file rpki_engine.py.

11.167.3.7 rpki.rpki_engine.ca_detail_obj.latest_manifest

Definition at line 913 of file rpki_engine.py.

11.167.3.8 rpki.rpki_engine.ca_detail_obj.latest_manifest_cert

Definition at line 730 of file rpki_engine.py.

11.167.3.9 rpki.rpki_engine.ca_detail_obj.manifest_private_key_id

Definition at line 728 of file rpki_engine.py.

11.167.3.10 rpki.rpki_engine.ca_detail_obj.manifest_public_key

Definition at line 729 of file rpki_engine.py.

11.167.3.11 rpki.rpki_engine.ca_detail_obj.manifest_published = None [static]

Definition at line 585 of file rpki_engine.py.

11.167.3.12 rpki.rpki_engine.ca_detail_obj.nextUpdate

Definition at line 706 of file rpki_engine.py.

11.167.3.13 rpki.rpki_engine.ca_detail_obj.private_key_id

Definition at line 727 of file rpki_engine.py.

11.167.3.14 rpki.rpki_engine.ca_detail_obj.public_key

Definition at line 772 of file rpki_engine.py.

11.167.3.15 tuple rpki.rpki_engine.ca_detail_obj.sql_template [static]

Initial value:

```
rpki.sql.template(
    "ca_detail",
    "ca_detail_id",
    ("private_key_id",          rpki.x509.RSA),
    ("public_key",              rpki.x509.RSApublic),
    ("latest_ca_cert",          rpki.x509.X509),
    ("manifest_private_key_id", rpki.x509.RSA),
    ("manifest_public_key",     rpki.x509.RSApublic),
    ("latest_manifest_cert",    rpki.x509.X509),
    ("latest_manifest",         rpki.x509.SignedManifest),
    ("latest_crl",              rpki.x509.CRL),
    ("crl_published",           rpki.sundial.datetime),
    ("manifest_published",      rpki.sundial.datetime),
    "state",
    "ca_cert_uri",
    "ca_id")
```

Definition at line 567 of file rpki_engine.py.

11.167.3.16 rpki.rpki_engine.ca_detail_obj.state

Definition at line 634 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- rpki_engine.py (3107)

11.168 rpki.rpki_engine.ca_obj Class Reference

Inherits rpki::sql::sql_persistent.

Collaboration diagram for rpki.rpki_engine.ca_obj:

Public Member Functions

- def ca_details
- def check_for_updates
- def construct_sia_uri
- def create
- def delete

- def fetch_active
- def fetch_deprecated
- def fetch_issue_response_candidates
- def fetch_pending
- def fetch_revoked
- def next_crl_number
- def next_manifest_number
- def next_serial_number
- def parent
- def rekey
- def revoke

Public Attributes

- gctx
- parent_id
- parent_resource_class
- sia_uri

Static Public Attributes

- int last_crl_sn = 0
- int last_issued_sn = 0
- int last_manifest_sn = 0
- tuple sql_template

11.168.1 Detailed Description

```
Internal CA object.
```

Definition at line 308 of file rpki_engine.py.

11.168.2 Member Function Documentation

11.168.2.1 def rpki.rpki_engine.ca_obj.ca_details (*self*)

```
Fetch all ca_detail objects that link to this CA object.
```

Definition at line 330 of file rpki_engine.py.

11.168.2.2 def rpki.rpki_engine.ca_obj.check_for_updates (*self*, *parent*, *rc*, *cb*, *eb*)

```
Parent has signaled continued existance of a resource class we
already knew about, so we need to check for an updated
certificate, changes in resource coverage, revocation and reissue
with the same key, etc.
```

Definition at line 371 of file rpki_engine.py.

11.168.2.3 def rpki.rpki_engine.ca_obj.construct_sia_uri (*self*, *parent*, *rc*)

```
Construct the sia_uri value for this CA given configured
information and the parent's up-down protocol list_response PDU.
```

Definition at line 358 of file rpki_engine.py.

11.168.2.4 def rpki.rpki_engine.ca_obj.create (*cls*, *parent*, *rc*, *cb*, *eb*)

```
Parent has signaled existance of a new resource class, so we need
to create and set up a corresponding CA object.
```

Definition at line 451 of file rpki_engine.py.

11.168.2.5 def rpki.rpki_engine.ca_obj.delete (*self*, *parent*, *callback*)

```
The list of current resource classes received from parent does not
include the class corresponding to this CA, so we need to delete
it (and its little dog too...).

All certs published by this CA are now invalid, so need to
withdraw them, the CRL, and the manifest from the repository,
delete all child_cert and ca_detail records associated with this
CA, then finally delete this CA itself.
```

Definition at line 475 of file rpki_engine.py.

11.168.2.6 def rpki.rpki_engine.ca_obj.fetch_active (*self*)

```
Fetch the active ca_detail for this CA, if any.
```

Definition at line 338 of file rpki_engine.py.

11.168.2.7 def rpki.rpki_engine.ca_obj.fetch_deprecated (*self*)

```
Fetch deprecated ca_details for this CA, if any.
```

Definition at line 342 of file rpki_engine.py.

11.168.2.8 def rpki.rpki_engine.ca_obj.fetch_issue_response_candidates (*self*)

```
Fetch ca_details which are candidates for consideration when
processing an up-down issue_response PDU.
```

Definition at line 350 of file rpki_engine.py.

11.168.2.9 def rpki.rpki_engine.ca_obj.fetch_pending (*self*)

```
Fetch the pending ca_details for this CA, if any.
```

Definition at line 334 of file rpki_engine.py.

11.168.2.10 def rpki.rpki_engine.ca_obj.fetch_revoked (*self*)

```
Fetch revoked ca_details for this CA, if any.
```

Definition at line 346 of file rpki_engine.py.

11.168.2.11 def rpki.rpki_engine.ca_obj.next_crl_number (*self*)

```
Allocate a CRL serial number.
```

Definition at line 517 of file rpki_engine.py.

11.168.2.12 def rpki.rpki_engine.ca_obj.next_manifest_number (*self*)

```
Allocate a manifest serial number.
```

Definition at line 509 of file rpki_engine.py.

11.168.2.13 def rpki.rpki_engine.ca_obj.next_serial_number (*self*)

```
Allocate a certificate serial number.
```

Definition at line 501 of file rpki_engine.py.

11.168.2.14 def rpki.rpki_engine.ca_obj.parent (*self*)

```
Fetch parent object to which this CA object links.
```

Definition at line 326 of file rpki_engine.py.

11.168.2.15 def rpki.rpki_engine.ca_obj.rekey (*self*, *cb*, *eb*)

```
Initiate a rekey operation for this ca.  Generate a new keypair.
Request cert from parent using new keypair.  Mark result as our
active ca_detail.  Reissue all child certs issued by this ca using
the new ca_detail.
```

Definition at line 525 of file rpki_engine.py.

11.168.2.16 def rpki.rpki_engine.ca_obj.revoke (*self*, *cb*, *eb*)

```
Revoke deprecated ca_detail objects associated with this ca.
```

Definition at line 550 of file rpki_engine.py.

11.168.3 Member Data Documentation

11.168.3.1 rpki.rpki_engine.ca_obj.gctx

Reimplemented from rpki.sql.sql_persistent.

Definition at line 458 of file rpki_engine.py.

11.168.3.2 int rpki.rpki_engine.ca_obj.last_crl_sn = 0 [static]

Definition at line 322 of file rpki_engine.py.

11.168.3.3 int rpki.rpki_engine.ca_obj.last_issued_sn = 0 [static]

Definition at line 323 of file rpki_engine.py.

11.168.3.4 int rpki.rpki_engine.ca_obj.last_manifest_sn = 0 [static]

Definition at line 324 of file rpki_engine.py.

11.168.3.5 rpki.rpki_engine.ca_obj.parent_id

Definition at line 459 of file rpki_engine.py.

11.168.3.6 rpki.rpki_engine.ca_obj.parent_resource_class

Definition at line 460 of file rpki_engine.py.

11.168.3.7 rpki.rpki_engine.ca_obj.sia_uri

Definition at line 382 of file rpki_engine.py.

11.168.3.8 tuple rpki.rpki_engine.ca_obj.sql_template [static]

Initial value:

```
rpki.sql.template(
    "ca",
    "ca_id",
    "last_crl_sn",
    ("next_crl_update", rpki.sundial.datetime),
    "last_issued_sn", "last_manifest_sn",
    ("next_manifest_update", rpki.sundial.datetime),
    "sia_uri", "parent_id", "parent_resource_class")
```

Definition at line 313 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- rpki_engine.py (3107)

11.169 rpki.rpki_engine.child_cert_obj Class Reference

Inherits rpki::sql::sql_persistent.

Collaboration diagram for rpki.rpki_engine.child_cert_obj:

Public Member Functions

- def __init__
- def ca_detail
- def child
- def fetch
- def published_callback

- def reissue
- def revoke
- def uri
- def uri_tail

Public Attributes

- ca_detail_id
- cert
- child_id
- gctx
- published

Static Public Attributes

- tuple sql_template

11.169.1 Detailed Description

```
Certificate that has been issued to a child.
```

Definition at line 936 of file rpki_engine.py.

11.169.2 Member Function Documentation

11.169.2.1 def rpki.rpki_engine.child_cert_obj.__init__ (*self*, *gctx* = `None`, *child_id* = `None`, *ca_detail_id* = `None`, *cert* = `None`)

```
Initialize a child_cert_obj.
```

Definition at line 950 of file rpki_engine.py.

11.169.2.2 def rpki.rpki_engine.child_cert_obj.ca_detail (*self*)

```
Fetch ca_detail object to which this child_cert object links.
```

Definition at line 967 of file rpki_engine.py.

11.169.2.3 def rpki.rpki_engine.child_cert_obj.child (*self*)

```
Fetch child object to which this child_cert object links.
```

Definition at line 963 of file rpki_engine.py.

11.169.2.4 def rpki.rpki_engine.child_cert_obj.fetch (*cls*, *gctx* = **None**, *child* = **None**, *ca_detail* = **None**, *ski* = **None**, *unique* = **False**)

```
Fetch all child_cert objects matching a particular set of
parameters.  This is a wrapper to consolidate various queries that
would otherwise be inline SQL WHERE expressions.  In most cases
code calls this indirectly, through methods in other classes.
```

Definition at line 1048 of file rpki_engine.py.

11.169.2.5 def rpki.rpki_engine.child_cert_obj.published_callback (*self*, *pdu*)

```
Publication callback: check result and mark published.
```

Definition at line 1080 of file rpki_engine.py.

11.169.2.6 def rpki.rpki_engine.child_cert_obj.reissue (*self*, *ca_detail*, *publisher*, *resources* = **None**, *sia* = **None**)

```
Reissue an existing child cert, reusing the public key.  If the
child cert we would generate is identical to the one we already
have, we just return the one we already have.  If we have to
revoke the old child cert when generating the new one, we have to
generate a new child_cert_obj, so calling code that needs the
updated child_cert_obj must use the return value from this method.
```

Definition at line 991 of file rpki_engine.py.

11.169.2.7 def rpki.rpki_engine.child_cert_obj.revoke (*self*, *publisher*)

```
Revoke a child cert.
```

Definition at line 979 of file rpki_engine.py.

11.169.2.8 def rpki.rpki_engine.child_cert_obj.uri (*self*, *ca*)

```
Return the publication URI for this child_cert.
```

Definition at line 975 of file rpki_engine.py.

11.169.2.9 def rpki.rpki_engine.child_cert_obj.uri_tail (*self*)

```
Return the tail (filename) portion of the URI for this child_cert.
```

Definition at line 971 of file rpki_engine.py.

11.169.3 Member Data Documentation

11.169.3.1 rpki.rpki_engine.child_cert_obj.ca_detail_id

Definition at line 957 of file rpki_engine.py.

11.169.3.2 rpki.rpki_engine.child_cert_obj.cert

Definition at line 958 of file rpki_engine.py.

11.169.3.3 rpki.rpki_engine.child_cert_obj.child_id

Definition at line 956 of file rpki_engine.py.

11.169.3.4 rpki.rpki_engine.child_cert_obj.gctx

Reimplemented from rpki.sql.sql_persistent.

Definition at line 955 of file rpki_engine.py.

11.169.3.5 rpki.rpki_engine.child_cert_obj.published

Definition at line 959 of file rpki_engine.py.

11.169.3.6 tuple rpki.rpki_engine.child_cert_obj.sql_template [static]

Initial value:

```
rpki.sql.template(
    "child_cert",
    "child_cert_id",
    ("cert", rpki.x509.X509),
    "child_id",
    "ca_detail_id",
    "ski",
    ("published", rpki.sundial.datetime))
```

Definition at line 941 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- rpki_engine.py (3107)

11.170 rpki.rpki_engine.publication_queue Class Reference

Inherits object.

Collaboration diagram for rpki.rpki_engine.publication_queue:

Public Member Functions

- def __init__
- def call_pubd
- def publish
- def withdraw

Public Attributes

- handlers
- msgs
- repositories
- uris

Static Public Attributes

- replace = True

Private Member Functions

- def _add

11.170.1 Detailed Description

```
Utility to simplify publication from within rpkid.

General idea here is to accumulate a collection of objects to be
published, in one or more repositories, each potentially with its
own completion callback.  Eventually we want to publish everything
we've accumulated, at which point we need to iterate over the
collection and do repository.call_pubd() for each repository.
```

Definition at line 1366 of file rpki_engine.py.

11.170.2 Member Function Documentation

11.170.2.1 def rpki.rpki_engine.publication_queue.__init__ (*self*)

Definition at line 1379 of file rpki_engine.py.

11.170.2.2 def rpki.rpki_engine.publication_queue._add (*self*, *cls*, *uri*, *obj*, *repository*, *handler*, *withdraw*) [private]

Definition at line 1386 of file rpki_engine.py.

11.170.2.3 def rpki.rpki_engine.publication_queue.call_pubd (*self*, *cb*, *eb*)

Definition at line 1409 of file rpki_engine.py.

11.170.2.4 def rpki.rpki_engine.publication_queue.publish (*self*, *cls*, *uri*, *obj*, *repository*, *handler* = None)

Definition at line 1403 of file rpki_engine.py.

11.170.2.5 def rpki.rpki_engine.publication_queue.withdraw (*self*, *cls*, *uri*, *obj*, *repository*, *handler* = `None`)

Definition at line 1406 of file rpki_engine.py.

11.170.3 Member Data Documentation

11.170.3.1 rpki.rpki_engine.publication_queue.handlers

Definition at line 1382 of file rpki_engine.py.

11.170.3.2 rpki.rpki_engine.publication_queue.msgs

Definition at line 1381 of file rpki_engine.py.

11.170.3.3 rpki.rpki_engine.publication_queue.replace = True `[static]`

Definition at line 1377 of file rpki_engine.py.

11.170.3.4 rpki.rpki_engine.publication_queue.repositories

Definition at line 1380 of file rpki_engine.py.

11.170.3.5 rpki.rpki_engine.publication_queue.uris

Definition at line 1384 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- rpki_engine.py (3107)

11.171 rpki.rpki_engine.revoked_cert_obj Class Reference

Inherits rpki::sql::sql_persistent.

Collaboration diagram for rpki.rpki_engine.revoked_cert_obj:

Public Member Functions

- def __init__
- def ca_detail

- def revoke

Public Attributes

- ca_detail_id
- expires
- gctx
- revoked
- serial

Static Public Attributes

- tuple sql_template

11.171.1 Detailed Description

```
Tombstone for a revoked certificate.
```

Definition at line 1088 of file rpki_engine.py.

11.171.2 Member Function Documentation

11.171.2.1 def rpki.rpki_engine.revoked_cert_obj.__init__ (*self*, *gctx* = `None`, *serial* = `None`, *revoked* = `None`, *expires* = `None`, *ca_detail_id* = `None`)

```
Initialize a revoked_cert_obj.
```

Definition at line 1101 of file rpki_engine.py.

11.171.2.2 def rpki.rpki_engine.revoked_cert_obj.ca_detail (*self*)

```
Fetch ca_detail object to which this revoked_cert_obj links.
```

Definition at line 1112 of file rpki_engine.py.

11.171.2.3 def rpki.rpki_engine.revoked_cert_obj.revoke (*cls*, *cert*, *ca_detail*)

```
Revoke a certificate.
```

Definition at line 1117 of file rpki_engine.py.

11.171.3 Member Data Documentation

11.171.3.1 rpki.rpki_engine.revoked_cert_obj.ca_detail_id

Definition at line 1108 of file rpki_engine.py.

11.171.3.2 rpki.rpki_engine.revoked_cert_obj.expires

Definition at line 1107 of file rpki_engine.py.

11.171.3.3 rpki.rpki_engine.revoked_cert_obj.gctx

Reimplemented from rpki.sql.sql_persistent.

Definition at line 1104 of file rpki_engine.py.

11.171.3.4 rpki.rpki_engine.revoked_cert_obj.revoked

Definition at line 1106 of file rpki_engine.py.

11.171.3.5 rpki.rpki_engine.revoked_cert_obj.serial

Definition at line 1105 of file rpki_engine.py.

11.171.3.6 tuple rpki.rpki_engine.revoked_cert_obj.sql_template [static]

Initial value:

```
rpki.sql.template(
    "revoked_cert",
    "revoked_cert_id",
    "serial",
    "ca_detail_id",
    ("revoked", rpki.sundial.datetime),
    ("expires", rpki.sundial.datetime))
```

Definition at line 1093 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- rpki_engine.py (3107)

11.172 rpki.rpki_engine.roa_obj Class Reference

Inherits rpki::sql::sql_persistent.

Collaboration diagram for rpki.rpki_engine.roa_obj:

Public Member Functions

- def __init__
- def ca_detail
- def generate
- def published_callback
- def regenerate

- def revoke
- def self
- def sql_delete_hook
- def sql_fetch_hook
- def sql_insert_hook
- def update
- def uri
- def uri_tail

Public Attributes

- asn
- gctx
- ipv4
- ipv6
- self_id

Static Public Attributes

- ca_detail_id = None
- cert = None
- published = None
- roa = None
- tuple sql_template

11.172.1 Detailed Description

```
Route Origin Authorization.
```

Definition at line 1128 of file rpki_engine.py.

11.172.2 Member Function Documentation

11.172.2.1 def rpki.rpki_engine.roa_obj.__init__ (*self*, *gctx* = `None`, *self_id* = `None`, *asn* = `None`, *ipv4* = `None`, *ipv6* = `None`)

Definition at line 1194 of file rpki_engine.py.

11.172.2.2 def rpki.rpki_engine.roa_obj.ca_detail (*self*)

```
Fetch ca_detail object to which this roa_obj links.
```

Definition at line 1154 of file rpki_engine.py.

11.172.2.3 def rpki.rpki_engine.roa_obj.generate (*self*, *publisher*)

```
Generate a ROA.

At present this does not support ROAs with multiple signatures
(neither does the current CMS code).

At present we have no way of performing a direct lookup from a
desired set of resources to a covering certificate, so we have to
search.  This could be quite slow if we have a lot of active
ca_detail objects.  Punt on the issue for now, revisit if
profiling shows this as a hotspot.

Once we have the right covering certificate, we generate the ROA
payload, generate a new EE certificate, use the EE certificate to
sign the ROA payload, publish the result, then throw away the
private key for the EE cert, all per the ROA specification.  This
implies that generating a lot of ROAs will tend to thrash
/dev/random, but there is not much we can do about that.
```

Definition at line 1237 of file rpki_engine.py.

11.172.2.4 def rpki.rpki_engine.roa_obj.published_callback (*self*, *pdu*)

```
Check publication result.
```

Definition at line 1303 of file rpki_engine.py.

11.172.2.5 def rpki.rpki_engine.roa_obj.regenerate (*self*, *publisher*)

```
Reissue ROA associated with this roa_obj.
```

Definition at line 1343 of file rpki_engine.py.

11.172.2.6 def rpki.rpki_engine.roa_obj.revoke (*self*, *publisher*, *regenerate* = `False`, *allow_failure* = `False`)

```
Withdraw ROA associated with this roa_obj.

In order to preserve make-before-break properties without
duplicating code, this method also handles generating a
replacement ROA when requested.

If allow_failure is set, failing to withdraw the ROA will not be
considered an error.
```

Definition at line 1311 of file rpki_engine.py.

11.172.2.7 def rpki.rpki_engine.roa_obj.self (*self*)

```
Fetch self object to which this roa_obj links.
```

Definition at line 1148 of file rpki_engine.py.

11.172.2.8 def rpki.rpki_engine.roa_obj.sql_delete_hook (*self*)

```
Extra SQL delete actions for roa_obj -- handle prefix lists.
```

Reimplemented from rpki.sql.sql_persistent.

Definition at line 1188 of file rpki_engine.py.

11.172.2.9 def rpki.rpki_engine.roa_obj.sql_fetch_hook (*self*)

```
Extra SQL fetch actions for roa_obj -- handle prefix lists.
```

Reimplemented from rpki.sql.sql_persistent.

Definition at line 1160 of file rpki_engine.py.

11.172.2.10 def rpki.rpki_engine.roa_obj.sql_insert_hook (*self*)

```
Extra SQL insert actions for roa_obj -- handle prefix lists.
```

Reimplemented from rpki.sql.sql_persistent.

Definition at line 1174 of file rpki_engine.py.

11.172.2.11 def rpki.rpki_engine.roa_obj.update (*self*, *publisher*)

```
Bring this roa_obj's ROA up to date if necesssary.
```

Definition at line 1207 of file rpki_engine.py.

11.172.2.12 def rpki.rpki_engine.roa_obj.uri (*self*, *key* = `None`)

```
Return the publication URI for this roa_obj's ROA.
```

Definition at line 1352 of file rpki_engine.py.

11.172.2.13 def rpki.rpki_engine.roa_obj.uri_tail (*self*, *key* = `None`)

```
Return the tail (filename portion) of the publication URI for this
roa_obj's ROA.
```

Definition at line 1358 of file rpki_engine.py.

11.172.3 Member Data Documentation

11.172.3.1 rpki.rpki_engine.roa_obj.asn

Definition at line 1198 of file rpki_engine.py.

11.172.3.2 rpki.rpki_engine.roa_obj.ca_detail_id = None `[static]`

Definition at line 1143 of file rpki_engine.py.

11.172.3.3 rpki.rpki_engine.roa_obj.cert = None [static]

Definition at line 1144 of file rpki_engine.py.

11.172.3.4 rpki.rpki_engine.roa_obj.gctx

Reimplemented from rpki.sql.sql_persistent.

Definition at line 1196 of file rpki_engine.py.

11.172.3.5 rpki.rpki_engine.roa_obj.ipv4

Definition at line 1199 of file rpki_engine.py.

11.172.3.6 rpki.rpki_engine.roa_obj.ipv6

Definition at line 1200 of file rpki_engine.py.

11.172.3.7 rpki.rpki_engine.roa_obj.published = None [static]

Definition at line 1146 of file rpki_engine.py.

11.172.3.8 rpki.rpki_engine.roa_obj.roa = None [static]

Definition at line 1145 of file rpki_engine.py.

11.172.3.9 rpki.rpki_engine.roa_obj.self_id

Definition at line 1197 of file rpki_engine.py.

11.172.3.10 tuple rpki.rpki_engine.roa_obj.sql_template [static]

Initial value:

```
rpki.sql.template(
    "roa",
    "roa_id",
    "ca_detail_id",
    "self_id",
    "asn",
    ("roa", rpki.x509.ROA),
    ("cert", rpki.x509.X509),
    ("published", rpki.sundial.datetime))
```

Definition at line 1133 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- rpki_engine.py (3107)

11.173 rpki.rpki_engine.rpkid_context Class Reference

Inherits object.

Collaboration diagram for rpki.rpki_engine.rpkid_context:

Public Member Functions

- def __init__
- def build_https_ta_cache
- def checkpoint
- def clear_https_ta_cache
- def cron

- def cronjob_handler
- def irdb_query
- def irdb_query_child_resources
- def irdb_query_roa_requests
- def left_right_handler
- def start_cron
- def up_down_handler

Public Attributes

- bpki_ta
- cron_keepalive
- cron_period
- cron_timeout
- cron_timer
- https_server_host
- https_server_port
- initial_delay
- irbe_cert
- irdb_cert
- irdb_url
- publication_kludge_base
- rpkid_cert
- rpkid_key
- sql
- use_internal_cron

Static Public Attributes

- https_ta_cache = None

  HTTPS trust anchor cache, to avoid regenerating it for every TLS connection.

- tuple up_down_url_regexp = re.compile("/up-down/([-A-Z0-9_]+)/([-A-Z0-9_-]+)$", re.I)

11.173.1 Detailed Description

```
A container for various global rpkid parameters.
```

Definition at line 39 of file rpki_engine.py.

11.173.2 Member Function Documentation

11.173.2.1 def rpki.rpki_engine.rpkid_context.__init__ (*self*, *cfg*)

Definition at line 44 of file rpki_engine.py.

11.173.2.2 def rpki.rpki_engine.rpkid_context.build_https_ta_cache (*self*)

```
Build dynamic TLS trust anchors.
```

Definition at line 288 of file rpki_engine.py.

11.173.2.3 def rpki.rpki_engine.rpkid_context.checkpoint (*self*)

```
Record that we were still alive when we got here, by resetting
keepalive timer.
```

Definition at line 200 of file rpki_engine.py.

11.173.2.4 def rpki.rpki_engine.rpkid_context.clear_https_ta_cache (*self*)

```
Clear dynamic TLS trust anchors.
```

Definition at line 279 of file rpki_engine.py.

11.173.2.5 def rpki.rpki_engine.rpkid_context.cron (*self*, *cb* = `None`)

```
Periodic tasks.
```

Definition at line 207 of file rpki_engine.py.

11.173.2.6 def rpki.rpki_engine.rpkid_context.cronjob_handler (*self*, *query*, *path*, *cb*)

```
External trigger for periodic tasks.  This is somewhat obsolete
now that we have internal timers, but the test framework still
uses it.
```

Definition at line 263 of file rpki_engine.py.

11.173.2.7 def rpki.rpki_engine.rpkid_context.irdb_query (*self*, *q_pdu*, *callback*, *errback*)

```
Perform an IRDB callback query.
```

Definition at line 86 of file rpki_engine.py.

11.173.2.8 def rpki.rpki_engine.rpkid_context.irdb_query_child_resources (*self*, *self_handle*, *child_handle*, *callback*, *errback*)

```
Ask IRDB about a child's resources.
```

Definition at line 112 of file rpki_engine.py.

11.173.2.9 def rpki.rpki_engine.rpkid_context.irdb_query_roa_requests (*self*, *self_handle*, *callback*, *errback*)

```
Ask IRDB about self's ROA requests.
```

Definition at line 134 of file rpki_engine.py.

11.173.2.10 def rpki.rpki_engine.rpkid_context.left_right_handler (*self*, *query*, *path*, *cb*)

```
Process one left-right PDU.
```

Definition at line 146 of file rpki_engine.py.

11.173.2.11 def rpki.rpki_engine.rpkid_context.start_cron (*self*)

```
Start clock for rpkid's internal cron process.
```

Definition at line 73 of file rpki_engine.py.

11.173.2.12 def rpki.rpki_engine.rpkid_context.up_down_handler (*self*, *query*, *path*, *cb*)

```
Process one up-down PDU.
```

Definition at line 172 of file rpki_engine.py.

11.173.3 Member Data Documentation

11.173.3.1 rpki.rpki_engine.rpkid_context.bpki_ta

Definition at line 48 of file rpki_engine.py.

11.173.3.2 rpki.rpki_engine.rpkid_context.cron_keepalive

Definition at line 68 of file rpki_engine.py.

11.173.3.3 rpki.rpki_engine.rpkid_context.cron_period

Definition at line 67 of file rpki_engine.py.

11.173.3.4 rpki.rpki_engine.rpkid_context.cron_timeout

Definition at line 71 of file rpki_engine.py.

11.173.3.5 rpki.rpki_engine.rpkid_context.cron_timer

Definition at line 79 of file rpki_engine.py.

11.173.3.6 rpki.rpki_engine.rpkid_context.https_server_host

Definition at line 56 of file rpki_engine.py.

11.173.3.7 rpki.rpki_engine.rpkid_context.https_server_port

Definition at line 57 of file rpki_engine.py.

11.173.3.8 rpki::rpki_engine.rpkid_context::https_ta_cache = None [static]

HTTPS trust anchor cache, to avoid regenerating it for every TLS connection.

Definition at line 277 of file rpki_engine.py.

11.173.3.9 rpki.rpki_engine.rpkid_context.initial_delay

Definition at line 63 of file rpki_engine.py.

11.173.3.10 rpki.rpki_engine.rpkid_context.irbe_cert

Definition at line 50 of file rpki_engine.py.

11.173.3.11 rpki.rpki_engine.rpkid_context.irdb_cert

Definition at line 49 of file rpki_engine.py.

11.173.3.12 rpki.rpki_engine.rpkid_context.irdb_url

Definition at line 54 of file rpki_engine.py.

11.173.3.13 rpki.rpki_engine.rpkid_context.publication_kludge_base

Definition at line 59 of file rpki_engine.py.

11.173.3.14 rpki.rpki_engine.rpkid_context.rpkid_cert

Definition at line 51 of file rpki_engine.py.

11.173.3.15 rpki.rpki_engine.rpkid_context.rpkid_key

Definition at line 52 of file rpki_engine.py.

11.173.3.16 rpki.rpki_engine.rpkid_context.sql

Definition at line 46 of file rpki_engine.py.

11.173.3.17 tuple rpki.rpki_engine.rpkid_context.up_down_url_regexp = re.compile("/up-down/([-A-Z0-9_]+)/([-A-Z0-9_]+)$", re.I) `[static]`

Definition at line 170 of file rpki_engine.py.

11.173.3.18 rpki.rpki_engine.rpkid_context.use_internal_cron

Definition at line 61 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- rpki_engine.py (3107)

11.174 rpki.sql.session Class Reference

Inherits object.

Collaboration diagram for rpki.sql.session:

Public Member Functions

- def __init__
- def assert_pristine
- def cache_clear
- def close
- def connect
- def execute
- def executemany
- def fetchall
- def lastrowid
- def ping
- def sweep

Public Attributes

- cache
- cur
- database
- db
- dirty
- password
- username

Private Member Functions

- def _wrap_execute

Static Private Attributes

- _exceptions_enabled = False

11.174.1 Detailed Description

```
SQL session layer.
```

Definition at line 50 of file sql.py.

11.174.2 Member Function Documentation

11.174.2.1 def rpki.sql.session.__init__ (*self*, *cfg*)

Definition at line 57 of file sql.py.

11.174.2.2 def rpki.sql.session._wrap_execute (*self*, *func*, *query*, *args*) [private]

Definition at line 88 of file sql.py.

11.174.2.3 def rpki.sql.session.assert_pristine (*self*)

```
Assert that there are no dirty objects in the cache.
```

Definition at line 112 of file sql.py.

11.174.2.4 def rpki.sql.session.cache_clear (*self*)

```
Clear the object cache.
```

Definition at line 108 of file sql.py.

11.174.2.5 def rpki.sql.session.close (*self*)

Definition at line 77 of file sql.py.

11.174.2.6 def rpki.sql.session.connect (*self*)

Definition at line 72 of file sql.py.

11.174.2.7 def rpki.sql.session.execute (*self*, *query*, *args* = `None`)

Definition at line 96 of file sql.py.

11.174.2.8 def rpki.sql.session.executemany (*self*, *query*, *args*)

Definition at line 99 of file sql.py.

11.174.2.9 def rpki.sql.session.fetchall (*self*)

Definition at line 102 of file sql.py.

11.174.2.10 def rpki.sql.session.lastrowid (*self*)

Definition at line 105 of file sql.py.

11.174.2.11 def rpki.sql.session.ping (*self*)

Definition at line 85 of file sql.py.

11.174.2.12 def rpki.sql.session.sweep (*self*)

```
Write any dirty objects out to SQL.
```

Definition at line 116 of file sql.py.

11.174.3 Member Data Documentation

11.174.3.1 rpki.sql.session._exceptions_enabled = False [static, private]

Definition at line 55 of file sql.py.

11.174.3.2 rpki.sql.session.cache

Definition at line 67 of file sql.py.

11.174.3.3 rpki.sql.session.cur

Definition at line 74 of file sql.py.

11.174.3.4 rpki.sql.session.database

Definition at line 64 of file sql.py.

11.174.3.5 rpki.sql.session.db

Definition at line 73 of file sql.py.

11.174.3.6 rpki.sql.session.dirty

Definition at line 68 of file sql.py.

11.174.3.7 rpki.sql.session.password

Definition at line 65 of file sql.py.

11.174.3.8 rpki.sql.session.username

Definition at line 63 of file sql.py.

The documentation for this class was generated from the following file:

- sql.py (2895)

11.175 rpki.sql.sql_persistent Class Reference

Inherits object.

Inherited by rpki.left_right.data_elt, rpki.publication.control_elt, rpki.rpki_engine.ca_-detail_obj, rpki.rpki_engine.ca_obj, rpki.rpki_engine.child_cert_obj, rpki.rpki_-engine.revoked_cert_obj, and rpki.rpki_engine.roa_obj.

Collaboration diagram for rpki.sql.sql_persistent:

Public Member Functions

- def sql_decode
- def sql_delete
- def sql_delete_hook
- def sql_encode
- def sql_fetch

- def sql_fetch_all
- def sql_fetch_hook
- def sql_fetch_where
- def sql_fetch_where1
- def sql_init
- def sql_insert_hook
- def sql_is_dirty
- def sql_mark_clean
- def sql_mark_deleted
- def sql_mark_dirty
- def sql_store
- def sql_update_hook

Public Attributes

- gctx

Static Public Attributes

- sql_debug = False

  Enable logging of SQL actions.

- sql_deleted = False

  Whether our cached copy of this object has been deleted.

- sql_in_db = False

  Whether this object is already in SQL or not.

11.175.1 Detailed Description

```
Mixin for persistent class that needs to be stored in SQL.
```

Definition at line 152 of file sql.py.

11.175.2 Member Function Documentation

11.175.2.1 def rpki.sql.sql_persistent.sql_decode (*self*, *vals*)

```
Initialize an object with values returned by self.sql_fetch().
This is a default version that assumes a one-to-one mapping
between column names in SQL and attribute names in Python.  If you
need something fancier, override this.
```

Reimplemented in rpki.rpki_engine.ca_detail_obj.

Definition at line 322 of file sql.py.

11.175.2.2 def rpki.sql.sql_persistent.sql_delete (*self*)

```
Delete this object from SQL.
```

Definition at line 293 of file sql.py.

11.175.2.3 def rpki.sql.sql_persistent.sql_delete_hook (*self*)

```
Customization hook.
```

Reimplemented in rpki.rpki_engine.roa_obj.

Definition at line 348 of file sql.py.

11.175.2.4 def rpki.sql.sql_persistent.sql_encode (*self*)

```
Convert object attributes into a dict for use with canned SQL
queries.  This is a default version that assumes a one-to-one
mapping between column names in SQL and attribute names in Python.
If you need something fancier, override this.
```

Definition at line 309 of file sql.py.

11.175.2.5 def rpki.sql.sql_persistent.sql_fetch (*cls*, *gctx*, *id*)

```
Fetch one object from SQL, based on its primary key.

Since in this one case we know that the primary index is also the
cache key, we check for a cache hit directly in the hope of
bypassing the SQL lookup entirely.
```

```
This method is usually called via a one-line class-specific
wrapper.  As a convenience, we also accept an id of None, and just
return None in this case.
```

Definition at line 173 of file sql.py.

11.175.2.6 def rpki.sql.sql_persistent.sql_fetch_all (*cls*, *gctx*)

```
Fetch all objects of this type from SQL.
```

Definition at line 211 of file sql.py.

11.175.2.7 def rpki.sql.sql_persistent.sql_fetch_hook (*self*)

```
Customization hook.
```

Reimplemented in rpki.rpki_engine.roa_obj.

Definition at line 335 of file sql.py.

11.175.2.8 def rpki.sql.sql_persistent.sql_fetch_where (*cls*, *gctx*, *where*, *args* = `None`, *also_from* = `None`)

```
Fetch objects of this type matching an arbitrary SQL WHERE expression.
```

Definition at line 216 of file sql.py.

11.175.2.9 def rpki.sql.sql_persistent.sql_fetch_where1 (*cls*, *gctx*, *where*, *args* = `None`, *also_from* = `None`)

```
Fetch one object from SQL, based on an arbitrary SQL WHERE expression.
```

Definition at line 196 of file sql.py.

11.175.2.10 def rpki.sql.sql_persistent.sql_init (*cls*, *gctx*, *row*, *key*)

```
Initialize one Python object from the result of a SQL query.
```

Definition at line 243 of file sql.py.

11.175.2.11 def rpki.sql.sql_persistent.sql_insert_hook (*self*)

```
Customization hook.
```

Reimplemented in rpki.rpki_engine.roa_obj.

Definition at line 339 of file sql.py.

11.175.2.12 def rpki.sql.sql_persistent.sql_is_dirty (*self*)

```
Query whether this object needs to be written back to SQL.
```

Definition at line 263 of file sql.py.

11.175.2.13 def rpki.sql.sql_persistent.sql_mark_clean (*self*)

```
Mark this object as not needing to be written back to SQL.
```

Definition at line 259 of file sql.py.

11.175.2.14 def rpki.sql.sql_persistent.sql_mark_deleted (*self*)

```
Mark this object as needing to be deleted in SQL.
```

Definition at line 267 of file sql.py.

11.175.2.15 def rpki.sql.sql_persistent.sql_mark_dirty (*self*)

```
Mark this object as needing to be written back to SQL.
```

Definition at line 255 of file sql.py.

11.175.2.16 def rpki.sql.sql_persistent.sql_store (*self*)

```
Store this object to SQL.
```

Definition at line 271 of file sql.py.

11.175.2.17 def rpki.sql.sql_persistent.sql_update_hook (*self*)

```
Customization hook.
```

Definition at line 343 of file sql.py.

11.175.3 Member Data Documentation

11.175.3.1 rpki.sql.sql_persistent.gctx

Reimplemented in rpki.rpki_engine.ca_obj, rpki.rpki_engine.ca_detail_obj, rpki.rpki_engine.child_cert_obj, rpki.rpki_engine.revoked_cert_obj, and rpki.rpki_-engine.roa_obj.

Definition at line 248 of file sql.py.

11.175.3.2 rpki::sql.sql_persistent::sql_debug = False [static]

Enable logging of SQL actions.

Definition at line 170 of file sql.py.

11.175.3.3 rpki::sql.sql_persistent::sql_deleted = False [static]

Whether our cached copy of this object has been deleted.

Definition at line 165 of file sql.py.

11.175.3.4 rpki::sql.sql_persistent::sql_in_db = False [static]

Whether this object is already in SQL or not.

Definition at line 160 of file sql.py.

The documentation for this class was generated from the following file:

- sql.py (2895)

11.176 rpki.sql.template Class Reference

Inherits object.

Collaboration diagram for rpki.sql.template:

Public Member Functions

- def __init__

Public Attributes

- columns
- delete
- index
- insert
- map

- select
- table
- update

11.176.1 Detailed Description

```
SQL template generator.
```

Definition at line 128 of file sql.py.

11.176.2 Member Function Documentation

11.176.2.1 def rpki.sql.template.__init__ (*self*, *table_name*, *index_column*, *data_columns*)

```
Build a SQL template.
```

Definition at line 133 of file sql.py.

11.176.3 Member Data Documentation

11.176.3.1 rpki.sql.template.columns

Definition at line 140 of file sql.py.

11.176.3.2 rpki.sql.template.delete

Definition at line 150 of file sql.py.

11.176.3.3 rpki.sql.template.index

Definition at line 139 of file sql.py.

11.176.3.4 rpki.sql.template.insert

Definition at line 143 of file sql.py.

11.176.3.5 rpki.sql.template.map

Definition at line 141 of file sql.py.

11.176.3.6 rpki.sql.template.select

Definition at line 142 of file sql.py.

11.176.3.7 rpki.sql.template.table

Definition at line 138 of file sql.py.

11.176.3.8 rpki.sql.template.update

Definition at line 146 of file sql.py.

The documentation for this class was generated from the following file:

- sql.py (2895)

11.177 rpki.sundial.datetime Class Reference

Inherits pydatetime::datetime.

Collaboration diagram for rpki.sundial.datetime:

Public Member Functions

- def __add__
- def __radd__
- def __rsub__
- def __str__
- def __sub__

- def earlier
- def from_sql
- def fromASN1tuple
- def fromdatetime
- def fromGeneralizedTime
- def fromUTCTime
- def fromXMLtime
- def later
- def to_sql
- def toASN1tuple
- def toGeneralizedTime
- def totimestamp
- def toUTCTime
- def toXMLtime

Static Public Attributes

- tuple PKIX_threshhold = pydatetime.datetime(2050, 1, 1)

  Threshold specified in RFC 3280 for switchover from UTCTime to GeneralizedTime.

11.177.1 Detailed Description

```
RPKI extensions to standard datetime.datetime class.  All work here
is in UTC, so we use naive datetime objects.
```

Definition at line 54 of file sundial.py.

11.177.2 Member Function Documentation

11.177.2.1 def rpki.sundial.datetime.__add__ (*self*, *y*)

Definition at line 163 of file sundial.py.

11.177.2.2 def rpki.sundial.datetime.__radd__ (*self*, *y*)

Definition at line 164 of file sundial.py.

11.177.2.3 def rpki.sundial.datetime.__rsub__ (*self*, *y*)

Definition at line 165 of file sundial.py.

11.177.2.4 def rpki.sundial.datetime.__str__ (*self*)

Definition at line 124 of file sundial.py.

11.177.2.5 def rpki.sundial.datetime.__sub__ (*self*, *y*)

Definition at line 166 of file sundial.py.

11.177.2.6 def rpki.sundial.datetime.earlier (*self*, *other*)

```
Return the earlier of two timestamps.
```

Definition at line 159 of file sundial.py.

11.177.2.7 def rpki.sundial.datetime.from_sql (*cls*, *x*)

```
Convert from SQL storage format.
```

Definition at line 136 of file sundial.py.

11.177.2.8 def rpki.sundial.datetime.fromASN1tuple (*cls*, *x*)

```
Convert from ASN.1 tuple representation.
```

Definition at line 86 of file sundial.py.

11.177.2.9 def rpki.sundial.datetime.fromdatetime (*cls*, *x*)

```
Convert a datetime.datetime object into this subclass.  This is
whacky due to the weird constructors for datetime.
```

Definition at line 128 of file sundial.py.

11.177.2.10 def rpki.sundial.datetime.fromGeneralizedTime (*cls*, *x*)

```
Convert from ASN.1 GeneralizedTime.
```

Definition at line 77 of file sundial.py.

11.177.2.11 def rpki.sundial.datetime.fromUTCTime (*cls*, *x*)

```
Convert from ASN.1 UTCTime.
```

Definition at line 68 of file sundial.py.

11.177.2.12 def rpki.sundial.datetime.fromXMLtime (*cls*, *x*)

```
Convert from XML time representation.
```

Definition at line 111 of file sundial.py.

11.177.2.13 def rpki.sundial.datetime.later (*self*, *other*)

```
Return the later of two timestamps.
```

Definition at line 155 of file sundial.py.

11.177.2.14 def rpki.sundial.datetime.to_sql (*self*)

```
Convert to SQL storage format.

There's something whacky going on in the MySQLdb module, it throws
range errors when storing a derived type into a DATETIME column.
Investigate some day, but for now brute force this by copying the
relevant fields into a datetime.datetime for MySQLdb's
consumption.
```

Definition at line 140 of file sundial.py.

11.177.2.15 def rpki.sundial.datetime.toASN1tuple (*self*)

```
Convert to ASN.1 tuple representation.
```

Definition at line 101 of file sundial.py.

11.177.2.16 def rpki.sundial.datetime.toGeneralizedTime (*self*)

```
Convert to ASN.1 GeneralizedTime.
```

Definition at line 81 of file sundial.py.

11.177.2.17 def rpki.sundial.datetime.totimestamp (*self*)

```
Convert to seconds from epoch (like time.time()).  Conversion
method is a bit silly, but avoids time module timezone whackiness.
```

Definition at line 60 of file sundial.py.

11.177.2.18 def rpki.sundial.datetime.toUTCTime (*self*)

```
Convert to ASN.1 UTCTime.
```

Definition at line 72 of file sundial.py.

11.177.2.19 def rpki.sundial.datetime.toXMLtime (*self*)

```
Convert to XML time representation.
```

Definition at line 120 of file sundial.py.

11.177.3 Member Data Documentation

11.177.3.1 rpki::sundial.datetime::PKIX_threshhold = pydatetime.datetime(2050, 1, 1) [static]

Threshold specified in RFC 3280 for switchover from UTCTime to GeneralizedTime.

Definition at line 99 of file sundial.py.

The documentation for this class was generated from the following file:

- sundial.py (3191)

11.178 rpki.sundial.timedelta Class Reference

Inherits pydatetime::timedelta.

Collaboration diagram for rpki.sundial.timedelta:

Public Member Functions

- def __abs__
- def __add__
- def __div__
- def __floordiv__
- def __mul__

- def __neg__
- def __pos__
- def __radd__
- def __rdiv__
- def __rfloordiv__
- def __rmul__
- def __rsub__
- def __sub__
- def convert_to_seconds
- def fromtimedelta
- def parse

Static Public Attributes

- tuple regexp

  Hideously ugly regular expression to parse the complex text form.

- int years_to_seconds = 31556926

  Conversion factor from years to seconds (value furnished by the "units" program).

11.178.1 Detailed Description

```
Timedelta with text parsing.  This accepts two input formats:

- A simple integer, indicating a number of seconds.

- A string of the form "uY vW wD xH yM zS" where u, v, w, x, y, and z
  are integers and Y, W, D, H, M, and S indicate years, weeks, days,
  hours, minutes, and seconds.  All of the fields are optional, but
  at least one must be specified.  Eg,"3D4H" means "three days plus
  four hours".

There is no "months" format, because the definition of a month is too
fuzzy to be useful (what day is six months from August 30th?)

Similarly, the "years" conversion may produce surprising results, as
"one year" in conventional English does not refer to a fixed interval
but rather a fixed (and in some cases undefined) offset within the
Gregorian calendar (what day is one year from February 29th?)  1Y as
implemented by this code refers to a specific number of seconds.
If you mean 365 days or 52 weeks, say that instead.
```

Definition at line 168 of file sundial.py.

11.178.2 Member Function Documentation

11.178.2.1 def rpki.sundial.timedelta.__abs__ (*self*)

Definition at line 243 of file sundial.py.

11.178.2.2 def rpki.sundial.timedelta.__add__ (*self*, *x*)

Definition at line 244 of file sundial.py.

11.178.2.3 def rpki.sundial.timedelta.__div__ (*self*, *x*)

Definition at line 245 of file sundial.py.

11.178.2.4 def rpki.sundial.timedelta.__floordiv__ (*self*, *x*)

Definition at line 246 of file sundial.py.

11.178.2.5 def rpki.sundial.timedelta.__mul__ (*self*, *x*)

Definition at line 247 of file sundial.py.

11.178.2.6 def rpki.sundial.timedelta.__neg__ (*self*)

Definition at line 248 of file sundial.py.

11.178.2.7 def rpki.sundial.timedelta.__pos__ (*self*)

Definition at line 249 of file sundial.py.

11.178.2.8 def rpki.sundial.timedelta.__radd__ (*self*, *x*)

Definition at line 250 of file sundial.py.

11.178.2.9 def rpki.sundial.timedelta.__rdiv__ (*self*, *x*)

Definition at line 251 of file sundial.py.

11.178.2.10 def rpki.sundial.timedelta.__rfloordiv__ (*self*, *x*)

Definition at line 252 of file sundial.py.

11.178.2.11 def rpki.sundial.timedelta.__rmul__ (*self*, *x*)

Definition at line 253 of file sundial.py.

11.178.2.12 def rpki.sundial.timedelta.__rsub__ (*self*, *x*)

Definition at line 254 of file sundial.py.

11.178.2.13 def rpki.sundial.timedelta.__sub__ (*self*, *x*)

Definition at line 255 of file sundial.py.

11.178.2.14 def rpki.sundial.timedelta.convert_to_seconds (*self*)

```
Convert a timedelta interval to seconds.
```

Definition at line 234 of file sundial.py.

11.178.2.15 def rpki.sundial.timedelta.fromtimedelta (*cls*, *x*)

```
Convert a datetime.timedelta object into this subclass.
```

Definition at line 239 of file sundial.py.

11.178.2.16 def rpki.sundial.timedelta.parse (*cls*, *arg*)

```
Parse text into a timedelta object.
```

Definition at line 213 of file sundial.py.

11.178.3 Member Data Documentation

11.178.3.1 rpki::sundial.timedelta::regexp [static]

Initial value:

```
re.compile("\\s*".join(("^",
                                    "(?:(?P<years>\\d+)Y)?",
                                    "(?:(?P<weeks>\\d+)W)?",
                                    "(?:(?P<days>\\d+)D)?",
                                    "(?:(?P<hours>\\d+)H)?",
                                    "(?:(?P<minutes>\\d+)M)?",
                                    "(?:(?P<seconds>\\d+)S)?",
                                    "$")),
                        re.I)
```

Hideously ugly regular expression to parse the complex text form.

Tags are intended for use with re.MatchObject.groupdict() and map directly to the keywords expected by the timedelta constructor.

Definition at line 196 of file sundial.py.

11.178.3.2 rpki::sundial.timedelta::years_to_seconds = 31556926 [static]

Conversion factor from years to seconds (value furnished by the "units" program).

Definition at line 210 of file sundial.py.

The documentation for this class was generated from the following file:

- sundial.py (3191)

11.179 rpki.up_down.base_elt Class Reference

Inherits object.

Inherited by rpki.up_down.certificate_elt, rpki.up_down.class_elt, rpki.up_down.class_response_syntax, rpki.up_down.error_response_pdu, rpki.up_down.issue_pdu, rpki.up_down.list_pdu, rpki.up_down.message_pdu, and rpki.up_down.revoke_syntax.

Collaboration diagram for rpki.up_down.base_elt:

Public Member Functions

- def check_response
- def endElement
- def make_b64elt
- def make_elt
- def serve_pdu
- def startElement

11.179.1 Detailed Description

```
Generic PDU object.

Virtual class, just provides some default methods.
```

Definition at line 43 of file up_down.py.

11.179.2 Member Function Documentation

11.179.2.1 def rpki.up_down.base_elt.check_response (*self*)

```
Placeholder for response checking.
```

Reimplemented in rpki.up_down.issue_response_pdu, and rpki.up_down.error_response_pdu.

Definition at line 91 of file up_down.py.

11.179.2.2 def rpki.up_down.base_elt.endElement (*self*, *stack*, *name*, *text*)

```
Ignore endElement() if there's no specific handler.

If we don't need to do anything else, just pop the stack.
```

Reimplemented in rpki.up_down.certificate_elt, rpki.up_down.class_elt, rpki.up_down.issue_pdu, and rpki.up_down.error_response_pdu.

Definition at line 59 of file up_down.py.

11.179.2.3 def rpki.up_down.base_elt.make_b64elt (*self*, *elt*, *name*, *value* = `None`)

```
Construct a sub-element with Base64 text content.
```

Definition at line 78 of file up_down.py.

11.179.2.4 def rpki.up_down.base_elt.make_elt (*self*, *name*, *attrs*)

```
Construct a element, copying over a set of attributes.
```

Definition at line 67 of file up_down.py.

11.179.2.5 def rpki.up_down.base_elt.serve_pdu (*self*, *q_msg*, *r_msg*, *child*, *callback*, *errback*)

```
Default PDU handler to catch unexpected types.
```

Reimplemented in rpki.up_down.list_pdu, rpki.up_down.issue_pdu, rpki.up_down.revoke_pdu, rootd.list_pdu, rootd.issue_pdu, and rootd.revoke_pdu.

Definition at line 87 of file up_down.py.

11.179.2.6 def rpki.up_down.base_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
Ignore startElement() if there's no specific handler.

Some elements have no attributes and we only care about their
text content.
```

Reimplemented in rpki.up_down.certificate_elt, rpki.up_down.class_elt, rpki.up_down.class_response_syntax, rpki.up_down.issue_pdu, rpki.up_down.revoke_syntax, and rpki.up_down.message_pdu.

Definition at line 50 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

11.180 rpki.up_down.certificate_elt Class Reference

Inherits rpki::up_down::base_elt.

Collaboration diagram for rpki.up_down.certificate_elt:

Public Member Functions

- def endElement
- def startElement
- def toXML

Public Attributes

- cert
- cert_url
- req_resource_set_as
- req_resource_set_ipv4
- req_resource_set_ipv6

11.180.1 Detailed Description

```
Up-Down protocol representation of an issued certificate.
```

Definition at line 128 of file up_down.py.

11.180.2 Member Function Documentation

11.180.2.1 def rpki.up_down.certificate_elt.endElement (*self*, *stack*, *name*, *text*)

```
Handle text content of a <certificate/> element.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 143 of file up_down.py.

11.180.2.2 def rpki.up_down.certificate_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle attributes of <certificate/> element.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 133 of file up_down.py.

11.180.2.3 def rpki.up_down.certificate_elt.toXML (*self*)

```
Generate a <certificate/> element.
```

Definition at line 151 of file up_down.py.

11.180.3 Member Data Documentation

11.180.3.1 rpki.up_down.certificate_elt.cert

Definition at line 148 of file up_down.py.

11.180.3.2 rpki.up_down.certificate_elt.cert_url

Definition at line 138 of file up_down.py.

11.180.3.3 rpki.up_down.certificate_elt.req_resource_set_as

Definition at line 139 of file up_down.py.

11.180.3.4 rpki.up_down.certificate_elt.req_resource_set_ipv4

Definition at line 140 of file up_down.py.

11.180.3.5 rpki.up_down.certificate_elt.req_resource_set_ipv6

Definition at line 141 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

11.181 rpki.up_down.class_elt Class Reference

Inherits rpki::up_down::base_elt.

Collaboration diagram for rpki.up_down.class_elt:

Public Member Functions

- def __init__
- def endElement
- def from_resource_bag
- def startElement
- def to_resource_bag
- def toXML

Public Attributes

- cert_url
- certs
- class_name
- resource_set_as
- resource_set_ipv4
- resource_set_ipv6
- resource_set_notafter
- suggested_sia_head

Static Public Attributes

- issuer = None

11.181.1 Detailed Description

```
Up-Down protocol representation of a resource class.
```

Definition at line 160 of file up_down.py.

11.181.2 Member Function Documentation

11.181.2.1 def rpki.up_down.class_elt.__init__ (*self*)

```
Initialize class_elt.
```

Definition at line 167 of file up_down.py.

11.181.2.2 def rpki.up_down.class_elt.endElement (*self*, *stack*, *name*, *text*)

```
Handle <class/> elements and their children.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 191 of file up_down.py.

11.181.2.3 def rpki.up_down.class_elt.from_resource_bag (*self*, *bag*)

```
Set resources of this class element from a resource_bag.
```

Definition at line 222 of file up_down.py.

11.181.2.4 def rpki.up_down.class_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle <class/> elements and their children.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 172 of file up_down.py.

11.181.2.5 def rpki.up_down.class_elt.to_resource_bag (*self*)

```
Build a resource_bag from from this <class/> element.
```

Definition at line 213 of file up_down.py.

11.181.2.6 def rpki.up_down.class_elt.toXML (*self*)

```
Generate a <class/> element.
```

Definition at line 201 of file up_down.py.

11.181.3 Member Data Documentation

11.181.3.1 rpki.up_down.class_elt.cert_url

Definition at line 184 of file up_down.py.

11.181.3.2 rpki.up_down.class_elt.certs

Definition at line 170 of file up_down.py.

11.181.3.3 rpki.up_down.class_elt.class_name

Definition at line 183 of file up_down.py.

11.181.3.4 rpki.up_down.class_elt.issuer = None [static]

Definition at line 165 of file up_down.py.

11.181.3.5 rpki.up_down.class_elt.resource_set_as

Definition at line 186 of file up_down.py.

11.181.3.6 rpki.up_down.class_elt.resource_set_ipv4

Definition at line 187 of file up_down.py.

11.181.3.7 rpki.up_down.class_elt.resource_set_ipv6

Definition at line 188 of file up_down.py.

11.181.3.8 rpki.up_down.class_elt.resource_set_notafter

Definition at line 189 of file up_down.py.

11.181.3.9 rpki.up_down.class_elt.suggested_sia_head

Definition at line 185 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

11.182 rpki.up_down.class_response_syntax Class Reference

Inherits rpki::up_down::base_elt.

Inherited by rpki.up_down.issue_response_pdu, and rpki.up_down.list_response_pdu.

Collaboration diagram for rpki.up_down.class_response_syntax:

Public Member Functions

- def __init__
- def startElement
- def toXML

Public Attributes

- classes

11.182.1 Detailed Description

```
Syntax for Up-Down protocol "list_response" and "issue_response" PDUs.
```

Definition at line 285 of file up_down.py.

11.182.2 Member Function Documentation

11.182.2.1 def rpki.up_down.class_response_syntax.__init__ (*self*)

```
Initialize class_response_syntax.
```

Definition at line 290 of file up_down.py.

11.182.2.2 def rpki.up_down.class_response_syntax.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle "list_response" and "issue_response" PDUs.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 297 of file up_down.py.

11.182.2.3 def rpki.up_down.class_response_syntax.toXML (*self*)

```
Generate payload of "list_response" and "issue_response" PDUs.
```

Definition at line 307 of file up_down.py.

11.182.3 Member Data Documentation

11.182.3.1 rpki.up_down.class_response_syntax.classes

Definition at line 295 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

11.183 rpki.up_down.cms_msg Class Reference

Inherits rpki::x509::XML_CMS_object.

Inherited by rootd.cms_msg.

Collaboration diagram for rpki.up_down.cms_msg:

Static Public Attributes

- string encoding = "UTF-8"
- saxify = sax_handler.saxify
- schema = rpki.relaxng.up_down

11.183.1 Detailed Description

```
Class to hold a CMS-signed up-down PDU.
```

Definition at line 685 of file up_down.py.

11.183.2 Member Data Documentation

11.183.2.1 string rpki.up_down.cms_msg.encoding = "UTF-8" [static]

Definition at line 690 of file up_down.py.

11.183.2.2 rpki.up_down.cms_msg.saxify = sax_handler.saxify [static]

Reimplemented in rootd.cms_msg.

Definition at line 692 of file up_down.py.

11.183.2.3 rpki.up_down.cms_msg.schema = rpki.relaxng.up_down [static]

Definition at line 691 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

11.184 rpki.up_down.error_response_pdu Class Reference

Inherits rpki::up_down::base_elt.

Collaboration diagram for rpki.up_down.error_response_pdu:

Public Member Functions

- def __init__
- def check_response
- def endElement
- def toXML

Public Attributes

- description
- status

Static Public Attributes

- dictionary codes
- dictionary exceptions

11.184.1 Detailed Description

```
Up-Down protocol "error_response" PDU.
```

Definition at line 505 of file up_down.py.

11.184.2 Member Function Documentation

11.184.2.1 def rpki.up_down.error_response_pdu.__init__ (*self*, *exception* = `None`)

```
Initialize an error_response PDU from an exception object.
```

Definition at line 524 of file up_down.py.

11.184.2.2 def rpki.up_down.error_response_pdu.check_response (*self*)

```
Handle an error response.  For now, just raise an exception,
perhaps figure out something more clever to do later.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 564 of file up_down.py.

11.184.2.3 def rpki.up_down.error_response_pdu.endElement (*self*, *stack*, *name*, *text*)

```
Handle "error_response" PDU.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 533 of file up_down.py.

11.184.2.4 def rpki.up_down.error_response_pdu.toXML (*self*)

```
Generate payload of "error_response" PDU.
```

Definition at line 549 of file up_down.py.

11.184.3 Member Data Documentation

11.184.3.1 dictionary rpki.up_down.error_response_pdu.codes [static]

Initial value:

```
{
    1101 : "Already processing request",
    1102 : "Version number error",
    1103 : "Unrecognised request type",
    1201 : "Request - no such resource class",
    1202 : "Request - no resources allocated in resource class",
    1203 : "Request - badly formed certificate request",
    1301 : "Revoke - no such resource class",
    1302 : "Revoke - no such key",
    2001 : "Internal Server Error - Request not performed" }
```

Definition at line 510 of file up_down.py.

11.184.3.2 rpki.up_down.error_response_pdu.description

Definition at line 531 of file up_down.py.

11.184.3.3 dictionary rpki.up_down.error_response_pdu.exceptions [static]

Initial value:

```
{
    rpki.exceptions.NoActiveCA : 1202 }
```

Definition at line 521 of file up_down.py.

11.184.3.4 rpki.up_down.error_response_pdu.status

Definition at line 530 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

11.185 rpki.up_down.issue_pdu Class Reference

Inherits rpki::up_down::base_elt.

Inherited by rootd.issue_pdu.

Collaboration diagram for rpki.up_down.issue_pdu:

Public Member Functions

- def endElement
- def query
- def serve_pdu
- def startElement
- def toXML

Public Attributes

- class_name
- pkcs10
- req_resource_set_as
- req_resource_set_ipv4
- req_resource_set_ipv6

11.185.1 Detailed Description

```
Up-Down protocol "issue" PDU.
```

Definition at line 317 of file up_down.py.

11.185.2 Member Function Documentation

11.185.2.1 def rpki.up_down.issue_pdu.endElement (*self*, *stack*, *name*, *text*)

```
Handle "issue" PDU.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 332 of file up_down.py.

11.185.2.2 def rpki.up_down.issue_pdu.query (*cls*, *parent*, *ca*, *ca_detail*, *callback*, *errback*)

```
Send an "issue" request to parent associated with ca.
```

Definition at line 418 of file up_down.py.

11.185.2.3 def rpki.up_down.issue_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*, *callback*, *errback*)

```
Serve one issue request PDU.
```

Reimplemented from rpki.up_down.base_elt.

Reimplemented in rootd.issue_pdu.

Definition at line 349 of file up_down.py.

11.185.2.4 def rpki.up_down.issue_pdu.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle "issue" PDU.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 322 of file up_down.py.

11.185.2.5 def rpki.up_down.issue_pdu.toXML (*self*)

```
Generate payload of "issue" PDU.
```

Definition at line 340 of file up_down.py.

11.185.3 Member Data Documentation

11.185.3.1 rpki.up_down.issue_pdu.class_name

Definition at line 327 of file up_down.py.

11.185.3.2 rpki.up_down.issue_pdu.pkcs10

Definition at line 337 of file up_down.py.

11.185.3.3 rpki.up_down.issue_pdu.req_resource_set_as

Definition at line 328 of file up_down.py.

11.185.3.4 rpki.up_down.issue_pdu.req_resource_set_ipv4

Definition at line 329 of file up_down.py.

11.185.3.5 rpki.up_down.issue_pdu.req_resource_set_ipv6

Definition at line 330 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

11.186 rpki.up_down.issue_response_pdu Class Reference

Inherits rpki::up_down::class_response_syntax.

Collaboration diagram for rpki.up_down.issue_response_pdu:

Public Member Functions

- def check_response

11.186.1 Detailed Description

```
Up-Down protocol "issue_response" PDU.
```

Definition at line 431 of file up_down.py.

11.186.2 Member Function Documentation

11.186.2.1 def rpki.up_down.issue_response_pdu.check_response (*self*)

```
Check whether this looks like a reasonable issue_response PDU.
XML schema should be tighter for this response.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 436 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

11.187 rpki.up_down.list_pdu Class Reference

Inherits rpki::up_down::base_elt.

Inherited by rootd.list_pdu.

Collaboration diagram for rpki.up_down.list_pdu:

Public Member Functions

- def query

- def serve_pdu
- def toXML

11.187.1 Detailed Description

```
Up-Down protocol "list" PDU.
```

Definition at line 231 of file up_down.py.

11.187.2 Member Function Documentation

11.187.2.1 def rpki.up_down.list_pdu.query (*cls*, *parent*, *cb*, *eb*)

```
Send a "list" query to parent.
```

Definition at line 273 of file up_down.py.

11.187.2.2 def rpki.up_down.list_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*, *callback*, *errback*)

```
Serve one "list" PDU.
```

Reimplemented from rpki.up_down.base_elt.

Reimplemented in rootd.list_pdu.

Definition at line 240 of file up_down.py.

11.187.2.3 def rpki.up_down.list_pdu.toXML (*self*)

```
Generate (empty) payload of "list" PDU.
```

Definition at line 236 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

11.188 rpki.up_down.list_response_pdu Class Reference

Inherits rpki::up_down::class_response_syntax.

Collaboration diagram for rpki.up_down.list_response_pdu:

11.188.1 Detailed Description

Up-Down protocol "list_response" PDU.

Definition at line 311 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

11.189 rpki.up_down.message_pdu Class Reference

Inherits rpki::up_down::base_elt.

Inherited by rootd.message_pdu.

Collaboration diagram for rpki.up_down.message_pdu:

Public Member Functions

- def __str__
- def log_query
- def make_query
- def serve_error
- def serve_top_level

- def startElement
- def toXML

Public Attributes

- payload
- recipient
- sender
- type
- version

Static Public Attributes

- dictionary name2type
- tuple type2name = dict((v, k) for k, v in name2type.items())
- int version = 1

11.189.1 Detailed Description

```
Up-Down protocol message wrapper PDU.
```

Definition at line 571 of file up_down.py.

11.189.2 Member Function Documentation

11.189.2.1 def rpki.up_down.message_pdu.__str__ (*self*)

```
Convert a message PDU to a string.
```

Definition at line 613 of file up_down.py.

11.189.2.2 def rpki.up_down.message_pdu.log_query (*self*, *child*)

```
Log query we're handling.  Separate method so rootd can override.
```

Reimplemented in rootd.message_pdu.

Definition at line 642 of file up_down.py.

11.189.2.3 def rpki.up_down.message_pdu.make_query (*cls*, *payload*, *sender*, *recipient*)

```
Construct one message PDU.
```

Definition at line 660 of file up_down.py.

11.189.2.4 def rpki.up_down.message_pdu.serve_error (*self*, *exception*)

```
Generate an error_response message PDU.
```

Definition at line 648 of file up_down.py.

11.189.2.5 def rpki.up_down.message_pdu.serve_top_level (*self*, *child*, *callback*)

```
Serve one message request PDU.
```

Definition at line 617 of file up_down.py.

11.189.2.6 def rpki.up_down.message_pdu.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle message PDU.

Payload of the <message/> element varies depending on the "type"
attribute, so after some basic checks we have to instantiate the
right class object to handle whatever kind of PDU this is.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 597 of file up_down.py.

11.189.2.7 def rpki.up_down.message_pdu.toXML (*self*)

```
Generate payload of message PDU.
```

Definition at line 589 of file up_down.py.

11.189.3 Member Data Documentation

11.189.3.1 dictionary rpki.up_down.message_pdu.name2type [static]

Initial value:

```
{
    "list"            : list_pdu,
    "list_response"   : list_response_pdu,
    "issue"           : issue_pdu,
    "issue_response"  : issue_response_pdu,
    "revoke"          : revoke_pdu,
    "revoke_response" : revoke_response_pdu,
    "error_response"  : error_response_pdu }
```

Reimplemented in rootd.message_pdu.

Definition at line 578 of file up_down.py.

11.189.3.2 rpki.up_down.message_pdu.payload

Definition at line 610 of file up_down.py.

11.189.3.3 rpki.up_down.message_pdu.recipient

Definition at line 608 of file up_down.py.

11.189.3.4 rpki.up_down.message_pdu.sender

Definition at line 607 of file up_down.py.

11.189.3.5 rpki.up_down.message_pdu.type

Definition at line 609 of file up_down.py.

11.189.3.6 tuple rpki.up_down.message_pdu.type2name = dict((v, k) for k, v in name2type.items()) [static]

Reimplemented in rootd.message_pdu.

Definition at line 587 of file up_down.py.

11.189.3.7 rpki.up_down.message_pdu.version

Definition at line 606 of file up_down.py.

11.189.3.8 int rpki.up_down.message_pdu.version = 1 `[static]`

Definition at line 576 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

11.190 rpki.up_down.multi_uri Class Reference

Inherits list.

Collaboration diagram for rpki.up_down.multi_uri:

Public Member Functions

- def __init__
- def __str__
- def rsync

11.190.1 Detailed Description

```
Container for a set of URIs.
```

Definition at line 95 of file up_down.py.

11.190.2 Member Function Documentation

11.190.2.1 def rpki.up_down.multi_uri.__init__ (*self*, *ini*)

```
Initialize a set of URIs, which includes basic some syntax checking.
```

Definition at line 100 of file up_down.py.

11.190.2.2 def rpki.up_down.multi_uri.__str__ (*self*)

```
Convert a multi_uri back to a string representation.
```

Definition at line 115 of file up_down.py.

11.190.2.3 def rpki.up_down.multi_uri.rsync (*self*)

```
Find first rsync://... URI in self.
```

Definition at line 119 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

11.191 rpki.up_down.revoke_pdu Class Reference

Inherits rpki::up_down::revoke_syntax.

Inherited by rootd.revoke_pdu.

Collaboration diagram for rpki.up_down.revoke_pdu:

Public Member Functions

- def get_SKI
- def query
- def serve_pdu

Public Attributes

- class_name
- ski

11.191.1 Detailed Description

```
Up-Down protocol "revoke" PDU.
```

Definition at line 458 of file up_down.py.

11.191.2 Member Function Documentation

11.191.2.1 def rpki.up_down.revoke_pdu.get_SKI (*self*)

```
Convert g(SKI) encoding from PDU back to raw SKI.
```

Definition at line 463 of file up_down.py.

11.191.2.2 def rpki.up_down.revoke_pdu.query (*cls*, *ca*, *gski*, *cb*, *eb*)

```
Send a "revoke" request for certificate(s) named by gski to parent associated with ca.
```

Definition at line 487 of file up_down.py.

11.191.2.3 def rpki.up_down.revoke_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*, *cb*, *eb*)

```
Serve one revoke request PDU.
```

Reimplemented from rpki.up_down.base_elt.

Reimplemented in rootd.revoke_pdu.

Definition at line 467 of file up_down.py.

11.191.3 Member Data Documentation

11.191.3.1 rpki.up_down.revoke_pdu.class_name

Reimplemented from rpki.up_down.revoke_syntax.

Definition at line 493 of file up_down.py.

11.191.3.2 rpki.up_down.revoke_pdu.ski

Reimplemented from rpki.up_down.revoke_syntax.

Definition at line 494 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

11.192 rpki.up_down.revoke_response_pdu Class Reference

Inherits rpki::up_down::revoke_syntax.

Collaboration diagram for rpki.up_down.revoke_response_pdu:

11.192.1 Detailed Description

```
Up-Down protocol "revoke_response" PDU.
```

Definition at line 498 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

11.193 rpki.up_down.revoke_syntax Class Reference

Inherits rpki::up_down::base_elt.

Inherited by rpki.up_down.revoke_pdu, and rpki.up_down.revoke_response_pdu.

Collaboration diagram for rpki.up_down.revoke_syntax:

Public Member Functions

- def startElement
- def toXML

Public Attributes

- class_name
- ski

11.193.1 Detailed Description

```
Syntax for Up-Down protocol "revoke" and "revoke_response" PDUs.
```

Definition at line 444 of file up_down.py.

11.193.2 Member Function Documentation

11.193.2.1 def rpki.up_down.revoke_syntax.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle "revoke" PDU.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 449 of file up_down.py.

11.193.2.2 def rpki.up_down.revoke_syntax.toXML (*self*)

```
Generate payload of "revoke" PDU.
```

Definition at line 454 of file up_down.py.

11.193.3 Member Data Documentation

11.193.3.1 rpki.up_down.revoke_syntax.class_name

Reimplemented in rpki.up_down.revoke_pdu.

Definition at line 451 of file up_down.py.

11.193.3.2 rpki.up_down.revoke_syntax.ski

Reimplemented in rpki.up_down.revoke_pdu.

Definition at line 452 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

11.194 rpki.up_down.sax_handler Class Reference

Inherits rpki::xml_utils::sax_handler.

Inherited by rootd.sax_handler.

Collaboration diagram for rpki.up_down.sax_handler:

Static Public Attributes

- string name = "message"
- pdu = message_pdu
- string version = "1"

11.194.1 Detailed Description

```
SAX handler for Up-Down protocol.
```

Definition at line 676 of file up_down.py.

11.194.2 Member Data Documentation

11.194.2.1 string rpki.up_down.sax_handler.name = "message" [static]

Definition at line 682 of file up_down.py.

11.194.2.2 rpki.up_down.sax_handler.pdu = message_pdu [static]

Reimplemented in rootd.sax_handler.

Definition at line 681 of file up_down.py.

11.194.2.3 string rpki.up_down.sax_handler.version = "1" [static]

Definition at line 683 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

11.195 rpki.x509.CMS_object Class Reference

Inherits rpki::x509::DER_object.

Inherited by rpki.x509.DER_CMS_object, and rpki.x509.XML_CMS_object.

Collaboration diagram for rpki.x509.CMS_object:

Public Member Functions

- def extract
- def get_content
- def get_DER
- def get_POW
- def set_content

- def sign
- def verify

Public Attributes

- content
- DER

  DER value of this object.

- POW

Static Public Attributes

- debug_cms_certs = False

  Set this to True to log a lot of chatter about CMS certificates.

- dump_on_verify_failure = True

  Set this to True to get dumpasn1 dumps of ASN.1 on CMS verify failures.

- tuple econtent_oid = POWify_OID("id-data")
- tuple formats = ("DER", "POW")

  Formats supported in this object.

- tuple other_clear = ("content",)

  Other attributes that self.clear() should whack.

- tuple pem_converter = PEM_converter("CMS")

  PEM converter for this object.

- print_on_der_error = True

  Set this to True to log alleged DER when we have trouble parsing it, in case it's really a Perl backtrace or something.

- require_crls = False

  Set this to False to make CMS CRLs optional in the cases where we would otherwise require them.

11.195.1 Detailed Description

```
Class to hold a CMS-wrapped object.

CMS-wrapped objects are a little different from the other DER_object
types because the signed object is CMS wrapping inner content that's
also ASN.1, and due to our current minimal support for CMS we can't
just handle this as a pretty composite object.  So, for now anyway,
a CMS_object is the outer CMS wrapped object so that the usual DER
and PEM operations do the obvious things, and the inner content is
handle via separate methods.
```

Definition at line 735 of file x509.py.

11.195.2 Member Function Documentation

11.195.2.1 def rpki.x509.CMS_object.extract (*self*)

```
Extract and store inner content from CMS wrapper without verifying
the CMS.

DANGER WILL ROBINSON!!!

Do not use this method on unvalidated data.  Use the verify()
method instead.

If you don't understand this warning, don't use this method.
```

Definition at line 886 of file x509.py.

11.195.2.2 def rpki.x509.CMS_object.get_content (*self*)

```
Get the inner content of this CMS_object.
```

Definition at line 797 of file x509.py.

11.195.2.3 def rpki.x509.CMS_object.get_DER (*self*)

```
Get the DER value of this CMS_object.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 776 of file x509.py.

11.195.2.4 def rpki.x509.CMS_object.get_POW (*self*)

```
Get the POW value of this CMS_object.
```

Definition at line 788 of file x509.py.

11.195.2.5 def rpki.x509.CMS_object.set_content (*self*, *content*)

```
Set the (inner) content of this CMS_object, clearing the wrapper.
```

Definition at line 805 of file x509.py.

11.195.2.6 def rpki.x509.CMS_object.sign (*self*, *keypair*, *certs*, *crls* = **None**, *no_certs* = **False**)

```
Sign and wrap inner content.
```

Definition at line 914 of file x509.py.

11.195.2.7 def rpki.x509.CMS_object.verify (*self*, *ta*)

```
Verify CMS wrapper and store inner content.
```

Definition at line 812 of file x509.py.

11.195.3 Member Data Documentation

11.195.3.1 rpki.x509.CMS_object.content

Reimplemented in rpki.x509.DER_CMS_object, and rpki.x509.XML_CMS_object.

Definition at line 810 of file x509.py.

11.195.3.2 rpki::x509.CMS_object::debug_cms_certs = False [static]

Set this to True to log a lot of chatter about CMS certificates.

Definition at line 761 of file x509.py.

11.195.3.3 rpki.x509.CMS_object.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 784 of file x509.py.

11.195.3.4 rpki::x509.CMS_object::dump_on_verify_failure = True [static]

Set this to True to get dumpasn1 dumps of ASN.1 on CMS verify failures.

Definition at line 756 of file x509.py.

11.195.3.5 tuple rpki.x509.CMS_object.econtent_oid = POWify_OID("id-data") [static]

Reimplemented in rpki.x509.SignedManifest, rpki.x509.ROA, and rpki.x509.XML_-CMS_object.

Definition at line 750 of file x509.py.

11.195.3.6 tuple rpki.x509.CMS_object.formats = ("DER", "POW") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 748 of file x509.py.

11.195.3.7 tuple rpki.x509.CMS_object.other_clear = ("content",) [static]

Other attributes that self.clear() should whack.

Reimplemented from rpki.x509.DER_object.

Definition at line 749 of file x509.py.

11.195.3.8 tuple rpki.x509.CMS_object.pem_converter = PEM_converter("CMS") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Reimplemented in rpki.x509.SignedManifest, and rpki.x509.ROA.

Definition at line 751 of file x509.py.

11.195.3.9 rpki.x509.CMS_object.POW

Definition at line 794 of file x509.py.

11.195.3.10 rpki::x509.CMS_object::print_on_der_error = True [static]

Set this to True to log alleged DER when we have trouble parsing it, in case it's really a Perl backtrace or something.

Definition at line 774 of file x509.py.

11.195.3.11 rpki::x509.CMS_object::require_crls = False [static]

Set this to False to make CMS CRLs optional in the cases where we would otherwise require them.

Some day this option should go away and CRLs should be uncondtionally mandatory in such cases.

Definition at line 768 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

11.196 rpki.x509.CRL Class Reference

Inherits rpki::x509::DER_object.

Collaboration diagram for rpki.x509.CRL:

Public Member Functions

- def generate
- def get_DER
- def get_POW
- def get_POWpkix
- def getIssuer
- def getNextUpdate
- def getThisUpdate

Public Attributes

- DER

  DER value of this object.

- POW
- POWpkix

Static Public Attributes

- tuple formats = ("DER", "POW", "POWpkix")

  Formats supported in this object.

- tuple pem_converter = PEM_converter("X509 CRL")

  PEM converter for this object.

11.196.1 Detailed Description

```
Class to hold a Certificate Revocation List.
```

Definition at line 1140 of file x509.py.

11.196.2 Member Function Documentation

11.196.2.1 def rpki.x509.CRL.generate (*cls*, *keypair*, *issuer*, *serial*, *thisUpdate*, *nextUpdate*, *revokedCertificates*, *version* = 1, *digestType* = "sha256WithRSAEncryption")

```
Generate a new CRL.
```

Definition at line 1196 of file x509.py.

11.196.2.2 def rpki.x509.CRL.get_DER (*self*)

```
Get the DER value of this CRL.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 1148 of file x509.py.

11.196.2.3 def rpki.x509.CRL.get_POW (*self*)

```
Get the POW value of this CRL.
```

Definition at line 1163 of file x509.py.

11.196.2.4 def rpki.x509.CRL.get_POWpkix (*self*)

```
Get the POW.pkix value of this CRL.
```

Definition at line 1172 of file x509.py.

11.196.2.5 def rpki.x509.CRL.getIssuer (*self*)

```
Get issuer value of this CRL.
```

Definition at line 1191 of file x509.py.

11.196.2.6 def rpki.x509.CRL.getNextUpdate (*self*)

```
Get nextUpdate value from this CRL.
```

Definition at line 1187 of file x509.py.

11.196.2.7 def rpki.x509.CRL.getThisUpdate (*self*)

```
Get thisUpdate value from this CRL.
```

Definition at line 1183 of file x509.py.

11.196.3 Member Data Documentation

11.196.3.1 rpki.x509.CRL.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 1156 of file x509.py.

11.196.3.2 tuple rpki.x509.CRL.formats = ("DER", "POW", "POWpkix") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 1145 of file x509.py.

11.196.3.3 tuple rpki.x509.CRL.pem_converter = PEM_converter("X509 CRL") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 1146 of file x509.py.

11.196.3.4 rpki.x509.CRL.POW

Definition at line 1169 of file x509.py.

11.196.3.5 rpki.x509.CRL.POWpkix

Definition at line 1180 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

11.197 rpki.x509.DeadDrop Class Reference

Inherits object.

Collaboration diagram for rpki.x509.DeadDrop:

Public Member Functions

- def __init__
- def dump

Public Attributes

- maildir
- pid

11.197.1 Detailed Description

```
Dead-drop utility for storing copies of CMS messages for debugging or
audit.  At the moment this uses Maildir mailbox format, as it has
approximately the right properties and a number of useful tools for
manipulating it already exist.
```

Definition at line 1035 of file x509.py.

11.197.2 Member Function Documentation

11.197.2.1 def rpki.x509.DeadDrop.__init__ (*self*, *name*)

Definition at line 1043 of file x509.py.

11.197.2.2 def rpki.x509.DeadDrop.dump (*self*, *obj*)

Definition at line 1047 of file x509.py.

11.197.3 Member Data Documentation

11.197.3.1 rpki.x509.DeadDrop.maildir

Definition at line 1044 of file x509.py.

11.197.3.2 rpki.x509.DeadDrop.pid

Definition at line 1045 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

11.198 rpki.x509.DER_CMS_object Class Reference

Inherits rpki::x509::CMS_object.

Inherited by rpki.x509.ROA, and rpki.x509.SignedManifest.

Collaboration diagram for rpki.x509.DER_CMS_object:

Public Member Functions

- def decode

- def encode

Public Attributes

- content

11.198.1 Detailed Description

```
Class to hold CMS objects with DER-based content.
```

Definition at line 950 of file x509.py.

11.198.2 Member Function Documentation

11.198.2.1 def rpki.x509.DER_CMS_object.decode (*self*, *der*)

```
Decode DER and set inner content.
```

Definition at line 959 of file x509.py.

11.198.2.2 def rpki.x509.DER_CMS_object.encode (*self*)

```
Encode inner content for signing.
```

Definition at line 955 of file x509.py.

11.198.3 Member Data Documentation

11.198.3.1 rpki.x509.DER_CMS_object.content

Reimplemented from rpki.x509.CMS_object.

Definition at line 965 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

11.199 rpki.x509.DER_object Class Reference

Inherits object.

Inherited by rpki.x509.CMS_object, rpki.x509.CRL, rpki.x509.PKCS10, rpki.x509.RSA, rpki.x509.RSApublic, and rpki.x509.X509.

Collaboration diagram for rpki.x509.DER_object:

Public Member Functions

- def __cmp__
- def __init__
- def clear
- def dumpasn1
- def empty
- def from_sql
- def gAKI
- def get_3779resources
- def get_AIA
- def get_aia_uri
- def get_AKI
- def get_Base64
- def get_basicConstraints
- def get_DER
- def get_PEM
- def get_SIA
- def get_sia_directory_uri
- def get_sia_manifest_uri
- def get_SKI
- def gSKI
- def hAKI
- def hSKI
- def is_CA
- def set
- def to_sql

Public Attributes

- DER

  DER value of this object.

Static Public Attributes

- tuple formats = ("DER",)

  Formats supported in this object.

- tuple other_clear = ()

  Other attributes that self.clear() should whack.

- pem_converter = None

  PEM converter for this object.

11.199.1 Detailed Description

```
Virtual class to hold a generic DER object.
```

Definition at line 117 of file x509.py.

11.199.2 Member Function Documentation

11.199.2.1 def rpki.x509.DER_object.__cmp__ (*self*, *other*)

```
Compare two DER-encoded objects.
```

Definition at line 212 of file x509.py.

11.199.2.2 def rpki.x509.DER_object.__init__ (*self*, *kw*)

```
Initialize a DER_object.
```

Definition at line 150 of file x509.py.

11.199.2.3 def rpki.x509.DER_object.clear (*self*)

```
Make this object empty.
```

Definition at line 143 of file x509.py.

11.199.2.4 def rpki.x509.DER_object.dumpasn1 (*self*)

```
Pretty print an ASN.1 DER object using cryptlib dumpasn1 tool.
Use a temporary file rather than popen4() because dumpasn1 uses
seek() when decoding ASN.1 content nested in OCTET STRING values.
```

Definition at line 341 of file x509.py.

11.199.2.5 def rpki.x509.DER_object.empty (*self*)

```
Test whether this object is empty.
```

Definition at line 134 of file x509.py.

11.199.2.6 def rpki.x509.DER_object.from_sql (*cls*, *x*)

```
Convert from SQL storage format.
```

Definition at line 333 of file x509.py.

11.199.2.7 def rpki.x509.DER_object.gAKI (*self*)

```
Calculate g(AKI) for this object.  Only work for subclasses
that implement get_AKI().
```

Definition at line 248 of file x509.py.

11.199.2.8 def rpki.x509.DER_object.get_3779resources (*self*)

```
Get RFC 3779 resources as rpki.resource_set objects.  Only works
for subclasses that support getExtensions().
```

Definition at line 320 of file x509.py.

11.199.2.9 def rpki.x509.DER_object.get_AIA (*self*)

```
Get the SIA extension from this object.  Only works for subclasses
that support getExtension().
```

Definition at line 291 of file x509.py.

11.199.2.10 def rpki.x509.DER_object.get_aia_uri (*self*)

```
Get AIA (id-ad-caIssuers) URI from this object.
Only works for subclasses that support getExtension().
```

Definition at line 298 of file x509.py.

11.199.2.11 def rpki.x509.DER_object.get_AKI (*self*)

```
Get the AKI extension from this object.  Only works for subclasses
that support getExtension().
```

Definition at line 255 of file x509.py.

11.199.2.12 def rpki.x509.DER_object.get_Base64 (*self*)

```
Get the Base64 encoding of the DER value of this object.
```

Definition at line 204 of file x509.py.

11.199.2.13 def rpki.x509.DER_object.get_basicConstraints (*self*)

```
Get the basicConstraints extension from this object.  Only works
for subclasses that support getExtension().
```

Definition at line 305 of file x509.py.

11.199.2.14 def rpki.x509.DER_object.get_DER (*self*)

```
Get the DER value of this object.

Subclasses will almost certainly override this method.
```

Reimplemented in rpki.x509.X509, rpki.x509.PKCS10, rpki.x509.RSA, rpki.x509.RSApublic, rpki.x509.CMS_object, and rpki.x509.CRL.

Definition at line 193 of file x509.py.

11.199.2.15 def rpki.x509.DER_object.get_PEM (*self*)

```
Get the PEM representation of this object.
```

Definition at line 208 of file x509.py.

11.199.2.16 def rpki.x509.DER_object.get_SIA (*self*)

```
Get the SIA extension from this object.  Only works for subclasses
that support getExtension().
```

Definition at line 270 of file x509.py.

11.199.2.17 def rpki.x509.DER_object.get_sia_directory_uri (*self*)

```
Get SIA directory (id-ad-caRepository) URI from this object.
Only works for subclasses that support getExtension().
```

Definition at line 277 of file x509.py.

11.199.2.18 def rpki.x509.DER_object.get_sia_manifest_uri (*self*)

```
Get SIA manifest (id-ad-rpkiManifest) URI from this object.
Only works for subclasses that support getExtension().
```

Definition at line 284 of file x509.py.

11.199.2.19 def rpki.x509.DER_object.get_SKI (*self*)

```
Get the SKI extension from this object.  Only works for subclasses
that support getExtension().
```

Reimplemented in rpki.x509.RSA, and rpki.x509.RSApublic.

Definition at line 263 of file x509.py.

11.199.2.20 def rpki.x509.DER_object.gSKI (*self*)

```
Calculate g(SKI) for this object.  Only work for subclasses
that implement get_SKI().
```

Definition at line 233 of file x509.py.

11.199.2.21 def rpki.x509.DER_object.hAKI (*self*)

```
Return hexadecimal string representation of AKI for this
object.  Only work for subclasses that implement get_AKI().
```

Definition at line 240 of file x509.py.

11.199.2.22 def rpki.x509.DER_object.hSKI (*self*)

```
Return hexadecimal string representation of SKI for this object.
Only work for subclasses that implement get_SKI().
```

Definition at line 225 of file x509.py.

11.199.2.23 def rpki.x509.DER_object.is_CA (*self*)

```
Return True if and only if object has the basicConstraints
extension and its cA value is true.
```

Definition at line 312 of file x509.py.

11.199.2.24 def rpki.x509.DER_object.set (*self*, *kw*)

```
Set this object by setting one of its known formats.

This method only allows one to set one format at a time.
Subsequent calls will clear the object first.  The point of all
this is to let the object's internal converters handle mustering
the object into whatever format you need at the moment.
```

Definition at line 158 of file x509.py.

11.199.2.25 def rpki.x509.DER_object.to_sql (*self*)

```
Convert to SQL storage format.
```

Definition at line 337 of file x509.py.

11.199.3 Member Data Documentation

11.199.3.1 rpki::x509.DER_object::DER

DER value of this object.

Reimplemented in rpki.x509.X509, rpki.x509.PKCS10, rpki.x509.RSA, rpki.x509.RSApublic, rpki.x509.CMS_object, and rpki.x509.CRL.

Definition at line 176 of file x509.py.

11.199.3.2 tuple rpki.x509.DER_object.formats = ("DER",) `[static]`

Formats supported in this object.

Reimplemented in rpki.x509.X509, rpki.x509.PKCS10, rpki.x509.RSA, rpki.x509.RSApublic, rpki.x509.CMS_object, and rpki.x509.CRL.

Definition at line 123 of file x509.py.

11.199.3.3 tuple rpki.x509.DER_object.other_clear = () `[static]`

Other attributes that self.clear() should whack.

Reimplemented in rpki.x509.CMS_object.

Definition at line 129 of file x509.py.

11.199.3.4 rpki.x509.DER_object.pem_converter = None `[static]`

PEM converter for this object.

Reimplemented in rpki.x509.X509, rpki.x509.PKCS10, rpki.x509.RSA, rpki.x509.RSApublic, rpki.x509.CMS_object, rpki.x509.SignedManifest, rpki.x509.ROA, and rpki.x509.CRL.

Definition at line 126 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

11.200 rpki.x509.PEM_converter Class Reference

Inherits object.

Collaboration diagram for rpki.x509.PEM_converter:

Public Member Functions

- def __init__
- def looks_like_PEM
- def to_DER

- def to_PEM

Public Attributes

- b
- e

11.200.1 Detailed Description

```
Convert between DER and PEM encodings for various kinds of ASN.1 data.
```

Definition at line 62 of file x509.py.

11.200.2 Member Function Documentation

11.200.2.1 def rpki.x509.PEM_converter.__init__ (*self*, *kind*)

```
Initialize PEM_converter.
```

Definition at line 67 of file x509.py.

11.200.2.2 def rpki.x509.PEM_converter.looks_like_PEM (*self*, *text*)

```
Guess whether text looks like a PEM encoding.
```

Definition at line 74 of file x509.py.

11.200.2.3 def rpki.x509.PEM_converter.to_DER (*self*, *pem*)

```
Convert from PEM to DER.
```

Definition at line 81 of file x509.py.

11.200.2.4 def rpki.x509.PEM_converter.to_PEM (*self*, *der*)

```
Convert from DER to PEM.
```

Definition at line 94 of file x509.py.

11.200.3 Member Data Documentation

11.200.3.1 rpki.x509.PEM_converter.b

Definition at line 71 of file x509.py.

11.200.3.2 rpki.x509.PEM_converter.e

Definition at line 72 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

11.201 rpki.x509.PKCS10 Class Reference

Inherits rpki::x509::DER_object.

Collaboration diagram for rpki.x509.PKCS10:

Public Member Functions

- def check_valid_rpki
- def create
- def create_ca
- def get_DER
- def get_POWpkix
- def getPublicKey

Public Attributes

- DER

  DER value of this object.

- POWpkix

Static Public Attributes

- tuple formats = ("DER", "POWpkix")

  Formats supported in this object.

- tuple pem_converter = PEM_converter("CERTIFICATE REQUEST")

  PEM converter for this object.

11.201.1 Detailed Description

```
Class to hold a PKCS #10 request.
```

Definition at line 534 of file x509.py.

11.201.2 Member Function Documentation

11.201.2.1 def rpki.x509.PKCS10.check_valid_rpki (*self*)

```
Check this certification request to see whether it's a valid
request for an RPKI certificate.  This is broken out of the
up-down protocol code because it's somewhat involved and the
up-down code doesn't need to know the details.

Throws an exception if the request isn't valid, so if this method
returns at all, the request is ok.
```

Definition at line 569 of file x509.py.

11.201.2.2 def rpki.x509.PKCS10.create (*cls*, *keypair*, *exts* = `None`)

```
Create a new request for a given keypair, including given extensions.
```

Definition at line 629 of file x509.py.

11.201.2.3 def rpki.x509.PKCS10.create_ca (*cls*, *keypair*, *sia* = `None`)

```
Create a new request for a given keypair, including given SIA value.
```

Definition at line 616 of file x509.py.

11.201.2.4 def rpki.x509.PKCS10.get_DER (*self*)

```
Get the DER value of this certification request.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 542 of file x509.py.

11.201.2.5 def rpki.x509.PKCS10.get_POWpkix (*self*)

```
Get the POW.pkix value of this certification request.
```

Definition at line 554 of file x509.py.

11.201.2.6 def rpki.x509.PKCS10.getPublicKey (*self*)

```
Extract the public key from this certification request.
```

Definition at line 565 of file x509.py.

11.201.3 Member Data Documentation

11.201.3.1 rpki.x509.PKCS10.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 550 of file x509.py.

11.201.3.2 tuple rpki.x509.PKCS10.formats = ("DER", "POWpkix") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 539 of file x509.py.

11.201.3.3 tuple rpki.x509.PKCS10.pem_converter = PEM_converter("CERTIFICATE REQUEST") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 540 of file x509.py.

11.201.3.4 rpki.x509.PKCS10.POWpkix

Definition at line 562 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

11.202 rpki.x509.ROA Class Reference

Inherits rpki::x509::DER_CMS_object.

Collaboration diagram for rpki.x509.ROA:

Public Member Functions

- def build

Static Public Attributes

- content_class = rpki.roa.RouteOriginAttestation

- tuple econtent_oid = POWify_OID("id-ct-routeOriginAttestation")
- tuple pem_converter = PEM_converter("ROUTE ORIGIN ATTESTATION")

  PEM converter for this object.

11.202.1 Detailed Description

```
Class to hold a signed ROA.
```

Definition at line 1007 of file x509.py.

11.202.2 Member Function Documentation

11.202.2.1 def rpki.x509.ROA.build (*cls*, *asn*, *ipv4*, *ipv6*, *keypair*, *certs*, *version* = 0)

```
Build a ROA.
```

Definition at line 1017 of file x509.py.

11.202.3 Member Data Documentation

11.202.3.1 rpki.x509.ROA.content_class = rpki.roa.RouteOriginAttestation [static]

Definition at line 1013 of file x509.py.

11.202.3.2 tuple rpki.x509.ROA.econtent_oid = POWify_OID("id-ct-routeOriginAttestation") [static]

Reimplemented from rpki.x509.CMS_object.

Definition at line 1014 of file x509.py.

11.202.3.3 tuple rpki.x509.ROA.pem_converter = PEM_converter("ROUTE ORIGIN ATTESTATION") [static]

PEM converter for this object.

Reimplemented from rpki.x509.CMS_object.

Definition at line 1012 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

11.203 rpki.x509.RSA Class Reference

Inherits rpki::x509::DER_object.

Collaboration diagram for rpki.x509.RSA:

Public Member Functions

- def generate
- def get_DER
- def get_POW
- def get_public_DER
- def get_RSApublic
- def get_SKI

Public Attributes

- DER

  DER value of this object.

- POW

Static Public Attributes

- tuple formats = ("DER", "POW")

  Formats supported in this object.

- tuple pem_converter = PEM_converter("RSA PRIVATE KEY")

  PEM converter for this object.

11.203.1 Detailed Description

```
Class to hold an RSA key pair.
```

Definition at line 643 of file x509.py.

11.203.2 Member Function Documentation

11.203.2.1 def rpki.x509.RSA.generate (*cls*, *keylength* = 2048)

```
Generate a new keypair.
```

Definition at line 673 of file x509.py.

11.203.2.2 def rpki.x509.RSA.get_DER (*self*)

```
Get the DER value of this keypair.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 651 of file x509.py.

11.203.2.3 def rpki.x509.RSA.get_POW (*self*)

```
Get the POW value of this keypair.
```

Definition at line 663 of file x509.py.

11.203.2.4 def rpki.x509.RSA.get_public_DER (*self*)

```
Get the DER encoding of the public key from this keypair.
```

Definition at line 680 of file x509.py.

11.203.2.5 def rpki.x509.RSA.get_RSApublic (*self*)

```
Convert the public key of this keypair into a RSApublic object.
```

Definition at line 688 of file x509.py.

11.203.2.6 def rpki.x509.RSA.get_SKI (*self*)

```
Calculate the SKI of this keypair.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 684 of file x509.py.

11.203.3 Member Data Documentation

11.203.3.1 rpki.x509.RSA.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 659 of file x509.py.

11.203.3.2 tuple rpki.x509.RSA.formats = ("DER", "POW") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 648 of file x509.py.

11.203.3.3 tuple rpki.x509.RSA.pem_converter = PEM_converter("RSA PRIVATE KEY") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 649 of file x509.py.

11.203.3.4 rpki.x509.RSA.POW

Definition at line 669 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

11.204 rpki.x509.RSApublic Class Reference

Inherits rpki::x509::DER_object.

Collaboration diagram for rpki.x509.RSApublic:

Public Member Functions

- def get_DER
- def get_POW
- def get_SKI

Public Attributes

- DER

  DER value of this object.

- POW

Static Public Attributes

- tuple formats = ("DER", "POW")

  Formats supported in this object.

- tuple pem_converter = PEM_converter("RSA PUBLIC KEY")

  PEM converter for this object.

11.204.1 Detailed Description

```
Class to hold an RSA public key.
```

Definition at line 692 of file x509.py.

11.204.2 Member Function Documentation

11.204.2.1 def rpki.x509.RSApublic.get_DER (*self*)

```
Get the DER value of this public key.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 700 of file x509.py.

11.204.2.2 def rpki.x509.RSApublic.get_POW (*self*)

```
Get the POW value of this public key.
```

Definition at line 712 of file x509.py.

11.204.2.3 def rpki.x509.RSApublic.get_SKI (*self*)

```
Calculate the SKI of this public key.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 721 of file x509.py.

11.204.3 Member Data Documentation

11.204.3.1 rpki.x509.RSApublic.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 708 of file x509.py.

11.204.3.2 tuple rpki.x509.RSApublic.formats = ("DER", "POW") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 697 of file x509.py.

11.204.3.3 tuple rpki.x509.RSApublic.pem_converter = PEM_converter("RSA PUBLIC KEY") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 698 of file x509.py.

11.204.3.4 rpki.x509.RSApublic.POW

Definition at line 718 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

11.205 rpki.x509.SignedManifest Class Reference

Inherits rpki::x509::DER_CMS_object.

Collaboration diagram for rpki.x509.SignedManifest:

Public Member Functions

- def build
- def getNextUpdate
- def getThisUpdate

Static Public Attributes

- content_class = rpki.manifest.Manifest
- tuple econtent_oid = POWify_OID("id-ct-rpkiManifest")
- tuple pem_converter = PEM_converter("RPKI MANIFEST")

  PEM converter for this object.

11.205.1 Detailed Description

```
Class to hold a signed manifest.
```

Definition at line 967 of file x509.py.

11.205.2 Member Function Documentation

11.205.2.1 def rpki.x509.SignedManifest.build (*cls*, *serial*, *thisUpdate*, *nextUpdate*, *names_and_objs*, *keypair*, *certs*, *version* = 0)

```
Build a signed manifest.
```

Definition at line 985 of file x509.py.

11.205.2.2 def rpki.x509.SignedManifest.getNextUpdate (*self*)

```
Get nextUpdate value from this manifest.
```

Definition at line 980 of file x509.py.

11.205.2.3 def rpki.x509.SignedManifest.getThisUpdate (*self*)

```
Get thisUpdate value from this manifest.
```

Definition at line 976 of file x509.py.

11.205.3 Member Data Documentation

11.205.3.1 rpki.x509.SignedManifest.content_class = rpki.manifest.Manifest [static]

Definition at line 973 of file x509.py.

11.205.3.2 tuple rpki.x509.SignedManifest.econtent_oid = POWify_OID("id-ct-rpkiManifest") [static]

Reimplemented from rpki.x509.CMS_object.

Definition at line 974 of file x509.py.

11.205.3.3 tuple rpki.x509.SignedManifest.pem_converter = PEM_converter("RPKI MANIFEST") [static]

PEM converter for this object.

Reimplemented from rpki.x509.CMS_object.

Definition at line 972 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

11.206 rpki.x509.X509 Class Reference

Inherits rpki::x509::DER_object.

Collaboration diagram for rpki.x509.X509:

Public Member Functions

- def cross_certify
- def expired
- def get_DER
- def get_POW
- def get_POWpkix

- def getIssuer
- def getNotAfter
- def getNotBefore
- def getPublicKey
- def getSerial
- def getSubject
- def issue
- def normalize_chain

Public Attributes

- DER

  DER value of this object.

- POW
- POWpkix

Static Public Attributes

- tuple formats = ("DER", "POW", "POWpkix")

  Formats supported in this object.

- tuple pem_converter = PEM_converter("CERTIFICATE")

  PEM converter for this object.

11.206.1 Detailed Description

```
X.509 certificates.

This class is designed to hold all the different representations of
X.509 certs we're using and convert between them.  X.509 support in
Python a nasty maze of half-cooked stuff (except perhaps for
cryptlib, which is just different).  Users of this module should not
have to care about this implementation nightmare.
```

Definition at line 360 of file x509.py.

11.206.2 Member Function Documentation

11.206.2.1 def rpki.x509.X509.cross_certify (*self*, *keypair*, *source_cert*, *serial*, *notAfter*, *now* = `None`, *pathLenConstraint* = `0`)

```
Issue a certificate with values taking from an existing certificate.
This is used to construct some kinds oF BPKI certificates.
```

Definition at line 492 of file x509.py.

11.206.2.2 def rpki.x509.X509.expired (*self*)

```
Test whether this certificate has expired.
```

Definition at line 433 of file x509.py.

11.206.2.3 def rpki.x509.X509.get_DER (*self*)

```
Get the DER value of this certificate.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 374 of file x509.py.

11.206.2.4 def rpki.x509.X509.get_POW (*self*)

```
Get the POW value of this certificate.
```

Definition at line 389 of file x509.py.

11.206.2.5 def rpki.x509.X509.get_POWpkix (*self*)

```
Get the POW.pkix value of this certificate.
```

Definition at line 398 of file x509.py.

11.206.2.6 def rpki.x509.X509.getIssuer (*self*)

```
Get the issuer of this certificate.
```

Definition at line 409 of file x509.py.

11.206.2.7 def rpki.x509.X509.getNotAfter (*self*)

```
Get the expiration time of this certificate.
```

Definition at line 421 of file x509.py.

11.206.2.8 def rpki.x509.X509.getNotBefore (*self*)

```
Get the inception time of this certificate.
```

Definition at line 417 of file x509.py.

11.206.2.9 def rpki.x509.X509.getPublicKey (*self*)

```
Extract the public key from this certificate.
```

Definition at line 429 of file x509.py.

11.206.2.10 def rpki.x509.X509.getSerial (*self*)

```
Get the serial number of this certificate.
```

Definition at line 425 of file x509.py.

11.206.2.11 def rpki.x509.X509.getSubject (*self*)

```
Get the subject of this certificate.
```

Definition at line 413 of file x509.py.

11.206.2.12 def rpki.x509.X509.issue (*self*, *keypair*, *subject_key*, *serial*, *sia*, *aia*, *crldp*, *notAfter*, *cn* = `None`, *resources* = `None`, *is_ca* = `True`)

```
Issue a certificate.
```

Definition at line 437 of file x509.py.

11.206.2.13 def rpki.x509.X509.normalize_chain (*cls*, *chain*)

```
Normalize a chain of certificates into a tuple of X509 objects.
Given all the glue certificates needed for BPKI cross
certification, it's easiest to allow sloppy arguments to the HTTPS
and CMS validation methods and provide a single method that
normalizes the allowed cases.  So this method allows X509, None,
lists, and tuples, and returns a tuple of X509 objects.
```

Definition at line 521 of file x509.py.

11.206.3 Member Data Documentation

11.206.3.1 rpki.x509.X509.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 382 of file x509.py.

11.206.3.2 tuple rpki.x509.X509.formats = ("DER", "POW", "POWpkix") `[static]`

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 371 of file x509.py.

11.206.3.3 tuple rpki.x509.X509.pem_converter = PEM_converter("CERTIFICATE") `[static]`

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 372 of file x509.py.

11.206.3.4 rpki.x509.X509.POW

Definition at line 395 of file x509.py.

11.206.3.5 rpki.x509.X509.POWpkix

Definition at line 406 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

11.207 rpki.x509.XML_CMS_object Class Reference

Inherits rpki::x509::CMS_object.

Inherited by rpki.left_right.cms_msg, rpki.publication.cms_msg, and rpki.up_-down.cms_msg.

Collaboration diagram for rpki.x509.XML_CMS_object:

Public Member Functions

- def decode
- def dump_to_disk
- def encode
- def pretty_print_content
- def schema_check

- def unwrap
- def wrap

Public Attributes

- content

Static Public Attributes

- dump_inbound_cms = None

  If set, we write all inbound XML-CMS PDUs to disk, for debugging.

- dump_outbound_cms = None

  If set, we write all outbound XML-CMS PDUs to disk, for debugging.

- tuple econtent_oid = POWify_OID("id-ct-xml")

11.207.1 Detailed Description

```
Class to hold CMS-wrapped XML protocol data.
```

Definition at line 1058 of file x509.py.

11.207.2 Member Function Documentation

11.207.2.1 def rpki.x509.XML_CMS_object.decode (*self*, *xml*)

```
Decode XML and set inner content.
```

Definition at line 1081 of file x509.py.

11.207.2.2 def rpki.x509.XML_CMS_object.dump_to_disk (*self*, *prefix*)

```
Write DER of current message to disk, for debugging.
```

Definition at line 1099 of file x509.py.

11.207.2.3 def rpki.x509.XML_CMS_object.encode (*self*)

```
Encode inner content for signing.
```

Definition at line 1077 of file x509.py.

11.207.2.4 def rpki.x509.XML_CMS_object.pretty_print_content (*self*)

```
Pretty print XML content of this message.
```

Definition at line 1085 of file x509.py.

11.207.2.5 def rpki.x509.XML_CMS_object.schema_check (*self*)

```
Handle XML RelaxNG schema check.
```

Definition at line 1089 of file x509.py.

11.207.2.6 def rpki.x509.XML_CMS_object.unwrap (*cls*, *der*, *ta*, *pretty_print* = `False`)

```
Unwrap a CMS-wrapped XML PDU and return Python objects.
```

Definition at line 1125 of file x509.py.

11.207.2.7 def rpki.x509.XML_CMS_object.wrap (*cls*, *msg*, *keypair*, *certs*, *crls* = `None`, *pretty_print* = `False`)

```
Build a CMS-wrapped XML PDU and return its DER encoding.
```

Definition at line 1108 of file x509.py.

11.207.3 Member Data Documentation

11.207.3.1 rpki.x509.XML_CMS_object.content

Reimplemented from rpki.x509.CMS_object.

Definition at line 1083 of file x509.py.

11.207.3.2 rpki::x509.XML_CMS_object::dump_inbound_cms = None [static]

If set, we write all inbound XML-CMS PDUs to disk, for debugging.

If set, value should be a DeadDrop object.

Definition at line 1075 of file x509.py.

11.207.3.3 rpki::x509.XML_CMS_object::dump_outbound_cms = None [static]

If set, we write all outbound XML-CMS PDUs to disk, for debugging.

If set, value should be a DeadDrop object.

Definition at line 1069 of file x509.py.

11.207.3.4 tuple rpki.x509.XML_CMS_object.econtent_oid = POWify_OID("id-ct-xml") [static]

Reimplemented from rpki.x509.CMS_object.

Definition at line 1063 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

11.208 rpki.xml_utils.base_elt Class Reference

Inherits object.

Inherited by rpki.left_right.list_received_resources_elt, rpki.left_right.list_resources_-elt, rpki.left_right.list_roa_requests_elt, rpki.publication.publication_object_elt, rpki.xml_utils.data_elt, and rpki.xml_utils.text_elt.

Collaboration diagram for rpki.xml_utils.base_elt:

Public Member Functions

- def __str__
- def endElement

- def make_b64elt
- def make_elt
- def make_pdu
- def read_attrs
- def startElement
- def toXML

Static Public Attributes

- tuple attributes = ()

  XML attributes for this element.

- tuple booleans = ()

  Boolean attributes (value "yes" or "no") for this element.

- tuple elements = ()

  XML elements contained by this element.

11.208.1 Detailed Description

```
Virtual base class for XML message elements.  The left-right and
publication protocols use this.  At least for now, the up-down
protocol does not, due to different design assumptions.
```

Definition at line 126 of file xml_utils.py.

11.208.2 Member Function Documentation

11.208.2.1 def rpki.xml_utils.base_elt.__str__ (*self*)

```
Convert a base_elt object to string format.
```

Reimplemented in rpki.publication.report_error_elt.

Definition at line 201 of file xml_utils.py.

11.208.2.2 def rpki.xml_utils.base_elt.endElement (*self*, *stack*, *name*, *text*)

```
Default endElement() handler: just pop the stack.
```

Reimplemented in rpki.left_right.child_elt, rpki.publication.client_elt, rpki.publication.publication_object_elt, rpki.xml_utils.text_elt, and rpki.xml_-utils.data_elt.

Definition at line 153 of file xml_utils.py.

11.208.2.3 def rpki.xml_utils.base_elt.make_b64elt (*self*, *elt*, *name*, *value* = `None`)

```
Constructor for Base64-encoded subelement.
```

Definition at line 192 of file xml_utils.py.

11.208.2.4 def rpki.xml_utils.base_elt.make_elt (*self*)

```
XML element constructor.
```

Definition at line 178 of file xml_utils.py.

11.208.2.5 def rpki.xml_utils.base_elt.make_pdu (*cls*, *kargs*)

```
Generic PDU constructor.
```

Definition at line 208 of file xml_utils.py.

11.208.2.6 def rpki.xml_utils.base_elt.read_attrs (*self*, *attrs*)

```
Template-driven attribute reader.
```

Definition at line 166 of file xml_utils.py.

11.208.2.7 def rpki.xml_utils.base_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
Default startElement() handler: just process attributes.
```

Reimplemented in rpki.left_right.list_resources_elt, rpki.left_right.list_roa_requests_-elt, and rpki.publication.config_elt.

Definition at line 145 of file xml_utils.py.

11.208.2.8 def rpki.xml_utils.base_elt.toXML (*self*)

```
Default toXML() element generator.
```

Reimplemented in rpki.left_right.list_resources_elt, rpki.publication.publication_-object_elt, rpki.xml_utils.text_elt, and rpki.xml_utils.data_elt.

Definition at line 160 of file xml_utils.py.

11.208.3 Member Data Documentation

11.208.3.1 rpki::xml_utils.base_elt::attributes = () [static]

XML attributes for this element.

Reimplemented in rpki.left_right.self_elt, rpki.left_right.bsc_elt, rpki.left_-right.repository_elt, rpki.left_right.parent_elt, rpki.left_right.child_elt, rpki.left_-right.list_resources_elt, rpki.left_right.list_roa_requests_elt, rpki.left_right.list_-published_objects_elt, rpki.left_right.list_received_resources_elt, rpki.left_-right.report_error_elt, rpki.publication.config_elt, rpki.publication.client_elt, rpki.publication.publication_object_elt, and rpki.publication.report_error_elt.

Definition at line 135 of file xml_utils.py.

11.208.3.2 rpki::xml_utils.base_elt::booleans = () [static]

Boolean attributes (value "yes" or "no") for this element.

Reimplemented in rpki.left_right.self_elt, rpki.left_right.bsc_elt, rpki.left_-right.parent_elt, and rpki.left_right.child_elt.

Definition at line 143 of file xml_utils.py.

11.208.3.3 rpki::xml_utils.base_elt::elements = () [static]

XML elements contained by this element.

Reimplemented in rpki.left_right.self_elt, rpki.left_right.bsc_elt, rpki.left_-right.repository_elt, rpki.left_right.parent_elt, rpki.left_right.child_elt, rpki.publication.config_elt, and rpki.publication.client_elt.

Definition at line 139 of file xml_utils.py.

The documentation for this class was generated from the following file:

- xml_utils.py (2836)

11.209 rpki.xml_utils.data_elt Class Reference

Inherits rpki::xml_utils::base_elt.

Inherited by rpki.left_right.data_elt, and rpki.publication.control_elt.

Collaboration diagram for rpki.xml_utils.data_elt:

Public Member Functions

- def endElement
- def make_reply
- def make_reply_clone_hook
- def serve_create
- def serve_destroy

- def serve_destroy_hook
- def serve_dispatch
- def serve_fetch_one
- def serve_get
- def serve_list
- def serve_post_save_hook
- def serve_pre_save_hook
- def serve_set
- def toXML
- def unimplemented_control

11.209.1 Detailed Description

```
Virtual base class for PDUs that map to SQL objects.  These objects
all implement the create/set/get/list/destroy action attribute.
```

Definition at line 243 of file xml_utils.py.

11.209.2 Member Function Documentation

11.209.2.1 def rpki.xml_utils.data_elt.endElement (*self*, *stack*, *name*, *text*)

```
Default endElement handler for SQL-based objects.  This assumes
that sub-elements are Base64-encoded using the sql_template
mechanism.
```

Reimplemented from rpki.xml_utils.base_elt.

Reimplemented in rpki.left_right.child_elt, and rpki.publication.client_elt.

Definition at line 249 of file xml_utils.py.

11.209.2.2 def rpki.xml_utils.data_elt.make_reply (*self*, *r_pdu* = `None`)

```
Construct a reply PDU.
```

Definition at line 275 of file xml_utils.py.

11.209.2.3 def rpki.xml_utils.data_elt.make_reply_clone_hook (*self*, *r_pdu*)

```
Overridable hook.
```

Reimplemented in rpki.left_right.data_elt.

Definition at line 292 of file xml_utils.py.

11.209.2.4 def rpki.xml_utils.data_elt.serve_create (*self*, *r_msg*, *cb*, *eb*)

```
Handle a create action.
```

Definition at line 314 of file xml_utils.py.

11.209.2.5 def rpki.xml_utils.data_elt.serve_destroy (*self*, *r_msg*, *cb*, *eb*)

```
Handle a destroy action.
```

Definition at line 384 of file xml_utils.py.

11.209.2.6 def rpki.xml_utils.data_elt.serve_destroy_hook (*self*, *cb*, *eb*)

```
Overridable hook.
```

Reimplemented in rpki.left_right.child_elt.

Definition at line 378 of file xml_utils.py.

11.209.2.7 def rpki.xml_utils.data_elt.serve_dispatch (*self*, *r_msg*, *cb*, *eb*)

```
Action dispatch handler.
```

Reimplemented in rpki.publication.control_elt.

Definition at line 395 of file xml_utils.py.

11.209.2.8 def rpki.xml_utils.data_elt.serve_fetch_one (*self*)

```
Find the object on which a get, set, or destroy method should
operate.
```

Definition at line 296 of file xml_utils.py.

11.209.2.9 def rpki.xml_utils.data_elt.serve_get (*self*, *r_msg*, *cb*, *eb*)

```
Handle a get action.
```

Definition at line 360 of file xml_utils.py.

11.209.2.10 def rpki.xml_utils.data_elt.serve_list (*self*, *r_msg*, *cb*, *eb*)

```
Handle a list action for non-self objects.
```

Definition at line 369 of file xml_utils.py.

11.209.2.11 def rpki.xml_utils.data_elt.serve_post_save_hook (*self*, *q_pdu*, *r_pdu*, *cb*, *eb*)

```
Overridable hook.
```

Reimplemented in rpki.left_right.self_elt, rpki.left_right.parent_elt, rpki.left_-right.child_elt, and rpki.publication.client_elt.

Definition at line 310 of file xml_utils.py.

11.209.2.12 def rpki.xml_utils.data_elt.serve_pre_save_hook (*self*, *q_pdu*, *r_pdu*, *cb*, *eb*)

```
Overridable hook.
```

Reimplemented in rpki.left_right.data_elt, and rpki.left_right.bsc_elt.

Definition at line 306 of file xml_utils.py.

11.209.2.13 def rpki.xml_utils.data_elt.serve_set (*self*, *r_msg*, *cb*, *eb*)

```
Handle a set action.
```

Reimplemented in rpki.publication.config_elt.

Definition at line 337 of file xml_utils.py.

11.209.2.14 def rpki.xml_utils.data_elt.toXML (*self*)

```
Default element generator for SQL-based objects.  This assumes
that sub-elements are Base64-encoded DER objects.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 263 of file xml_utils.py.

11.209.2.15 def rpki.xml_utils.data_elt.unimplemented_control (*self*, *controls*)

```
Uniform handling for unimplemented control operations.
```

Definition at line 408 of file xml_utils.py.

The documentation for this class was generated from the following file:

- xml_utils.py (2836)

11.210 rpki.xml_utils.msg Class Reference

Inherits list.

Inherited by rpki.left_right.msg, and rpki.publication.msg.

Collaboration diagram for rpki.xml_utils.msg:

Public Member Functions

- def __str__
- def endElement
- def is_query
- def is_reply
- def query
- def reply
- def startElement
- def toXML

Public Attributes

- type
- version

11.210.1 Detailed Description

```
Generic top-level PDU.
```

Definition at line 416 of file xml_utils.py.

11.210.2 Member Function Documentation

11.210.2.1 def rpki.xml_utils.msg.__str__ (*self*)

```
Convert msg object to string.
```

Definition at line 442 of file xml_utils.py.

11.210.2.2 def rpki.xml_utils.msg.endElement (*self*, *stack*, *name*, *text*)

```
Handle top-level PDU.
```

Definition at line 434 of file xml_utils.py.

11.210.2.3 def rpki.xml_utils.msg.is_query (*self*)

```
Is this msg a query?
```

Definition at line 468 of file xml_utils.py.

11.210.2.4 def rpki.xml_utils.msg.is_reply (*self*)

```
Is this msg a reply?
```

Definition at line 472 of file xml_utils.py.

11.210.2.5 def rpki.xml_utils.msg.query (*cls*, *args*)

```
Create a query PDU.
```

Definition at line 455 of file xml_utils.py.

11.210.2.6 def rpki.xml_utils.msg.reply (*cls*, *args*)

```
Create a reply PDU.
```

Definition at line 462 of file xml_utils.py.

11.210.2.7 def rpki.xml_utils.msg.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle top-level PDU.
```

Definition at line 421 of file xml_utils.py.

11.210.2.8 def rpki.xml_utils.msg.toXML (*self*)

```
Generate top-level PDU.
```

Definition at line 446 of file xml_utils.py.

11.210.3 Member Data Documentation

11.210.3.1 rpki.xml_utils.msg.type

Definition at line 427 of file xml_utils.py.

11.210.3.2 rpki.xml_utils.msg.version

Reimplemented in rpki.left_right.msg, and rpki.publication.msg.

Definition at line 426 of file xml_utils.py.

The documentation for this class was generated from the following file:

- xml_utils.py (2836)

11.211 rpki.xml_utils.sax_handler Class Reference

Inherits xml::sax::handler::ContentHandler.

Inherited by rpki.left_right.sax_handler, rpki.publication.sax_handler, and rpki.up_-down.sax_handler.

Collaboration diagram for rpki.xml_utils.sax_handler:

Public Member Functions

- def __init__
- def characters
- def create_top_level
- def endElement
- def endElementNS
- def saxify
- def startElement
- def startElementNS

Public Attributes

- result
- stack
- text

11.211.1 Detailed Description

```
SAX handler for RPKI protocols.

This class provides some basic amenities for parsing protocol XML of
the kind we use in the RPKI protocols, including whacking all the
protocol element text into US-ASCII, simplifying accumulation of
text fields, and hiding some of the fun relating to XML namespaces.

General assumption: by the time this parsing code gets invoked, the
XML has already passed RelaxNG validation, so we only have to check
for errors that the schema can't catch, and we don't have to play as
many XML namespace games.
```

Definition at line 38 of file xml_utils.py.

11.211.2 Member Function Documentation

11.211.2.1 def rpki.xml_utils.sax_handler.__init__ (*self*)

```
Initialize SAX handler.
```

Definition at line 53 of file xml_utils.py.

11.211.2.2 def rpki.xml_utils.sax_handler.characters (*self*, *content*)

```
Accumulate a chuck of element content (text).
```

Definition at line 69 of file xml_utils.py.

11.211.2.3 def rpki.xml_utils.sax_handler.create_top_level (*self*, *name*, *attrs*)

```
Handle top-level PDU for this protocol.
```

Definition at line 119 of file xml_utils.py.

11.211.2.4 def rpki.xml_utils.sax_handler.endElement (*self*, *name*)

```
Handle endElement() events.  Mostly this means handling any
accumulated element text.
```

Definition at line 101 of file xml_utils.py.

11.211.2.5 def rpki.xml_utils.sax_handler.endElementNS (*self*, *name*, *qname*)

```
Redirect endElementNS() events to endElement().
```

Definition at line 65 of file xml_utils.py.

11.211.2.6 def rpki.xml_utils.sax_handler.saxify (*cls*, *elt*)

```
Create a one-off SAX parser, parse an ETree, return the result.
```

Definition at line 111 of file xml_utils.py.

11.211.2.7 def rpki.xml_utils.sax_handler.startElement (*self*, *name*, *attrs*)

```
Handle startElement() events.

We maintain a stack of nested elements under construction so that
we can feed events directly to the current element rather than
having to pass them through all the nesting elements.

If the stack is empty, this event is for the outermost element, so
we call a virtual method to create the corresponding object and
that's the object we'll be returning as our final result.
```

Definition at line 73 of file xml_utils.py.

11.211.2.8 def rpki.xml_utils.sax_handler.startElementNS (*self*, *name*, *qname*, *attrs*)

```
Redirect startElementNS() events to startElement().
```

Definition at line 61 of file xml_utils.py.

11.211.3 Member Data Documentation

11.211.3.1 rpki.xml_utils.sax_handler.result

Definition at line 97 of file xml_utils.py.

11.211.3.2 rpki.xml_utils.sax_handler.stack

Definition at line 59 of file xml_utils.py.

11.211.3.3 rpki.xml_utils.sax_handler.text

Definition at line 58 of file xml_utils.py.

The documentation for this class was generated from the following file:

- xml_utils.py (2836)

11.212 rpki.xml_utils.text_elt Class Reference

Inherits rpki::xml_utils::base_elt.

Inherited by rpki.left_right.list_published_objects_elt, rpki.left_right.report_error_elt, and rpki.publication.report_error_elt.

Collaboration diagram for rpki.xml_utils.text_elt:

Public Member Functions

- def endElement
- def toXML

Static Public Attributes

- text_attribute = None

  Name of the class attribute that holds the text value.

11.212.1 Detailed Description

```
Virtual base class for XML message elements that contain text.
```

Definition at line 219 of file xml_utils.py.

11.212.2 Member Function Documentation

11.212.2.1 def rpki.xml_utils.text_elt.endElement (*self*, *stack*, *name*, *text*)

```
Extract text from parsed XML.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 228 of file xml_utils.py.

11.212.2.2 def rpki.xml_utils.text_elt.toXML (*self*)

```
Insert text into generated XML.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 235 of file xml_utils.py.

11.212.3 Member Data Documentation

11.212.3.1 rpki::xml_utils.text_elt::text_attribute = None [static]

Name of the class attribute that holds the text value.

Reimplemented in rpki.left_right.list_published_objects_elt, rpki.left_right.report_-error_elt, and rpki.publication.report_error_elt.

Definition at line 226 of file xml_utils.py.

The documentation for this class was generated from the following file:

- xml_utils.py (2836)

11.213 Sequence Class Reference

Inherited by rpki.manifest.FileAndHash, rpki.manifest.Manifest, rpki.roa.ROAIPAddress, rpki.roa.ROAIPAddressFamily, and rpki.roa.RouteOriginAttestation.

The documentation for this class was generated from the following file:

- roa.py (2424)

11.214 SequenceOf Class Reference

Inherited by rpki.manifest.FilesAndHashes, rpki.roa.ROAIPAddresses, and rpki.roa.ROAIPAddressFamilies.

The documentation for this class was generated from the following file:

- roa.py (2424)

11.215 TextWrapper Class Reference

Inherited by irbe_cli.UsageWrapper.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

11.216 ContentHandler Class Reference

Inherited by rpki.xml_utils.sax_handler.

The documentation for this class was generated from the following file:

- xml_utils.py (2836)

12 File Documentation

12.1 __doc__.py File Reference

Packages

- package rpki.__doc__

12.1.1 Detailed Description

Documentation sourc, expressed as Python comments to make Doxygen happy.

Id

__doc__.py.in 3199 2010-04-14 13:19:14Z sra

Copyright (C) 2009-2010 Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008 American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Definition in file __doc__.py.

12.2 __init__.py File Reference

Packages

- package rpki

12.3 async.py File Reference

Classes

- class rpki.async.gc_summary
- class rpki.async.iterator
- class rpki.async.sync_wrapper
- class rpki.async.timer

Packages

- package rpki.async

Functions

- def rpki::async._raiseExitNow
- def rpki::async.defer
- def rpki::async.event_loop
- def rpki::async.exit_event_loop
- def rpki::async.run_deferred

Variables

- list rpki::async.deferred_queue = [ ]

  List to hold deferred actions.

- rpki::async.ExitNow = asyncore.ExitNow

12.4 cli.py File Reference

Classes

- class rpki.cli.Cmd

Packages

- package rpki.cli

Functions

- def rpki::cli.yes_or_no

Variables

- dictionary rpki::cli._yes_or_no_prompts
- rpki::cli.have_readline = True

12.5 config.py File Reference

Classes

- class rpki.config.parser

Packages

- package rpki.config

12.6 exceptions.py File Reference

Classes

- class rpki.exceptions.BadClassNameSyntax
- class rpki.exceptions.BadClientURL
- class rpki.exceptions.BadContactURL
- class rpki.exceptions.BadExtension
- class rpki.exceptions.BadIRDBReply
- class rpki.exceptions.BadIssueResponse
- class rpki.exceptions.BadPKCS10
- class rpki.exceptions.BadPublicationReply
- class rpki.exceptions.BadQuery
- class rpki.exceptions.BadSender
- class rpki.exceptions.BadStatusCode
- class rpki.exceptions.BadURISyntax
- class rpki.exceptions.BSCNotFound
- class rpki.exceptions.BSCNotReady

- class rpki.exceptions.ChildNotFound
- class rpki.exceptions.ClassNameMismatch
- class rpki.exceptions.ClassNameUnknown
- class rpki.exceptions.ClientNotFound
- class rpki.exceptions.CMSContentNotSet
- class rpki.exceptions.CMSCRLNotSet
- class rpki.exceptions.CMSVerificationFailed
- class rpki.exceptions.DBConsistancyError
- class rpki.exceptions.DERObjectConversionError
- class rpki.exceptions.DuplicateObject
- class rpki.exceptions.EmptyPEM
- class rpki.exceptions.EmptyROAPrefixList
- class rpki.exceptions.ForbiddenURI
- class rpki.exceptions.HandleTranslationError
- class rpki.exceptions.HTTPRequestFailed
- class rpki.exceptions.HTTPSBadVersion
- class rpki.exceptions.HTTPSClientAborted
- class rpki.exceptions.HTTPSUnexpectedState
- class rpki.exceptions.MissingCMSCRL
- class rpki.exceptions.MissingCMSEEcert
- class rpki.exceptions.MultipleTLSEECert
- class rpki.exceptions.MustBePrefix
- class rpki.exceptions.NoActiveCA
- class rpki.exceptions.NoCoveringCertForROA
- class rpki.exceptions.NoObjectAtURI
- class rpki.exceptions.NotACertificateChain
- class rpki.exceptions.NotFound
- class rpki.exceptions.NotImplementedYet
- class rpki.exceptions.NotInDatabase
- class rpki.exceptions.ReceivedTLSCACert
- class rpki.exceptions.RPKI_Exception
- class rpki.exceptions.ServerShuttingDown
- class rpki.exceptions.SKIMismatch
- class rpki.exceptions.SubprocessError
- class rpki.exceptions.TLSValidationError
- class rpki.exceptions.UnexpectedCMSCerts
- class rpki.exceptions.UnexpectedCMSCRLs
- class rpki.exceptions.UnparsableCMSDER
- class rpki.exceptions.UpstreamError
- class rpki.exceptions.WrongEContentType

Packages

- package rpki.exceptions

12.7 https.py File Reference

Classes

- class rpki.https.caller
- class rpki.https.http_client
- class rpki.https.http_listener
- class rpki.https.http_message
- class rpki.https.http_queue
- class rpki.https.http_request
- class rpki.https.http_response
- class rpki.https.http_server
- class rpki.https.http_stream

Packages

- package rpki.https

Functions

- def rpki::https.build_https_ta_cache
- def rpki::https.client
- def rpki::https.log_method
- def rpki::https.server

Variables

- dictionary rpki::https.client_queues = { }

  Map of (host, port) tuples to http_queue objects.

- rpki::https.debug_http = False

  Verbose chatter about HTTP streams.

- rpki::https.debug_tls_certs = False

  Verbose chatter about TLS certificates.

- tuple rpki::https.default_client_timeout = rpki.sundial.timedelta(minutes = 15)

  Default HTTP client connection timeout.

- tuple rpki::https.default_http_version = (1, 0)

  Preferred HTTP version.

- tuple rpki::https.default_server_timeout = rpki.sundial.timedelta(minutes = 20)

  Default HTTP server connection timeouts.

- string rpki::https.rpki_content_type = "application/x-rpki"

  HTTP content type used for all RPKI messages.

- tuple rpki::https.supported_address_families = (socket.AF_INET, socket.AF_-INET6)

  IP address families to support.

- rpki::https.want_persistent_client = False

  Whether we want persistent HTTP client streams, when server also supports them.

- rpki::https.want_persistent_server = False

  Whether we want persistent HTTP server streams, when client also supports them.

12.8 ipaddrs.py File Reference

Classes

- class rpki.ipaddrs.v4addr
- class rpki.ipaddrs.v6addr

Packages

- package rpki.ipaddrs

12.9 irbe_cli.py File Reference

Classes

- class irbe_cli.bsc_elt
- class irbe_cli.certificate_elt
- class irbe_cli.child_elt
- class irbe_cli.client_elt
- class irbe_cli.cmd_elt_mixin

- class irbe_cli.cmd_msg_mixin
- class irbe_cli.config_elt
- class irbe_cli.crl_elt
- class irbe_cli.left_right_cms_msg
- class irbe_cli.left_right_msg
- class irbe_cli.left_right_proto
- class irbe_cli.left_right_sax_handler
- class irbe_cli.list_published_objects_elt
- class irbe_cli.list_received_resources_elt
- class irbe_cli.manifest_elt
- class irbe_cli.parent_elt
- class irbe_cli.publication_cms_msg
- class irbe_cli.publication_msg
- class irbe_cli.publication_proto
- class irbe_cli.publication_sax_handler
- class irbe_cli.reply_elt_mixin
- class irbe_cli.report_error_elt
- class irbe_cli.report_error_elt
- class irbe_cli.repository_elt
- class irbe_cli.roa_elt
- class irbe_cli.self_elt
- class irbe_cli.UsageWrapper

Packages

- package irbe_cli

Functions

- def irbe_cli.usage

Variables

- list irbe_cli.argv = sys.argv[1:]
- tuple irbe_cli.call_pubd
- tuple irbe_cli.call_rpkid
- tuple irbe_cli.cfg = rpki.config.parser(cfg_file, "irbe_cli")
- string irbe_cli.cfg_file = "irbe.conf"
- irbe_cli.pem_out = None
- irbe_cli.q_msg = q_msg_left_right
- list irbe_cli.q_msg_left_right = [ ]
- list irbe_cli.q_msg_publication = [ ]

- list irbe_cli.q_pdu = left_right_msg.pdus[argv[0]]
- list irbe_cli.top_opts = ["config=", "help", "pem_out=", "quiet", "verbose"]
- tuple irbe_cli.usage_fill = UsageWrapper(subsequent_indent = " " ∗ 4)
- irbe_cli.verbose = True

12.10 irdbd.py File Reference

Packages

- package irdbd

Functions

- def irdbd.handle_list_resources
- def irdbd.handle_list_roa_requests
- def irdbd.handler

Variables

- tuple irdbd.bpki_ta = rpki.x509.X509(Auto_file = cfg.get("bpki-ta"))
- tuple irdbd.cfg = rpki.config.parser(cfg_file, "irdbd")
- string irdbd.cfg_file = "irdbd.conf"
- tuple irdbd.client_ta = (bpki_ta, rpkid_cert)
- tuple irdbd.cur = db.cursor()
- tuple irdbd.db
- dictionary irdbd.handle_dispatch
- tuple irdbd.handlers = ((u.path, handler),)
- string irdbd.host = "localhost"
- tuple irdbd.irdbd_cert = rpki.x509.X509(Auto_file = cfg.get("irdbd-cert"))
- tuple irdbd.irdbd_key = rpki.x509.RSA(Auto_file = cfg.get("irdbd-key"))
- int irdbd.port = 443
- tuple irdbd.rpkid_cert = rpki.x509.X509(Auto_file = cfg.get("rpkid-cert"))
- irdbd.server_cert = irdbd_cert,
- tuple irdbd.startup_msg = cfg.get("startup-message", "")
- tuple irdbd.u = urlparse.urlparse(cfg.get("https-url"))

12.11 left_right.py File Reference

Classes

- class rpki.left_right.bsc_elt

- class rpki.left_right.child_elt
- class rpki.left_right.cms_msg
- class rpki.left_right.data_elt
- class rpki.left_right.left_right_namespace
- class rpki.left_right.list_published_objects_elt
- class rpki.left_right.list_received_resources_elt
- class rpki.left_right.list_resources_elt
- class rpki.left_right.list_roa_requests_elt
- class rpki.left_right.msg
- class rpki.left_right.parent_elt
- class rpki.left_right.report_error_elt
- class rpki.left_right.repository_elt
- class rpki.left_right.sax_handler
- class rpki.left_right.self_elt

Packages

- package rpki.left_right

Variables

- rpki::left_right.enforce_strict_up_down_xml_sender = False

12.12 log.py File Reference

Classes

- class rpki.log.logger

Packages

- package rpki.log

Functions

- def rpki::log.init
- def rpki::log.set_trace
- def rpki::log.trace
- def rpki::log.traceback

Variables

- tuple rpki::log.debug = logger(syslog.LOG_DEBUG)
- rpki::log.enable_trace = False

  Whether call tracing is enabled.

- tuple rpki::log.error = logger(syslog.LOG_ERR)
- tuple rpki::log.info = logger(syslog.LOG_INFO)
- tuple rpki::log.note = logger(syslog.LOG_NOTICE)
- int rpki::log.pid = 0
- string rpki::log.tag = ""
- rpki::log.use_syslog = True

  Whether to use syslog.

- tuple rpki::log.warn = logger(syslog.LOG_WARNING)

12.13 manifest.py File Reference

Classes

- class rpki.manifest.FileAndHash
- class rpki.manifest.FilesAndHashes
- class rpki.manifest.Manifest

Packages

- package rpki.manifest

12.14 oids.py File Reference

Packages

- package rpki.oids

Variables

- tuple rpki::oids.name2oid = dict((v, k) for k, v in oid2name.items())

  Mapping table of string names to OIDs.

- dictionary rpki::oids.oid2name

  Mapping table of OIDs to conventional string names.

12.15 pubd.py File Reference

Classes

- class pubd.pubd_context

Packages

- package pubd

Functions

- def pubd.main

Variables

- string pubd.cfg_file = "pubd.conf"
- pubd.profile = False

12.16 publication.py File Reference

Classes

- class rpki.publication.certificate_elt
- class rpki.publication.client_elt
- class rpki.publication.cms_msg
- class rpki.publication.config_elt
- class rpki.publication.control_elt
- class rpki.publication.crl_elt
- class rpki.publication.manifest_elt
- class rpki.publication.msg
- class rpki.publication.publication_namespace
- class rpki.publication.publication_object_elt
- class rpki.publication.report_error_elt
- class rpki.publication.roa_elt
- class rpki.publication.sax_handler

Packages

- package rpki.publication

12.17 relaxng.py File Reference

Packages

- package rpki.relaxng

Variables

- tuple rpki::relaxng.left_right

  Parsed RelaxNG left_right schema.

- tuple rpki::relaxng.publication

  Parsed RelaxNG publication schema.

- tuple rpki::relaxng.up_down

  Parsed RelaxNG up_down schema.

12.18 resource_set.py File Reference

Classes

- class rpki.resource_set.resource_bag
- class rpki.resource_set.resource_range
- class rpki.resource_set.resource_range_as
- class rpki.resource_set.resource_range_ip
- class rpki.resource_set.resource_range_ipv4
- class rpki.resource_set.resource_range_ipv6
- class rpki.resource_set.resource_set
- class rpki.resource_set.resource_set_as
- class rpki.resource_set.resource_set_ip
- class rpki.resource_set.resource_set_ipv4
- class rpki.resource_set.resource_set_ipv6
- class rpki.resource_set.roa_prefix
- class rpki.resource_set.roa_prefix_ipv4
- class rpki.resource_set.roa_prefix_ipv6
- class rpki.resource_set.roa_prefix_set
- class rpki.resource_set.roa_prefix_set_ipv4
- class rpki.resource_set.roa_prefix_set_ipv6

Packages

- package rpki.resource_set

Functions

- def rpki::resource_set._bs2long
- def rpki::resource_set._long2bs
- def rpki::resource_set._rsplit
- def rpki::resource_set.test1
- def rpki::resource_set.test2

Variables

- string rpki::resource_set.inherit_token = "<inherit>"

  Token used to indicate inheritance in read and print syntax.

12.19 roa.py File Reference

Classes

- class rpki.roa.ROAIPAddress
- class rpki.roa.ROAIPAddresses
- class rpki.roa.ROAIPAddressFamilies
- class rpki.roa.ROAIPAddressFamily
- class rpki.roa.RouteOriginAttestation

Packages

- package rpki.roa

12.20 rootd.py File Reference

Classes

- class rootd.cms_msg
- class rootd.issue_pdu
- class rootd.list_pdu
- class rootd.message_pdu
- class rootd.revoke_pdu
- class rootd.sax_handler

Packages

- package rootd

Functions

- def rootd.compose_response
- def rootd.del_subject_cert
- def rootd.del_subject_pkcs10
- def rootd.get_root_cert
- def rootd.get_subject_cert
- def rootd.get_subject_pkcs10
- def rootd.issue_subject_cert_maybe
- def rootd.root_newer_than_subject
- def rootd.set_subject_cert
- def rootd.set_subject_pkcs10
- def rootd.up_down_handler

Variables

- tuple rootd.bpki_ta = rpki.x509.X509(Auto_file = cfg.get("bpki-ta"))
- tuple rootd.cfg = rpki.config.parser(cfg_file, "rootd")
- string rootd.cfg_file = "rootd.conf"
- tuple rootd.child_bpki_cert = rpki.x509.X509(Auto_file = cfg.get("child-bpki-cert"))
- tuple rootd.client_ta = (bpki_ta, child_bpki_cert)
- rootd.handlers = up_down_handler)
- rootd.host = https_server_host,
- tuple rootd.https_server_host = cfg.get("server-host", "")
- tuple rootd.https_server_port = int(cfg.get("server-port"))
- rootd.port = https_server_port,
- tuple rootd.rootd_bpki_cert = rpki.x509.X509(Auto_file = cfg.get("rootd-bpki-cert"))
- tuple rootd.rootd_bpki_crl = rpki.x509.CRL(Auto_file = cfg.get("rootd-bpki-crl"))
- tuple rootd.rootd_bpki_key = rpki.x509.RSA(Auto_file = cfg.get("rootd-bpki-key"))
- tuple rootd.rpki_base_uri = cfg.get("rpki-base-uri", "rsync://" + rpki_class_name + ".invalid/")
- tuple rootd.rpki_class_name = cfg.get("rpki-class-name", "wombat")
- rootd.rpki_root_cert = None
- tuple rootd.rpki_root_cert_file = cfg.get("rpki-root-cert")
- tuple rootd.rpki_root_cert_uri = cfg.get("rpki-root-cert-uri", rpki_base_uri + "Root.cer")
- tuple rootd.rpki_root_crl = cfg.get("rpki-root-crl", "Root.crl")
- tuple rootd.rpki_root_dir = cfg.get("rpki-root-dir")

- tuple rootd.rpki_root_key = rpki.x509.RSA(Auto_file = cfg.get("rpki-root-key"))
- tuple rootd.rpki_root_manifest = cfg.get("rpki-root-manifest", "Root.mnf")
- tuple rootd.rpki_subject_cert = cfg.get("rpki-subject-cert", "Child.cer")
- tuple rootd.rpki_subject_lifetime = rpki.sundial.timedelta.parse(cfg.get("rpki-subject-lifetime", "30d"))
- tuple rootd.rpki_subject_pkcs10 = cfg.get("rpki-subject-pkcs10", "Child.pkcs10")
- tuple rootd.rpki_subject_regen = rpki.sundial.timedelta.parse(cfg.get("rpki-subject-regen", rpki_subject_lifetime.convert_to_seconds() / 2))
- rootd.server_cert = rootd_bpki_cert,

12.21 rpki_engine.py File Reference

Classes

- class rpki.rpki_engine.ca_detail_obj
- class rpki.rpki_engine.ca_obj
- class rpki.rpki_engine.child_cert_obj
- class rpki.rpki_engine.publication_queue
- class rpki.rpki_engine.revoked_cert_obj
- class rpki.rpki_engine.roa_obj
- class rpki.rpki_engine.rpkid_context

Packages

- package rpki.rpki_engine

12.22 rpkid.py File Reference

Packages

- package rpkid

Functions

- def rpkid.main

Variables

- string rpkid.cfg_file = "rpkid.conf"
- rpkid.profile = None

12.23 sql.py File Reference

Classes

- class rpki.sql.session
- class rpki.sql.sql_persistent
- class rpki.sql.template

Packages

- package rpki.sql

12.24 sundial.py File Reference

Classes

- class rpki.sundial.datetime
- class rpki.sundial.timedelta

Packages

- package rpki.sundial

Functions

- def rpki::sundial._cast
- def rpki::sundial.now
- def rpki::sundial.test

12.25 up_down.py File Reference

Classes

- class rpki.up_down.base_elt
- class rpki.up_down.certificate_elt
- class rpki.up_down.class_elt
- class rpki.up_down.class_response_syntax
- class rpki.up_down.cms_msg
- class rpki.up_down.error_response_pdu
- class rpki.up_down.issue_pdu
- class rpki.up_down.issue_response_pdu

- class rpki.up_down.list_pdu
- class rpki.up_down.list_response_pdu
- class rpki.up_down.message_pdu
- class rpki.up_down.multi_uri
- class rpki.up_down.revoke_pdu
- class rpki.up_down.revoke_response_pdu
- class rpki.up_down.revoke_syntax
- class rpki.up_down.sax_handler

Packages

- package rpki.up_down

Variables

- dictionary rpki::up_down.nsmap = { None : xmlns }
- string rpki::up_down.xmlns = "http://www.apnic.net/specs/rescerts/up-down/"

12.26 x509.py File Reference

Classes

- class rpki.x509.CMS_object
- class rpki.x509.CRL
- class rpki.x509.DeadDrop
- class rpki.x509.DER_CMS_object
- class rpki.x509.DER_object
- class rpki.x509.PEM_converter
- class rpki.x509.PKCS10
- class rpki.x509.ROA
- class rpki.x509.RSA
- class rpki.x509.RSApublic
- class rpki.x509.SignedManifest
- class rpki.x509.X509
- class rpki.x509.XML_CMS_object

Packages

- package rpki.x509

Functions

- def rpki::x509._find_xia_uri
- def rpki::x509.calculate_SKI
- def rpki::x509.POWify_OID

12.27 xml_utils.py File Reference

Classes

- class rpki.xml_utils.base_elt
- class rpki.xml_utils.data_elt
- class rpki.xml_utils.msg
- class rpki.xml_utils.sax_handler
- class rpki.xml_utils.text_elt

Packages

- package rpki.xml_utils

Index

__abs__
  rpki::sundial::timedelta, 515
__add__
  rpki::sundial::datetime, 508
  rpki::sundial::timedelta, 515
__call__
  irbe_cli::UsageWrapper, 151
  rpki::async::iterator, 171
  rpki::async::sync_wrapper, 175
  rpki::https::caller, 250
  rpki::log::logger, 352
__cmp__
  rpki::async::timer, 179
  rpki::resource_set::resource_range, 401
  rpki::resource_set::roa_prefix, 427
  rpki::x509::DER_object, 579
__del__
  rpki::async::timer, 179
__div__
  rpki::sundial::timedelta, 515
__doc__.py, 635
__eq__
  rpki::resource_set::resource_bag, 397
__floordiv__
  rpki::sundial::timedelta, 515
__init__
  pubd::pubd_context, 153
  rpki::async::gc_summary, 169
  rpki::async::iterator, 171
  rpki::async::sync_wrapper, 175
  rpki::async::timer, 179
  rpki::cli::Cmd, 184
  rpki::config::parser, 189
  rpki::https::caller, 250
  rpki::https::http_client, 253
  rpki::https::http_listener, 259
  rpki::https::http_message, 262
  rpki::https::http_queue, 266
  rpki::https::http_request, 270
  rpki::https::http_response, 273
  rpki::https::http_server, 276
  rpki::https::http_stream, 282
  rpki::log::logger, 352
  rpki::manifest::FileAndHash, 354
  rpki::manifest::FilesAndHashes, 355
  rpki::manifest::Manifest, 357
  rpki::resource_set::resource_bag, 397
  rpki::resource_set::resource_range, 401
  rpki::resource_set::resource_set, 413
  rpki::resource_set::roa_prefix, 427
  rpki::resource_set::roa_prefix_set, 435
  rpki::roa::ROAIPAddress, 441
  rpki::roa::ROAIPAddresses, 443
  rpki::roa::ROAIPAddressFamilies, 444
  rpki::roa::ROAIPAddressFamily, 445
  rpki::roa::RouteOriginAttestation, 447
  rpki::rpki_engine::child_cert_obj, 466
  rpki::rpki_engine::publication_-queue, 471
  rpki::rpki_engine::revoked_cert_obj, 474
  rpki::rpki_engine::roa_obj, 478
  rpki::rpki_engine::rpkid_context, 486
  rpki::sql::session, 493
  rpki::sql::template, 505
  rpki::up_down::class_elt, 525
  rpki::up_down::class_response_-syntax, 529
  rpki::up_down::error_response_pdu, 534
  rpki::up_down::multi_uri, 552
  rpki::x509::DeadDrop, 574
  rpki::x509::DER_object, 579
  rpki::x509::PEM_converter, 586

rpki::xml_utils::sax_handler, 629
__init__.py(3150), 636
__mul__
rpki::sundial::timedelta, 515
__ne__
rpki::resource_set::resource_bag, 397
__neg__
rpki::sundial::timedelta, 515
__new__
rpki::ipaddrs::v4addr, 289
rpki::ipaddrs::v6addr, 292
__pos__
rpki::sundial::timedelta, 515
__radd__
rpki::sundial::datetime, 508
rpki::sundial::timedelta, 515
__rdiv__
rpki::sundial::timedelta, 516
__repr__
rpki::async::iterator, 172
rpki::async::timer, 179
__rfloordiv__
rpki::sundial::timedelta, 516
__rmul__
rpki::sundial::timedelta, 516
__rsub__
rpki::sundial::datetime, 508
rpki::sundial::timedelta, 516
__str__
rpki::https::http_message, 262
rpki::ipaddrs::v4addr, 289
rpki::ipaddrs::v6addr, 292
rpki::publication::report_error_elt, 389
rpki::resource_set::resource_bag, 398
rpki::resource_set::resource_range_as, 403
rpki::resource_set::resource_range_ip, 406
rpki::resource_set::resource_set, 413
rpki::resource_set::roa_prefix, 427
rpki::resource_set::roa_prefix_set, 435
rpki::sundial::datetime, 509
rpki::up_down::message_pdu, 548
rpki::up_down::multi_uri, 553
rpki::xml_utils::base_elt, 616
rpki::xml_utils::msg, 626
__sub__
rpki::sundial::datetime, 509
rpki::sundial::timedelta, 516
_add
rpki::rpki_engine::publication_queue, 471
_bs2long
rpki::resource_set, 89
_cast
rpki::sundial, 94
_comm
rpki::resource_set::resource_set, 413
_exceptions_enabled
rpki::sql::session, 494
_find_xia_uri
rpki::x509, 98
_long2bs
rpki::resource_set, 89
_prefixlen
rpki::resource_set::resource_range_ip, 406
_raiseExitNow
rpki::async, 67
_regexp
rpki::config::parser, 191
_repl
rpki::config::parser, 189
_rsplit
rpki::resource_set, 89
_wrap_execute
rpki::sql::session, 493
_yes_or_no_prompts
rpki::cli, 70

activate
rpki::rpki_engine::ca_detail_obj, 451
address
rpki::roa::ROAIPAddress, 442
addresses
rpki::roa::ROAIPAddressFamily, 446

addressFamily
rpki::roa::ROAIPAddressFamily, 446
af
rpki::https::http_client, 256
afi
rpki::resource_set::resource_set_-ipv4, 423
rpki::resource_set::resource_set_-ipv6, 425
argv
irbe_cli, 50
asID
rpki::roa::RouteOriginAttestation, 447
asn
rpki::left_right::list_resources_elt, 320
rpki::resource_set::resource_bag, 399
rpki::rpki_engine::roa_obj, 481
assert_pristine
rpki::sql::session, 493
async.py(3191), 636
asynchat::async_chat, 101
asyncore::dispatcher, 101
attributes
rpki::left_right::bsc_elt, 296
rpki::left_right::child_elt, 302
rpki::left_right::list_published_-objects_elt, 314
rpki::left_right::list_received_-resources_elt, 316
rpki::left_right::list_resources_elt, 320
rpki::left_right::list_roa_requests_-elt, 322
rpki::left_right::parent_elt, 330
rpki::left_right::report_error_elt, 335
rpki::left_right::repository_elt, 339
rpki::left_right::self_elt, 349
rpki::publication::client_elt, 363
rpki::publication::config_elt, 370
rpki::publication::publication_-object_elt, 386
rpki::publication::report_error_elt, 390
rpki::xml_utils::base_elt, 618

b
rpki::x509::PEM_converter, 587
base_uri
rpki::publication::client_elt, 363
bits
rpki::ipaddrs::v4addr, 290
rpki::ipaddrs::v6addr, 292
body
rpki::https::http_message, 264
booleans
rpki::left_right::bsc_elt, 296
rpki::left_right::child_elt, 302
rpki::left_right::parent_elt, 330
rpki::left_right::self_elt, 349
rpki::xml_utils::base_elt, 618
bpki_cert
irbe_cli::cmd_elt_mixin, 114
rpki::left_right::child_elt, 302
rpki::left_right::repository_elt, 339
rpki::left_right::self_elt, 349
rpki::publication::client_elt, 364
bpki_cms_cert
irbe_cli::cmd_elt_mixin, 114
rpki::left_right::parent_elt, 330
bpki_cms_glue
irbe_cli::cmd_elt_mixin, 114
rpki::left_right::parent_elt, 330
bpki_crl
irbe_cli::config_elt, 118
bpki_glue
irbe_cli::cmd_elt_mixin, 114
rpki::left_right::child_elt, 302
rpki::left_right::repository_elt, 339
rpki::left_right::self_elt, 349
rpki::publication::client_elt, 364
bpki_https_cert
irbe_cli::cmd_elt_mixin, 114
rpki::left_right::parent_elt, 331
bpki_https_glue
irbe_cli::cmd_elt_mixin, 114
rpki::left_right::parent_elt, 331
bpki_ta

irdbd, 54
pubd::pubd_context, 154
rootd, 62
rpki::rpki_engine::rpkid_context, 488
bsc
rpki::left_right::data_elt, 307
bscs
rpki::left_right::self_elt, 345
buffer
rpki::https::http_stream, 287
build
rpki::x509::ROA, 593
rpki::x509::SignedManifest, 603
build_https_ta_cache
pubd::pubd_context, 153
rpki::https, 75
rpki::rpki_engine::rpkid_context, 486

ca
rpki::rpki_engine::ca_detail_obj, 451
ca_cert_uri
rpki::rpki_engine::ca_detail_obj, 455
ca_detail
rpki::rpki_engine::child_cert_obj, 466
rpki::rpki_engine::revoked_cert_obj, 474
rpki::rpki_engine::roa_obj, 478
ca_detail_id
rpki::rpki_engine::child_cert_obj, 468
rpki::rpki_engine::revoked_cert_obj, 475
rpki::rpki_engine::roa_obj, 481
ca_details
rpki::rpki_engine::ca_obj, 459
ca_from_class_name
rpki::left_right::child_elt, 300
ca_id
rpki::rpki_engine::ca_detail_obj, 455
cache
rpki::sql::session, 495
cache_clear
rpki::sql::session, 493
calculate_SKI
rpki::x509, 98
call_pubd
irbe_cli, 50
rpki::left_right::repository_elt, 338
rpki::rpki_engine::publication_-queue, 471
call_rpkid
irbe_cli, 50
callback
rpki::https::http_request, 271
caller_function
rpki::async::iterator, 172
cancel
rpki::async::timer, 179
cas
rpki::left_right::parent_elt, 328
cb
rpki::async::sync_wrapper, 175
cert
rpki::https::http_client, 256
rpki::https::http_listener, 260
rpki::https::http_queue, 267
rpki::rpki_engine::child_cert_obj, 468
rpki::rpki_engine::roa_obj, 481
rpki::up_down::certificate_elt, 523
cert_url
rpki::up_down::certificate_elt, 523
rpki::up_down::class_elt, 526
certs
rpki::up_down::class_elt, 526
cfg
irbe_cli, 50
irdbd, 54
rootd, 62
rpki::config::parser, 191
cfg_file
irbe_cli, 51
irdbd, 54
pubd, 58
rootd, 62
rpkid, 100

characters
rpki::xml_utils::sax_handler, 629
check_allowed_uri
rpki::publication::client_elt, 362
check_for_updates
rpki::rpki_engine::ca_obj, 459
check_response
rpki::up_down::base_elt, 519
rpki::up_down::error_response_pdu, 534
rpki::up_down::issue_response_pdu, 542
check_valid_rpki
rpki::x509::PKCS10, 589
checkpoint
rpki::rpki_engine::rpkid_context, 486
child
rpki::rpki_engine::child_cert_obj, 466
child_bpki_cert
rootd, 62
child_certs
rpki::left_right::child_elt, 300
rpki::rpki_engine::ca_detail_obj, 451
child_id
rpki::rpki_engine::child_cert_obj, 468
children
rpki::left_right::bsc_elt, 295
rpki::left_right::self_elt, 345
chunk_body
rpki::https::http_stream, 282
chunk_discard_crlf
rpki::https::http_stream, 282
chunk_discard_trailer
rpki::https::http_stream, 282
chunk_handler
rpki::https::http_stream, 287
chunk_header
rpki::https::http_stream, 282
class_name
rpki::up_down::class_elt, 526
rpki::up_down::issue_pdu, 539
rpki::up_down::revoke_pdu, 556
rpki::up_down::revoke_syntax, 559
classes
rpki::up_down::class_response_-syntax, 530
clear
rpki::async::timer, 179
rpki::x509::DER_object, 579
clear_https_ta_cache
pubd::pubd_context, 153
rpki::left_right::child_elt, 302
rpki::publication::client_elt, 364
rpki::rpki_engine::rpkid_context, 486
cli.py(3191), 636
client
rpki::https, 75
rpki::https::http_queue, 267
client_cert
rpki::https::caller, 250
client_getopt
irbe_cli::cmd_elt_mixin, 112
client_handler
pubd::pubd_context, 154
client_key
rpki::https::caller, 250
client_poll
rpki::left_right::self_elt, 345
client_query_bpki_cert
irbe_cli::cmd_elt_mixin, 112
client_query_bpki_cms_cert
irbe_cli::cmd_elt_mixin, 112
client_query_bpki_crl
irbe_cli::config_elt, 118
client_query_bpki_https_cert
irbe_cli::cmd_elt_mixin, 113
client_query_cms_glue
irbe_cli::cmd_elt_mixin, 113
client_query_glue
irbe_cli::cmd_elt_mixin, 113
client_query_https_glue
irbe_cli::cmd_elt_mixin, 113
client_query_signing_cert
irbe_cli::bsc_elt, 103
client_query_signing_cert_crl
irbe_cli::bsc_elt, 103
client_queues

rpki::https, 76
client_reply_decode
irbe_cli::bsc_elt, 103
irbe_cli::reply_elt_mixin, 142
client_reply_show
irbe_cli::reply_elt_mixin, 143
client_ta
irdbd, 54
rootd, 62
client_url_regexp
pubd::pubd_context, 154
close
rpki::https::http_stream, 282
rpki::sql::session, 493
cmd
rpki::https::http_request, 271
cmd::Cmd, 101
cmdloop_with_history
rpki::cli::Cmd, 184, 186
cms_msg
irbe_cli::left_right_proto, 124
irbe_cli::publication_proto, 139
code
rpki::https::http_response, 273
codes
rpki::up_down::error_response_pdu, 535
collect_incoming_data
rpki::https::http_stream, 283
columns
rpki::sql::template, 505
complete_help
rpki::cli::Cmd, 184
completenames
rpki::cli::Cmd, 185
compose_response
rootd, 60
config.py(3107), 637
config_id
rpki::publication::config_elt, 370
connect
rpki::sql::session, 493
construct_sia_uri
rpki::rpki_engine::ca_obj, 460
contains
rpki::resource_set::resource_set, 414
content
rpki::x509::CMS_object, 566
rpki::x509::DER_CMS_object, 576
rpki::x509::XML_CMS_object, 614
content_class
rpki::x509::ROA, 593
rpki::x509::SignedManifest, 604
control_handler
pubd::pubd_context, 154
convert_to_seconds
rpki::sundial::timedelta, 516
create
rpki::rpki_engine::ca_detail_obj, 451
rpki::rpki_engine::ca_obj, 460
rpki::x509::PKCS10, 589
create_ca
rpki::x509::PKCS10, 589
create_top_level
rpki::xml_utils::sax_handler, 630
crl_interval
rpki::left_right::self_elt, 350
crl_published
rpki::rpki_engine::ca_detail_obj, 455
crl_published_callback
rpki::rpki_engine::ca_detail_obj, 451
crl_uri
rpki::rpki_engine::ca_detail_obj, 451
crl_uri_tail
rpki::rpki_engine::ca_detail_obj, 452
cron
rpki::left_right::self_elt, 345
rpki::rpki_engine::rpkid_context, 486
cron_keepalive
rpki::rpki_engine::rpkid_context, 488
cron_period
rpki::rpki_engine::rpkid_context, 488
cron_timeout

rpki::rpki_engine::rpkid_context, 488
cron_timer
rpki::rpki_engine::rpkid_context, 488
cronjob_handler
rpki::rpki_engine::rpkid_context, 486
cross_certify
rpki::x509::X509, 606
cur
irdbd, 54
rpki::sql::session, 495

database
rpki::sql::session, 495
datum_type
rpki::resource_set::resource_range_-as, 403
rpki::resource_set::resource_range_-ipv4, 409
rpki::resource_set::resource_range_-ipv6, 411
db
irdbd, 54
rpki::sql::session, 495
debug
rpki::https::caller, 251
rpki::log, 82
debug_cms_certs
rpki::x509::CMS_object, 566
debug_http
rpki::https, 76
debug_tls_certs
rpki::https, 76
decode
rpki::x509::DER_CMS_object, 576
rpki::x509::XML_CMS_object, 612
default_client_timeout
rpki::https, 76
default_http_version
rpki::https, 76
default_pubd_handler
rpki::left_right::repository_elt, 338
default_section
rpki::config::parser, 192
default_server_timeout
rpki::https, 76
defer
rpki::async, 67
deferred_queue
rpki::async, 68
del_subject_cert
rootd, 60
del_subject_pkcs10
rootd, 60
delete
rpki::rpki_engine::ca_detail_obj, 452
rpki::rpki_engine::ca_obj, 460
rpki::sql::template, 505
DER
rpki::x509::CMS_object, 567
rpki::x509::CRL, 572
rpki::x509::DER_object, 584
rpki::x509::PKCS10, 590
rpki::x509::RSA, 597
rpki::x509::RSApublic, 601
rpki::x509::X509, 609
description
rpki::up_down::error_response_pdu, 535
detach
rpki::https::http_queue, 266
difference
rpki::resource_set::resource_set, 414
dirty
rpki::sql::session, 495
do_EOF
rpki::cli::Cmd, 185
do_exit
rpki::cli::Cmd, 185
do_quit
rpki::cli::Cmd, 186
doit
rpki::async::iterator, 172
done_callback
rpki::async::iterator, 172
dump
rpki::x509::DeadDrop, 574
dump_inbound_cms
rpki::x509::XML_CMS_object, 614

dump_on_verify_failure
rpki::x509::CMS_object, 567
dump_outbound_cms
rpki::x509::XML_CMS_object, 614
dump_to_disk
rpki::x509::XML_CMS_object, 612
dumpasn1
rpki::x509::DER_object, 579
dynamic_ta
rpki::https::http_listener, 260

e
rpki::x509::PEM_converter, 587
earlier
rpki::sundial::datetime, 509
eb
rpki::async::sync_wrapper, 175
econtent_oid
rpki::x509::CMS_object, 567
rpki::x509::ROA, 593
rpki::x509::SignedManifest, 604
rpki::x509::XML_CMS_object, 614
element_name
rpki::left_right::bsc_elt, 297
rpki::left_right::child_elt, 302
rpki::left_right::list_published_-objects_elt, 314
rpki::left_right::list_received_-resources_elt, 316
rpki::left_right::list_resources_elt, 320
rpki::left_right::list_roa_requests_-elt, 322
rpki::left_right::parent_elt, 331
rpki::left_right::report_error_elt, 335
rpki::left_right::repository_elt, 339
rpki::left_right::self_elt, 350
rpki::publication::certificate_elt, 360
rpki::publication::client_elt, 364
rpki::publication::config_elt, 371
rpki::publication::crl_elt, 376
rpki::publication::manifest_elt, 378
rpki::publication::report_error_elt, 390
rpki::publication::roa_elt, 393
elements
rpki::left_right::bsc_elt, 297
rpki::left_right::child_elt, 303
rpki::left_right::parent_elt, 331
rpki::left_right::repository_elt, 340
rpki::left_right::self_elt, 350
rpki::publication::client_elt, 364
rpki::publication::config_elt, 371
rpki::xml_utils::base_elt, 618
empty
rpki::resource_set::resource_bag, 398
rpki::x509::DER_object, 579
emptyline
rpki::cli::Cmd, 185
emptyline_repeats_last_command
rpki::cli::Cmd, 186
enable_trace
rpki::log, 82
encode
rpki::x509::DER_CMS_object, 576
rpki::x509::XML_CMS_object, 612
encoding
rpki::left_right::cms_msg, 305
rpki::publication::cms_msg, 367
rpki::up_down::cms_msg, 532
endElement
rpki::left_right::child_elt, 301
rpki::publication::client_elt, 362
rpki::publication::publication_-object_elt, 384
rpki::up_down::base_elt, 519
rpki::up_down::certificate_elt, 522
rpki::up_down::class_elt, 525
rpki::up_down::error_response_pdu, 534
rpki::up_down::issue_pdu, 538
rpki::xml_utils::base_elt, 616
rpki::xml_utils::data_elt, 621
rpki::xml_utils::msg, 626
rpki::xml_utils::sax_handler, 630
rpki::xml_utils::text_elt, 633
endElementNS
rpki::xml_utils::sax_handler, 630
enforce_strict_up_down_xml_sender
rpki::left_right, 80
EOF_exits_command_loop

rpki::cli::Cmd, 187
err
rpki::async::sync_wrapper, 176
errback
rpki::async::timer, 179, 181
rpki::https::http_request, 271
error
rpki::log, 82
error_code
rpki::left_right::report_error_elt, 335
rpki::publication::report_error_elt, 390
error_text
rpki::left_right::report_error_elt, 335
rpki::publication::report_error_elt, 390
event_loop
rpki::async, 68
Exception, 101
exceptions
rpki::up_down::error_response_pdu, 535
exceptions.py(2907), 637
excludes
irbe_cli::bsc_elt, 104
irbe_cli::cmd_elt_mixin, 114
irbe_cli::list_published_objects_elt, 128
irbe_cli::list_received_resources_elt, 130
execute
rpki::sql::session, 493
executemany
rpki::sql::session, 494
exit_event_loop
rpki::async, 68
ExitNow
rpki::async, 68
expect_close
rpki::https::http_client, 256
rpki::https::http_server, 278
expired
rpki::x509::X509, 607
expires
rpki::rpki_engine::revoked_cert_obj, 475
explicitVersion
rpki::manifest::Manifest, 357
rpki::roa::RouteOriginAttestation, 447
extract
rpki::x509::CMS_object, 565

fetch
rpki::publication::config_elt, 369
rpki::rpki_engine::child_cert_obj, 467
fetch_active
rpki::rpki_engine::ca_obj, 460
fetch_deprecated
rpki::rpki_engine::ca_obj, 461
fetch_issue_response_candidates
rpki::rpki_engine::ca_obj, 461
fetch_pending
rpki::rpki_engine::ca_obj, 461
fetch_revoked
rpki::rpki_engine::ca_obj, 461
fetchall
rpki::sql::session, 494
file
rpki::manifest::FileAndHash, 354
fileHashAlg
rpki::manifest::Manifest, 357
fileList
rpki::manifest::Manifest, 357
filename
rpki::config::parser, 192
filename_complete
rpki::cli::Cmd, 185
find_handler
rpki::https::http_server, 276
format
rpki::https::http_message, 262
format_first_line
rpki::https::http_request, 270
rpki::https::http_response, 273
formats
rpki::x509::CMS_object, 567
rpki::x509::CRL, 572
rpki::x509::DER_object, 584
rpki::x509::PKCS10, 590
rpki::x509::RSA, 597

rpki::x509::RSApublic, 601
rpki::x509::X509, 609
found_terminator
rpki::https::http_stream, 283
from_bytes
rpki::ipaddrs::v4addr, 289
rpki::ipaddrs::v6addr, 292
from_exception
rpki::left_right::report_error_elt, 334
rpki::publication::report_error_elt, 389
from_resource_bag
rpki::up_down::class_elt, 525
from_rfc3779_tuples
rpki::resource_set::resource_bag, 398
from_sql
rpki::resource_set::resource_set, 414
rpki::resource_set::roa_prefix_set, 435
rpki::sundial::datetime, 509
rpki::x509::DER_object, 580
fromASN1tuple
rpki::sundial::datetime, 509
fromdatetime
rpki::sundial::datetime, 509
fromGeneralizedTime
rpki::sundial::datetime, 510
fromtimedelta
rpki::sundial::timedelta, 516
fromUTCTime
rpki::sundial::datetime, 510
fromXMLtime
rpki::sundial::datetime, 510
func
rpki::async::sync_wrapper, 176

gAKI
rpki::x509::DER_object, 580
gc_debug
rpki::async::timer, 181
gctx
rpki::rpki_engine::ca_detail_obj, 455
rpki::rpki_engine::ca_obj, 463
rpki::rpki_engine::child_cert_obj, 468
rpki::rpki_engine::revoked_cert_obj, 475
rpki::rpki_engine::roa_obj, 482
rpki::sql::sql_persistent, 502
generate
rpki::rpki_engine::roa_obj, 479
rpki::x509::CRL, 570
rpki::x509::RSA, 596
generate_crl
rpki::rpki_engine::ca_detail_obj, 452
generate_manifest
rpki::rpki_engine::ca_detail_obj, 452
generate_manifest_cert
rpki::rpki_engine::ca_detail_obj, 452
get
rpki::config::parser, 190
get_3779resources
rpki::x509::DER_object, 580
get_AIA
rpki::x509::DER_object, 580
get_aia_uri
rpki::x509::DER_object, 580
get_AKI
rpki::x509::DER_object, 581
get_Base64
rpki::x509::DER_object, 581
get_basicConstraints
rpki::x509::DER_object, 581
get_buffer
rpki::https::http_stream, 283
get_content
rpki::x509::CMS_object, 565
get_DER
rpki::x509::CMS_object, 565
rpki::x509::CRL, 570
rpki::x509::DER_object, 581
rpki::x509::PKCS10, 590
rpki::x509::RSA, 596
rpki::x509::RSApublic, 600
rpki::x509::X509, 607
get_PEM

rpki::x509::DER_object, 581
get_POW
rpki::x509::CMS_object, 565
rpki::x509::CRL, 571
rpki::x509::RSA, 596
rpki::x509::RSApublic, 600
rpki::x509::X509, 607
get_POWpkix
rpki::x509::CRL, 571
rpki::x509::PKCS10, 590
rpki::x509::X509, 607
get_public_DER
rpki::x509::RSA, 597
get_root_cert
rootd, 60
get_RSApublic
rpki::x509::RSA, 597
get_SIA
rpki::x509::DER_object, 582
get_sia_directory_uri
rpki::x509::DER_object, 582
get_sia_manifest_uri
rpki::x509::DER_object, 582
get_SKI
rpki::up_down::revoke_pdu, 555
rpki::x509::DER_object, 582
rpki::x509::RSA, 597
rpki::x509::RSApublic, 600
get_subject_cert
rootd, 61
get_subject_pkcs10
rootd, 61
getboolean
rpki::config::parser, 190
getint
rpki::config::parser, 190
getIssuer
rpki::x509::CRL, 571
rpki::x509::X509, 607
getlong
rpki::config::parser, 190
getNextUpdate
rpki::x509::CRL, 571
rpki::x509::SignedManifest, 603
getNotAfter
rpki::x509::X509, 607
getNotBefore
rpki::x509::X509, 608
getPublicKey
rpki::x509::PKCS10, 590
rpki::x509::X509, 608
getSerial
rpki::x509::X509, 608
getSubject
rpki::x509::X509, 608
getThisUpdate
rpki::x509::CRL, 571
rpki::x509::SignedManifest, 603
gSKI
rpki::x509::DER_object, 582

hAKI
rpki::x509::DER_object, 583
handle_accept
rpki::https::http_listener, 259
handle_body
rpki::https::http_stream, 283
handle_close
rpki::https::http_client, 253
rpki::https::http_stream, 284
handle_connect
rpki::https::http_client, 254
handle_dispatch
irdbd, 55
handle_error
rpki::https::http_client, 254
rpki::https::http_listener, 259
rpki::https::http_stream, 284
handle_list_resources
irdbd, 53
handle_list_roa_requests
irdbd, 53
handle_message
rpki::https::http_client, 254
rpki::https::http_server, 276
handle_no_content_length
rpki::https::http_client, 254
rpki::https::http_server, 277
handle_read
rpki::https::http_stream, 284
handle_timeout
rpki::https::http_client, 255

rpki::https::http_stream, 284
handle_write
rpki::https::http_stream, 285
handler
irdbd, 54
rpki::async::gc_summary, 169
rpki::async::timer, 180, 182
handler_common
pubd::pubd_context, 154
handlers
irdbd, 55
rootd, 62
rpki::https::http_listener, 260
rpki::https::http_server, 278
rpki::rpki_engine::publication_-queue, 472
handles
rpki::left_right::bsc_elt, 297
rpki::left_right::child_elt, 303
rpki::left_right::data_elt, 309
rpki::left_right::parent_elt, 331
rpki::left_right::repository_elt, 340
rpki::left_right::self_elt, 350
has_option
rpki::config::parser, 190
has_section
rpki::config::parser, 191
hash
rpki::manifest::FileAndHash, 354
have_readline
rpki::cli, 70
headers
rpki::https::http_message, 264
help_help
rpki::cli::Cmd, 186
histfile
rpki::cli::Cmd, 187
host
irdbd, 55
rootd, 62
hostport
rpki::https::http_client, 256
rpki::https::http_queue, 268
hSKI
rpki::x509::DER_object, 583
https.py(3191), 639
https_server_host
pubd::pubd_context, 155
rootd, 63
rpki::rpki_engine::rpkid_context, 489
https_server_port
pubd::pubd_context, 155
rootd, 63
rpki::rpki_engine::rpkid_context, 489
https_ta_cache
pubd::pubd_context, 155
rpki::rpki_engine::rpkid_context, 489

identchars
rpki::cli::Cmd, 187
index
rpki::sql::template, 505
info
rpki::log, 82
inherit
rpki::resource_set::resource_set, 415
rpki::resource_set::resource_set_as, 418
rpki::resource_set::resource_set_ip, 421
inherit_token
rpki::resource_set, 90
init
rpki::log, 81
initial_delay
rpki::rpki_engine::rpkid_context, 489
initiate_send
rpki::https::http_stream, 285
insert
rpki::sql::template, 505
intersection
rpki::resource_set::resource_bag, 398
rpki::resource_set::resource_set, 414
interval
rpki::async::gc_summary, 169
ipAddrBlocks

rpki::roa::RouteOriginAttestation, 447
ipaddrs.py(2424), 640
ipv4
rpki::left_right::list_resources_elt, 320
rpki::left_right::list_roa_requests_-elt, 323
rpki::rpki_engine::roa_obj, 482
ipv6
rpki::left_right::list_resources_elt, 320
rpki::left_right::list_roa_requests_-elt, 323
rpki::rpki_engine::roa_obj, 482
irbe_cert
pubd::pubd_context, 155
rpki::rpki_engine::rpkid_context, 489
irbe_cli, 48
argv, 50
call_pubd, 50
call_rpkid, 50
cfg, 50
cfg_file, 51
pem_out, 51
q_msg, 51
q_msg_left_right, 51
q_msg_publication, 51
q_pdu, 51
top_opts, 51
usage, 50
usage_fill, 52
verbose, 52
irbe_cli.py(3107), 640
irbe_cli::bsc_elt, 101
client_query_signing_cert, 103
client_query_signing_cert_crl, 103
client_reply_decode, 103
excludes, 104
signing_cert, 104
signing_cert_crl, 104
irbe_cli::certificate_elt, 104
irbe_cli::child_elt, 106
irbe_cli::client_elt, 108
irbe_cli::cmd_elt_mixin, 110
bpki_cert, 114
bpki_cms_cert, 114
bpki_cms_glue, 114
bpki_glue, 114
bpki_https_cert, 114
bpki_https_glue, 114
client_getopt, 112
client_query_bpki_cert, 112
client_query_bpki_cms_cert, 112
client_query_bpki_https_cert, 113
client_query_cms_glue, 113
client_query_glue, 113
client_query_https_glue, 113
excludes, 114
is_cmd, 115
usage, 113
irbe_cli::cmd_msg_mixin, 115
usage, 116
irbe_cli::config_elt, 116
bpki_crl, 118
client_query_bpki_crl, 118
irbe_cli::crl_elt, 118
irbe_cli::left_right_cms_msg, 120
saxify, 121
irbe_cli::left_right_msg, 121
pdus, 123
irbe_cli::left_right_proto, 123
cms_msg, 124
msg, 124
irbe_cli::left_right_sax_handler, 125
pdu, 126
irbe_cli::list_published_objects_elt, 126
excludes, 128
irbe_cli::list_received_resources_elt, 128
excludes, 130
irbe_cli::manifest_elt, 130
irbe_cli::parent_elt, 132
irbe_cli::publication_cms_msg, 134
saxify, 136
irbe_cli::publication_msg, 136
pdus, 138
irbe_cli::publication_proto, 138
cms_msg, 139
msg, 139
irbe_cli::publication_sax_handler, 140
pdu, 141

irbe_cli::reply_elt_mixin, 141
client_reply_decode, 142
client_reply_show, 143
is_cmd, 143
irbe_cli::report_error_elt, 143
irbe_cli::repository_elt, 144
irbe_cli::roa_elt, 146
irbe_cli::self_elt, 148
irbe_cli::UsageWrapper, 150
__call__, 151
irdb_cert
rpki::rpki_engine::rpkid_context, 489
irdb_query
rpki::rpki_engine::rpkid_context, 487
irdb_query_child_resources
rpki::rpki_engine::rpkid_context, 487
irdb_query_roa_requests
rpki::rpki_engine::rpkid_context, 487
irdb_url
rpki::rpki_engine::rpkid_context, 489
irdbd, 52
bpki_ta, 54
cfg, 54
cfg_file, 54
client_ta, 54
cur, 54
db, 54
handle_dispatch, 55
handle_list_resources, 53
handle_list_roa_requests, 53
handler, 54
handlers, 55
host, 55
irdbd_cert, 55
irdbd_key, 55
port, 55
rpkid_cert, 56
server_cert, 56
startup_msg, 56
u, 56
irdbd.py(2913), 642
irdbd_cert
irdbd, 55
irdbd_key
irdbd, 55
is_CA
rpki::x509::DER_object, 583
is_cmd
irbe_cli::cmd_elt_mixin, 115
irbe_cli::reply_elt_mixin, 143
is_query
rpki::xml_utils::msg, 626
is_reply
rpki::xml_utils::msg, 626
is_set
rpki::async::timer, 180
issubset
rpki::resource_set::resource_set, 414
issue
rpki::rpki_engine::ca_detail_obj, 453
rpki::x509::X509, 608
issue_ee
rpki::rpki_engine::ca_detail_obj, 453
issue_subject_cert_maybe
rootd, 61
issuer
rpki::up_down::class_elt, 527
issuperset
rpki::resource_set::resource_set, 415
item_callback
rpki::async::iterator, 172
iterator
rpki::async::iterator, 172

key
rpki::https::http_client, 256
rpki::https::http_listener, 260
rpki::https::http_queue, 268

last_crl_sn
rpki::rpki_engine::ca_obj, 463
last_issued_sn
rpki::rpki_engine::ca_obj, 463
last_manifest_sn
rpki::rpki_engine::ca_obj, 463

lastrowid
rpki::sql::session, 494
later
rpki::sundial::datetime, 510
latest_ca_cert
rpki::rpki_engine::ca_detail_obj, 455
latest_crl
rpki::rpki_engine::ca_detail_obj, 455
latest_manifest
rpki::rpki_engine::ca_detail_obj, 456
latest_manifest_cert
rpki::rpki_engine::ca_detail_obj, 456
left_right
rpki::relaxng, 87
left_right.py(3191), 642
left_right_handler
rpki::rpki_engine::rpkid_context, 487
log
rpki::https::http_listener, 260
rpki::https::http_queue, 268
rpki::https::http_stream, 287
log.py(3107), 643
log_cert
rpki::https::http_stream, 285
log_method
rpki::https, 75
log_query
rootd::message_pdu, 164
rpki::up_down::message_pdu, 548
long, 151
looks_like_PEM
rpki::x509::PEM_converter, 586

maildir
rpki::x509::DeadDrop, 574
main
pubd, 57
rpkid, 100
make_b64elt
rpki::up_down::base_elt, 519
rpki::xml_utils::base_elt, 617
make_elt
rpki::up_down::base_elt, 519
rpki::xml_utils::base_elt, 617
make_pdu
rpki::xml_utils::base_elt, 617
make_prefix
rpki::resource_set::resource_range_-ip, 406
make_publish
rpki::publication::publication_-object_elt, 384
make_query
rpki::up_down::message_pdu, 548
make_reply
rpki::left_right::list_published_-objects_elt, 313
rpki::left_right::list_received_-resources_elt, 316
rpki::xml_utils::data_elt, 621
make_reply_clone_hook
rpki::left_right::data_elt, 307
rpki::xml_utils::data_elt, 621
make_withdraw
rpki::publication::publication_-object_elt, 385
manifest.py(2424), 644
manifest_private_key_id
rpki::rpki_engine::ca_detail_obj, 456
manifest_public_key
rpki::rpki_engine::ca_detail_obj, 456
manifest_published
rpki::rpki_engine::ca_detail_obj, 456
manifest_published_callback
rpki::rpki_engine::ca_detail_obj, 453
manifest_uri
rpki::rpki_engine::ca_detail_obj, 453
manifestNumber
rpki::manifest::Manifest, 357
map
rpki::sql::template, 506
max

rpki::resource_set::resource_range, 401
rpki::resource_set::roa_prefix, 427
max_prefixlen
rpki::resource_set::roa_prefix, 428
maxLength
rpki::roa::ROAIPAddress, 442
min
rpki::resource_set::resource_range, 401
rpki::resource_set::resource_range_-as, 404
rpki::resource_set::roa_prefix, 428
msg
irbe_cli::left_right_proto, 124
irbe_cli::publication_proto, 139
rpki::https::http_stream, 287
msgs
rpki::rpki_engine::publication_-queue, 472
multiget
rpki::config::parser, 191

name
rpki::left_right::sax_handler, 342
rpki::publication::sax_handler, 395
rpki::up_down::sax_handler, 562
name2oid
rpki::oids, 85
name2type
rootd::message_pdu, 164
rpki::up_down::message_pdu, 550
next_crl_number
rpki::rpki_engine::ca_obj, 461
next_manifest_number
rpki::rpki_engine::ca_obj, 462
next_serial_number
rpki::rpki_engine::ca_obj, 462
nextUpdate
rpki::manifest::Manifest, 357
rpki::rpki_engine::ca_detail_obj, 456
normalize_chain
rpki::x509::X509, 609
normalize_headers
rpki::https::http_message, 263
note
rpki::log, 83
now
rpki::sundial, 94
nsmap
rpki::left_right::left_right_-namespace, 310
rpki::publication::publication_-namespace, 382
rpki::up_down, 96

obj
rpki::left_right::list_published_-objects_elt, 314
object, 151
oid2name
rpki::oids, 85
oids.py(2424), 644
onecmd
rpki::cli::Cmd, 186
other_clear
rpki::x509::CMS_object, 567
rpki::x509::DER_object, 584
oversized
rpki::resource_set::resource_bag, 398

parent
rpki::rpki_engine::ca_obj, 462
parent_id
rpki::rpki_engine::ca_obj, 463
parent_resource_class
rpki::rpki_engine::ca_obj, 463
parents
rpki::left_right::bsc_elt, 295
rpki::left_right::child_elt, 301
rpki::left_right::repository_elt, 339
rpki::left_right::self_elt, 345
parse
rpki::sundial::timedelta, 517
parse_first_line
rpki::https::http_request, 270
rpki::https::http_response, 273
parse_from_wire
rpki::https::http_message, 263
parse_rfc3779_tuple

rpki::resource_set::resource_set_as, 417
rpki::resource_set::resource_set_ip, 420
parse_str
rpki::resource_set::resource_set_as, 417
rpki::resource_set::resource_set_ip, 420
rpki::resource_set::roa_prefix_set, 435
parse_type
rpki::https::http_client, 256
rpki::https::http_server, 278
parse_version
rpki::https::http_message, 263
password
rpki::sql::session, 495
path
rpki::https::http_request, 271
payload
rpki::publication::publication_-object_elt, 386
rpki::up_down::message_pdu, 550
payload_type
rpki::publication::certificate_elt, 360
rpki::publication::crl_elt, 376
rpki::publication::manifest_elt, 378
rpki::publication::publication_-object_elt, 386
rpki::publication::roa_elt, 393
pdu
irbe_cli::left_right_sax_handler, 126
irbe_cli::publication_sax_handler, 141
rootd::sax_handler, 168
rpki::left_right::sax_handler, 342
rpki::publication::sax_handler, 395
rpki::up_down::sax_handler, 562
pdus
irbe_cli::left_right_msg, 123
irbe_cli::publication_msg, 138
rpki::left_right::msg, 325
rpki::publication::msg, 380
pem_converter
rpki::x509::CMS_object, 568
rpki::x509::CRL, 572
rpki::x509::DER_object, 584
rpki::x509::PKCS10, 591
rpki::x509::ROA, 593
rpki::x509::RSA, 598
rpki::x509::RSApublic, 601
rpki::x509::SignedManifest, 604
rpki::x509::X509, 609
pem_out
irbe_cli, 51
persistent
rpki::https::http_message, 263
pid
rpki::log, 83
rpki::x509::DeadDrop, 574
ping
rpki::sql::session, 494
pkcs10
rpki::up_down::issue_pdu, 539
pkcs10_request
rpki::left_right::bsc_elt, 297
PKIX_threshhold
rpki::sundial::datetime, 512
port
irdbd, 55
rootd, 63
POW
rpki::x509::CMS_object, 568
rpki::x509::CRL, 572
rpki::x509::RSA, 598
rpki::x509::RSApublic, 601
rpki::x509::X509, 610
POWify_OID
rpki::x509, 98
POWpkix
rpki::x509::CRL, 572
rpki::x509::PKCS10, 591
rpki::x509::X509, 610
prefix
rpki::resource_set::roa_prefix, 428
prefix_type
rpki::resource_set::roa_prefix_set_-ipv4, 438
rpki::resource_set::roa_prefix_set_-ipv6, 440
prefixlen

rpki::resource_set::roa_prefix, 429
pretty_print_content
rpki::x509::XML_CMS_object, 613
print_on_der_error
rpki::x509::CMS_object, 568
priority
rpki::log::logger, 352
private_key_id
rpki::left_right::bsc_elt, 297
rpki::rpki_engine::ca_detail_obj, 456
profile
pubd, 58
rpkid, 100
proto
rpki::https::caller, 251
pubd, 56
cfg_file, 58
main, 57
profile, 58
pubd.py(3107), 645
pubd::pubd_context, 151
__init__, 153
bpki_ta, 154
build_https_ta_cache, 153
clear_https_ta_cache, 153
client_handler, 154
client_url_regexp, 154
control_handler, 154
handler_common, 154
https_server_host, 155
https_server_port, 155
https_ta_cache, 155
irbe_cert, 155
pubd_cert, 155
pubd_key, 155
publication_base, 155
publication_multimodule, 156
sql, 156
pubd_cert
pubd::pubd_context, 155
pubd_key
pubd::pubd_context, 155
public_key
rpki::rpki_engine::ca_detail_obj, 457
publication
rpki::relaxng, 87
publication.py(3107), 645
publication_base
pubd::pubd_context, 155
publication_kludge_base
rpki::rpki_engine::rpkid_context, 490
publication_multimodule
pubd::pubd_context, 156
publish
rpki::rpki_engine::publication_-queue, 471
published
rpki::rpki_engine::child_cert_obj, 468
rpki::rpki_engine::roa_obj, 482
published_callback
rpki::rpki_engine::child_cert_obj, 467
rpki::rpki_engine::roa_obj, 479
pydatetime::datetime, 156
pydatetime::timedelta, 156

q_msg
irbe_cli, 51
q_msg_left_right
irbe_cli, 51
q_msg_publication
irbe_cli, 51
q_pdu
irbe_cli, 51
query
rpki::up_down::issue_pdu, 538
rpki::up_down::list_pdu, 544
rpki::up_down::revoke_pdu, 555
rpki::xml_utils::msg, 626
query_up_down
rpki::left_right::parent_elt, 328
queue
rpki::async::timer, 182
rpki::https::http_client, 257
rpki::https::http_queue, 268

raise_if_error

rpki::publication::publication_-object_elt, 385
rpki::publication::report_error_elt, 390
range_type
rpki::resource_set::resource_set_as, 418
rpki::resource_set::resource_set_-ipv4, 423
rpki::resource_set::resource_set_-ipv6, 425
rpki::resource_set::roa_prefix_ipv4, 431
rpki::resource_set::roa_prefix_ipv6, 433
read_attrs
rpki::xml_utils::base_elt, 617
readable
rpki::https::http_stream, 285
reason
rpki::https::http_response, 273
recipient
rpki::up_down::message_pdu, 550
recv
rpki::https::http_stream, 285
regen_margin
rpki::left_right::self_elt, 350
regenerate
rpki::rpki_engine::roa_obj, 479
regenerate_crls_and_manifests
rpki::left_right::self_elt, 346
regexp
rpki::sundial::timedelta, 517
reissue
rpki::rpki_engine::child_cert_obj, 467
rekey
rpki::rpki_engine::ca_obj, 462
relaxng.py(3110), 646
replace
rpki::rpki_engine::publication_-queue, 472
reply
rpki::xml_utils::msg, 627
repositories
rpki::left_right::bsc_elt, 296
rpki::left_right::self_elt, 346
rpki::rpki_engine::publication_-queue, 472
repository
rpki::left_right::parent_elt, 329
req_resource_set_as
rpki::up_down::certificate_elt, 523
rpki::up_down::issue_pdu, 539
req_resource_set_ipv4
rpki::up_down::certificate_elt, 523
rpki::up_down::issue_pdu, 539
req_resource_set_ipv6
rpki::up_down::certificate_elt, 523
rpki::up_down::issue_pdu, 539
request
rpki::https::http_queue, 266
require_crls
rpki::x509::CMS_object, 568
res
rpki::async::sync_wrapper, 176
resource_set.py(3107), 646
resource_set_as
rpki::up_down::class_elt, 527
resource_set_ipv4
rpki::up_down::class_elt, 527
resource_set_ipv6
rpki::up_down::class_elt, 527
resource_set_notafter
rpki::up_down::class_elt, 527
resource_set_type
rpki::resource_set::roa_prefix_set_-ipv4, 438
rpki::resource_set::roa_prefix_set_-ipv6, 440
restart
rpki::https::http_queue, 267
rpki::https::http_stream, 286
result
rpki::xml_utils::sax_handler, 631
retried
rpki::https::http_request, 271
retry_read
rpki::https::http_client, 257
rpki::https::http_server, 278
rpki::https::http_stream, 287
retry_write

rpki::https::http_client, 257
rpki::https::http_server, 278
rpki::https::http_stream, 287
return_result
rpki::https::http_queue, 267
revoke
rpki::rpki_engine::ca_detail_obj, 453
rpki::rpki_engine::ca_obj, 462
rpki::rpki_engine::child_cert_obj, 467
rpki::rpki_engine::revoked_cert_obj, 474
rpki::rpki_engine::roa_obj, 479
revoked
rpki::rpki_engine::revoked_cert_obj, 475
revoked_certs
rpki::rpki_engine::ca_detail_obj, 454
roa
rpki::rpki_engine::roa_obj, 482
roa.py(2424), 647
roas
rpki::left_right::self_elt, 346
rpki::rpki_engine::ca_detail_obj, 454
root_newer_than_subject
rootd, 61
rootd, 58
bpki_ta, 62
cfg, 62
cfg_file, 62
child_bpki_cert, 62
client_ta, 62
compose_response, 60
del_subject_cert, 60
del_subject_pkcs10, 60
get_root_cert, 60
get_subject_cert, 61
get_subject_pkcs10, 61
handlers, 62
host, 62
https_server_host, 63
https_server_port, 63
issue_subject_cert_maybe, 61
port, 63
root_newer_than_subject, 61
rootd_bpki_cert, 63
rootd_bpki_crl, 63
rootd_bpki_key, 63
rpki_base_uri, 63
rpki_class_name, 64
rpki_root_cert, 64
rpki_root_cert_file, 64
rpki_root_cert_uri, 64
rpki_root_crl, 64
rpki_root_dir, 64
rpki_root_key, 64
rpki_root_manifest, 65
rpki_subject_cert, 65
rpki_subject_lifetime, 65
rpki_subject_pkcs10, 65
rpki_subject_regen, 65
server_cert, 65
set_subject_cert, 61
set_subject_pkcs10, 61
up_down_handler, 61
rootd.py(2913), 647
rootd::cms_msg, 156
saxify, 158
rootd::issue_pdu, 158
serve_pdu, 160
rootd::list_pdu, 160
serve_pdu, 162
rootd::message_pdu, 162
log_query, 164
name2type, 164
type2name, 164
rootd::revoke_pdu, 165
serve_pdu, 166
rootd::sax_handler, 166
pdu, 168
rootd_bpki_cert
rootd, 63
rootd_bpki_crl
rootd, 63
rootd_bpki_key
rootd, 63
rpki, 66
rpki.__doc__, 66
rpki.async, 66

rpki.cli, 69
rpki.config, 70
rpki.exceptions, 71
rpki.https, 73
rpki.ipaddrs, 78
rpki.left_right, 79
rpki.log, 80
rpki.manifest, 83
rpki.oids, 84
rpki.publication, 86
rpki.relaxng, 87
rpki.resource_set, 87
rpki.roa, 90
rpki.rpki_engine, 91
rpki.sql, 92
rpki.sundial, 93
rpki.up_down, 95
rpki.x509, 96
rpki.xml_utils, 98
rpki::async
    _raiseExitNow, 67
    defer, 67
    deferred_queue, 68
    event_loop, 68
    exit_event_loop, 68
    ExitNow, 68
    run_deferred, 68
rpki::async::gc_summary, 168
    __init__, 169
    handler, 169
    interval, 169
    threshold, 169
    timer, 169
rpki::async::iterator, 170
    __call__, 171
    __init__, 171
    __repr__, 172
    caller_function, 172
    doit, 172
    done_callback, 172
    item_callback, 172
    iterator, 172
    unwind_stack, 173
rpki::async::sync_wrapper, 173
    __call__, 175
    __init__, 175
    cb, 175
    eb, 175
    err, 176
    func, 176
    res, 176
rpki::async::timer, 176
    __cmp__, 179
    __del__, 179
    __init__, 179
    __repr__, 179
    cancel, 179
    clear, 179
    errback, 179, 181
    gc_debug, 181
    handler, 180, 182
    is_set, 180
    queue, 182
    run_debug, 182
    runq, 180
    seconds_until_wakeup, 180
    set, 180
    set_errback, 181
    set_handler, 181
    trace, 181
    when, 182
rpki::cli
    _yes_or_no_prompts, 70
    have_readline, 70
    yes_or_no, 69
rpki::cli::Cmd, 182
    __init__, 184
    cmdloop_with_history, 184, 186
    complete_help, 184
    completenames, 185
    do_EOF, 185
    do_exit, 185
    do_quit, 186
    emptyline, 185
    emptyline_repeats_last_command, 186
    EOF_exits_command_loop, 187
    filename_complete, 185
    help_help, 186
    histfile, 187
    identchars, 187
    onecmd, 186

rpki::config::parser, 187
__init__, 189
_regexp, 191
_repl, 189
cfg, 191
default_section, 192
filename, 192
get, 190
getboolean, 190
getint, 190
getlong, 190
has_option, 190
has_section, 191
multiget, 191
set_global_flags, 191
rpki::exceptions::BadClassNameSyntax, 192
rpki::exceptions::BadClientURL, 193
rpki::exceptions::BadContactURL, 194
rpki::exceptions::BadExtension, 195
rpki::exceptions::BadIRDBReply, 196
rpki::exceptions::BadIssueResponse, 197
rpki::exceptions::BadPKCS10, 198
rpki::exceptions::BadPublicationReply, 199
rpki::exceptions::BadQuery, 200
rpki::exceptions::BadSender, 201
rpki::exceptions::BadStatusCode, 202
rpki::exceptions::BadURISyntax, 203
rpki::exceptions::BSCNotFound, 204
rpki::exceptions::BSCNotReady, 205
rpki::exceptions::ChildNotFound, 206
rpki::exceptions::ClassNameMismatch, 207
rpki::exceptions::ClassNameUnknown, 208
rpki::exceptions::ClientNotFound, 209
rpki::exceptions::CMSContentNotSet, 210
rpki::exceptions::CMSCRLNotSet, 212
rpki::exceptions::CMSVerificationFailed, 213
rpki::exceptions::DBConsistancyError, 214
rpki::exceptions::DERObjectConversionError, 215
rpki::exceptions::DuplicateObject, 216
rpki::exceptions::EmptyPEM, 217
rpki::exceptions::EmptyROAPrefixList, 218
rpki::exceptions::ForbiddenURI, 219
rpki::exceptions::HandleTranslationError, 220
rpki::exceptions::HTTPRequestFailed, 221
rpki::exceptions::HTTPSBadVersion, 222
rpki::exceptions::HTTPSClientAborted, 223
rpki::exceptions::HTTPSUnexpectedState, 224
rpki::exceptions::MissingCMSCRL, 225
rpki::exceptions::MissingCMSEEcert, 226
rpki::exceptions::MultipleTLSEECert, 227
rpki::exceptions::MustBePrefix, 228
rpki::exceptions::NoActiveCA, 229
rpki::exceptions::NoCoveringCertForROA, 230
rpki::exceptions::NoObjectAtURI, 231
rpki::exceptions::NotACertificateChain, 232
rpki::exceptions::NotFound, 233
rpki::exceptions::NotImplementedYet, 234
rpki::exceptions::NotInDatabase, 235
rpki::exceptions::ReceivedTLSCACert, 236
rpki::exceptions::RPKI_Exception, 238
rpki::exceptions::ServerShuttingDown, 239
rpki::exceptions::SKIMismatch, 240
rpki::exceptions::SubprocessError, 241
rpki::exceptions::TLSValidationError, 242
rpki::exceptions::UnexpectedCMSCerts, 244
rpki::exceptions::UnexpectedCMSCRLs, 245
rpki::exceptions::UnparsableCMSDER, 246
rpki::exceptions::UpstreamError, 247

rpki::exceptions::WrongEContentType, 248
rpki::https
build_https_ta_cache, 75
client, 75
client_queues, 76
debug_http, 76
debug_tls_certs, 76
default_client_timeout, 76
default_http_version, 76
default_server_timeout, 76
log_method, 75
rpki_content_type, 77
server, 75
supported_address_families, 77
want_persistent_client, 77
want_persistent_server, 77
rpki::https::caller, 249
__call__, 250
__init__, 250
client_cert, 250
client_key, 250
debug, 251
proto, 251
server_cert, 251
server_ta, 251
url, 251
rpki::https::http_client, 251
__init__, 253
af, 256
cert, 256
expect_close, 256
handle_close, 253
handle_connect, 254
handle_error, 254
handle_message, 254
handle_no_content_length, 254
handle_timeout, 255
hostport, 256
key, 256
parse_type, 256
queue, 257
retry_read, 257
retry_write, 257
send_request, 255
set_state, 255
start, 255
state, 257
ta, 257
timeout, 257
tls, 257
tls_connect, 255
rpki::https::http_listener, 258
__init__, 259
cert, 260
dynamic_ta, 260
handle_accept, 259
handle_error, 259
handlers, 260
key, 260
log, 260
ta, 260
rpki::https::http_message, 261
__init__, 262
__str__, 262
body, 264
format, 262
headers, 264
normalize_headers, 263
parse_from_wire, 263
parse_version, 263
persistent, 263
software_name, 264
version, 264
rpki::https::http_queue, 264
__init__, 266
cert, 267
client, 267
detach, 266
hostport, 268
key, 268
log, 268
queue, 268
request, 266
restart, 267
return_result, 267
send_request, 267
ta, 268
rpki::https::http_request, 268
__init__, 270
callback, 271
cmd, 271

errback, 271
format_first_line, 270
parse_first_line, 270
path, 271
retried, 271
rpki::https::http_response, 271
__init__, 273
code, 273
format_first_line, 273
parse_first_line, 273
reason, 273
rpki::https::http_server, 274
__init__, 276
expect_close, 278
find_handler, 276
handle_message, 276
handle_no_content_length, 277
handlers, 278
parse_type, 278
retry_read, 278
retry_write, 278
send_error, 277
send_message, 277
send_reply, 277
timeout, 279
tls, 279
tls_accept, 277
rpki::https::http_stream, 279
__init__, 282
buffer, 287
chunk_body, 282
chunk_discard_crlf, 282
chunk_discard_trailer, 282
chunk_handler, 287
chunk_header, 282
close, 282
collect_incoming_data, 283
found_terminator, 283
get_buffer, 283
handle_body, 283
handle_close, 284
handle_error, 284
handle_read, 284
handle_timeout, 284
handle_write, 285
initiate_send, 285
log, 287
log_cert, 285
msg, 287
readable, 285
recv, 285
restart, 286
retry_read, 287
retry_write, 287
send, 286
timer, 287
tls, 288
update_timeout, 286
writeable, 286
rpki::ipaddrs::v4addr, 288
__new__, 289
__str__, 289
bits, 290
from_bytes, 289
to_bytes, 289
rpki::ipaddrs::v6addr, 290
__new__, 292
__str__, 292
bits, 292
from_bytes, 292
to_bytes, 292
rpki::left_right
enforce_strict_up_down_xml_-sender, 80
rpki::left_right::bsc_elt, 293
attributes, 296
booleans, 296
children, 295
element_name, 297
elements, 297
handles, 297
parents, 295
pkcs10_request, 297
private_key_id, 297
repositories, 296
serve_pre_save_hook, 296
signing_cert, 297
signing_cert_crl, 298
sql_template, 298
rpki::left_right::child_elt, 298
attributes, 302
booleans, 302

bpki_cert, 302
bpki_glue, 302
ca_from_class_name, 300
child_certs, 300
clear_https_ta_cache, 302
element_name, 302
elements, 303
endElement, 301
handles, 303
parents, 301
serve_destroy_hook, 301
serve_post_save_hook, 301
serve_up_down, 301
sql_template, 303
rpki::left_right::cms_msg, 303
encoding, 305
saxify, 305
schema, 305
rpki::left_right::data_elt, 305
bsc, 307
handles, 309
make_reply_clone_hook, 307
self, 307
self_handle, 309
self_id, 309
serve_fetch_all, 308
serve_fetch_handle, 308
serve_fetch_one_maybe, 308
serve_pre_save_hook, 308
rpki::left_right::left_right_namespace, 309
nsmap, 310
xmlns, 310
rpki::left_right::list_published_objects_-elt, 311
attributes, 314
element_name, 314
make_reply, 313
obj, 314
serve_dispatch, 313
text_attribute, 314
rpki::left_right::list_received_resources_-elt, 314
attributes, 316
element_name, 316
make_reply, 316
serve_dispatch, 316
rpki::left_right::list_resources_elt, 317
asn, 320
attributes, 320
element_name, 320
ipv4, 320
ipv6, 320
startElement, 319
toXML, 319
valid_until, 320
rpki::left_right::list_roa_requests_elt, 321
attributes, 322
element_name, 322
ipv4, 323
ipv6, 323
startElement, 322
rpki::left_right::msg, 323
pdus, 325
serve_top_level, 325
version, 325
rpki::left_right::parent_elt, 326
attributes, 330
booleans, 330
bpki_cms_cert, 330
bpki_cms_glue, 330
bpki_https_cert, 331
bpki_https_glue, 331
cas, 328
element_name, 331
elements, 331
handles, 331
query_up_down, 328
repository, 329
serve_post_save_hook, 329
serve_rekey, 329
serve_revoke, 329
serve_revoke_forgotten, 329
sql_template, 331
rpki::left_right::report_error_elt, 332
attributes, 335
element_name, 335
error_code, 335
error_text, 335
from_exception, 334
self_handle, 335
tag, 335

text_attribute, 335
rpki::left_right::repository_elt, 336
attributes, 339
bpki_cert, 339
bpki_glue, 339
call_pubd, 338
default_pubd_handler, 338
element_name, 339
elements, 340
handles, 340
parents, 339
sql_template, 340
rpki::left_right::sax_handler, 340
name, 342
pdu, 342
version, 342
rpki::left_right::self_elt, 342
attributes, 349
booleans, 349
bpki_cert, 349
bpki_glue, 349
bscs, 345
children, 345
client_poll, 345
crl_interval, 350
cron, 345
element_name, 350
elements, 350
handles, 350
parents, 345
regen_margin, 350
regenerate_crls_and_manifests, 346
repositories, 346
roas, 346
serve_fetch_all, 346
serve_fetch_handle, 347
serve_fetch_one_maybe, 347
serve_post_save_hook, 347
serve_publish_world_now, 347
serve_rekey, 348
serve_revoke, 348
serve_revoke_forgotten, 348
serve_run_now, 348
sql_template, 350
update_children, 348
update_roas, 349
use_hsm, 351
rpki::log
debug, 82
enable_trace, 82
error, 82
info, 82
init, 81
note, 83
pid, 83
set_trace, 81
tag, 83
trace, 82
traceback, 82
use_syslog, 83
warn, 83
rpki::log::logger, 351
__call__, 352
__init__, 352
priority, 352
rpki::manifest::FileAndHash, 353
__init__, 354
file, 354
hash, 354
rpki::manifest::FilesAndHashes, 354
__init__, 355
rpki::manifest::Manifest, 356
__init__, 357
explicitVersion, 357
fileHashAlg, 357
fileList, 357
manifestNumber, 357
nextUpdate, 357
thisUpdate, 358
version, 358
rpki::oids
name2oid, 85
oid2name, 85
rpki::publication::certificate_elt, 358
element_name, 360
payload_type, 360
rpki::publication::client_elt, 360
attributes, 363
base_uri, 363
bpki_cert, 364
bpki_glue, 364
check_allowed_uri, 362

clear_https_ta_cache, 364
element_name, 364
elements, 364
endElement, 362
serve_fetch_all, 363
serve_fetch_one_maybe, 363
serve_post_save_hook, 363
sql_template, 364
rpki::publication::cms_msg, 365
encoding, 367
saxify, 367
schema, 367
rpki::publication::config_elt, 367
attributes, 370
config_id, 370
element_name, 371
elements, 371
fetch, 369
serve_fetch_one_maybe, 369
serve_set, 370
sql_template, 371
startElement, 370
wired_in_config_id, 371
rpki::publication::control_elt, 371
serve_dispatch, 374
rpki::publication::crl_elt, 374
element_name, 376
payload_type, 376
rpki::publication::manifest_elt, 376
element_name, 378
payload_type, 378
rpki::publication::msg, 378
pdus, 380
serve_top_level, 380
version, 380
rpki::publication::publication_-namespace, 381
nsmap, 382
xmlns, 382
rpki::publication::publication_object_elt, 382
attributes, 386
endElement, 384
make_publish, 384
make_withdraw, 385
payload, 386
payload_type, 386
raise_if_error, 385
serve_dispatch, 385
serve_publish, 385
serve_withdraw, 385
toXML, 386
uri_to_filename, 386
rpki::publication::report_error_elt, 387
__str__, 389
attributes, 390
element_name, 390
error_code, 390
error_text, 390
from_exception, 389
raise_if_error, 390
tag, 391
text_attribute, 391
rpki::publication::roa_elt, 391
element_name, 393
payload_type, 393
rpki::publication::sax_handler, 393
name, 395
pdu, 395
version, 395
rpki::relaxng
left_right, 87
publication, 87
up_down, 87
rpki::resource_set
_bs2long, 89
_long2bs, 89
_rsplit, 89
inherit_token, 90
test1, 90
test2, 90
rpki::resource_set::resource_bag, 395
__eq__, 397
__init__, 397
__ne__, 397
__str__, 398
asn, 399
empty, 398
from_rfc3779_tuples, 398
intersection, 398
oversized, 398
undersized, 398

union, 399
v4, 399
v6, 399
valid_until, 399
rpki::resource_set::resource_range, 400
__cmp__, 401
__init__, 401
max, 401
min, 401
rpki::resource_set::resource_range_as, 402
__str__, 403
datum_type, 403
min, 404
to_rfc3779_tuple, 403
rpki::resource_set::resource_range_ip, 404
__str__, 406
_prefixlen, 406
make_prefix, 406
to_rfc3779_tuple, 406
rpki::resource_set::resource_range_ipv4, 407
datum_type, 409
rpki::resource_set::resource_range_ipv6, 409
datum_type, 411
rpki::resource_set::resource_set, 411
__init__, 413
__str__, 413
_comm, 413
contains, 414
difference, 414
from_sql, 414
inherit, 415
intersection, 414
issubset, 414
issuperset, 415
symmetric_difference, 415
union, 415
rpki::resource_set::resource_set_as, 416
inherit, 418
parse_rfc3779_tuple, 417
parse_str, 417
range_type, 418
to_rfc3779_tuple, 417
rpki::resource_set::resource_set_ip, 418
inherit, 421
parse_rfc3779_tuple, 420
parse_str, 420
to_rfc3779_tuple, 420
rpki::resource_set::resource_set_ipv4, 421
afi, 423
range_type, 423
rpki::resource_set::resource_set_ipv6, 423
afi, 425
range_type, 425
rpki::resource_set::roa_prefix, 425
__cmp__, 427
__init__, 427
__str__, 427
max, 427
max_prefixlen, 428
min, 428
prefix, 428
prefixlen, 429
to_resource_range, 428
to_roa_tuple, 428
rpki::resource_set::roa_prefix_ipv4, 429
range_type, 431
rpki::resource_set::roa_prefix_ipv6, 431
range_type, 433
rpki::resource_set::roa_prefix_set, 433
__init__, 435
__str__, 435
from_sql, 435
parse_str, 435
to_resource_set, 435
to_roa_tuple, 436
rpki::resource_set::roa_prefix_set_ipv4, 436
prefix_type, 438
resource_set_type, 438
rpki::resource_set::roa_prefix_set_ipv6, 438
prefix_type, 440
resource_set_type, 440
rpki::roa::ROAIPAddress, 440
__init__, 441
address, 442

maxLength, 442
rpki::roa::ROAIPAddresses, 442
__init__, 443
rpki::roa::ROAIPAddressFamilies, 443
__init__, 444
rpki::roa::ROAIPAddressFamily, 444
__init__, 445
addresses, 446
addressFamily, 446
rpki::roa::RouteOriginAttestation, 446
__init__, 447
asID, 447
explicitVersion, 447
ipAddrBlocks, 447
version, 447
rpki::rpki_engine::ca_detail_obj, 448
activate, 451
ca, 451
ca_cert_uri, 455
ca_id, 455
child_certs, 451
create, 451
crl_published, 455
crl_published_callback, 451
crl_uri, 451
crl_uri_tail, 452
delete, 452
gctx, 455
generate_crl, 452
generate_manifest, 452
generate_manifest_cert, 452
issue, 453
issue_ee, 453
latest_ca_cert, 455
latest_crl, 455
latest_manifest, 456
latest_manifest_cert, 456
manifest_private_key_id, 456
manifest_public_key, 456
manifest_published, 456
manifest_published_callback, 453
manifest_uri, 453
nextUpdate, 456
private_key_id, 456
public_key, 457
revoke, 453
revoked_certs, 454
roas, 454
sql_decode, 454
sql_template, 457
state, 457
update, 454
rpki::rpki_engine::ca_obj, 457
ca_details, 459
check_for_updates, 459
construct_sia_uri, 460
create, 460
delete, 460
fetch_active, 460
fetch_deprecated, 461
fetch_issue_response_candidates, 461
fetch_pending, 461
fetch_revoked, 461
gctx, 463
last_crl_sn, 463
last_issued_sn, 463
last_manifest_sn, 463
next_crl_number, 461
next_manifest_number, 462
next_serial_number, 462
parent, 462
parent_id, 463
parent_resource_class, 463
rekey, 462
revoke, 462
sia_uri, 464
sql_template, 464
rpki::rpki_engine::child_cert_obj, 464
__init__, 466
ca_detail, 466
ca_detail_id, 468
cert, 468
child, 466
child_id, 468
fetch, 467
gctx, 468
published, 468
published_callback, 467
reissue, 467
revoke, 467
sql_template, 469

uri, 467
uri_tail, 468
rpki::rpki_engine::publication_queue, 469
__init__, 471
_add, 471
call_pubd, 471
handlers, 472
msgs, 472
publish, 471
replace, 472
repositories, 472
uris, 472
withdraw, 472
rpki::rpki_engine::revoked_cert_obj, 473
__init__, 474
ca_detail, 474
ca_detail_id, 475
expires, 475
gctx, 475
revoke, 474
revoked, 475
serial, 475
sql_template, 475
rpki::rpki_engine::roa_obj, 476
__init__, 478
asn, 481
ca_detail, 478
ca_detail_id, 481
cert, 481
gctx, 482
generate, 479
ipv4, 482
ipv6, 482
published, 482
published_callback, 479
regenerate, 479
revoke, 479
roa, 482
self, 480
self_id, 482
sql_delete_hook, 480
sql_fetch_hook, 480
sql_insert_hook, 480
sql_template, 482
update, 481
uri, 481
uri_tail, 481
rpki::rpki_engine::rpkid_context, 483
__init__, 486
bpki_ta, 488
build_https_ta_cache, 486
checkpoint, 486
clear_https_ta_cache, 486
cron, 486
cron_keepalive, 488
cron_period, 488
cron_timeout, 488
cron_timer, 488
cronjob_handler, 486
https_server_host, 489
https_server_port, 489
https_ta_cache, 489
initial_delay, 489
irbe_cert, 489
irdb_cert, 489
irdb_query, 487
irdb_query_child_resources, 487
irdb_query_roa_requests, 487
irdb_url, 489
left_right_handler, 487
publication_kludge_base, 490
rpkid_cert, 490
rpkid_key, 490
sql, 490
start_cron, 487
up_down_handler, 488
up_down_url_regexp, 490
use_internal_cron, 490
rpki::sql::session, 491
__init__, 493
_exceptions_enabled, 494
_wrap_execute, 493
assert_pristine, 493
cache, 495
cache_clear, 493
close, 493
connect, 493
cur, 495
database, 495
db, 495
dirty, 495

execute, 493
executemany, 494
fetchall, 494
lastrowid, 494
password, 495
ping, 494
sweep, 494
username, 495
rpki::sql::sql_persistent, 496
gctx, 502
sql_debug, 502
sql_decode, 498
sql_delete, 499
sql_delete_hook, 499
sql_deleted, 502
sql_encode, 499
sql_fetch, 499
sql_fetch_all, 500
sql_fetch_hook, 500
sql_fetch_where, 500
sql_fetch_where1, 500
sql_in_db, 503
sql_init, 500
sql_insert_hook, 501
sql_is_dirty, 501
sql_mark_clean, 501
sql_mark_deleted, 501
sql_mark_dirty, 501
sql_store, 502
sql_update_hook, 502
rpki::sql::template, 503
__init__, 505
columns, 505
delete, 505
index, 505
insert, 505
map, 506
select, 506
table, 506
update, 506
rpki::sundial
_cast, 94
now, 94
test, 94
rpki::sundial::datetime, 506
__add__, 508
__radd__, 508
__rsub__, 508
__str__, 509
__sub__, 509
earlier, 509
from_sql, 509
fromASN1tuple, 509
fromdatetime, 509
fromGeneralizedTime, 510
fromUTCTime, 510
fromXMLtime, 510
later, 510
PKIX_threshhold, 512
to_sql, 510
toASN1tuple, 511
toGeneralizedTime, 511
totimestamp, 511
toUTCTime, 511
toXMLtime, 511
rpki::sundial::timedelta, 512
__abs__, 515
__add__, 515
__div__, 515
__floordiv__, 515
__mul__, 515
__neg__, 515
__pos__, 515
__radd__, 515
__rdiv__, 516
__rfloordiv__, 516
__rmul__, 516
__rsub__, 516
__sub__, 516
convert_to_seconds, 516
fromtimedelta, 516
parse, 517
regexp, 517
years_to_seconds, 517
rpki::up_down
nsmap, 96
xmlns, 96
rpki::up_down::base_elt, 518
check_response, 519
endElement, 519
make_b64elt, 519
make_elt, 519

serve_pdu, 520
startElement, 520
rpki::up_down::certificate_elt, 520
cert, 523
cert_url, 523
endElement, 522
req_resource_set_as, 523
req_resource_set_ipv4, 523
req_resource_set_ipv6, 523
startElement, 522
toXML, 522
rpki::up_down::class_elt, 523
__init__, 525
cert_url, 526
certs, 526
class_name, 526
endElement, 525
from_resource_bag, 525
issuer, 527
resource_set_as, 527
resource_set_ipv4, 527
resource_set_ipv6, 527
resource_set_notafter, 527
startElement, 526
suggested_sia_head, 527
to_resource_bag, 526
toXML, 526
rpki::up_down::class_response_syntax, 528
__init__, 529
classes, 530
startElement, 529
toXML, 529
rpki::up_down::cms_msg, 530
encoding, 532
saxify, 532
schema, 532
rpki::up_down::error_response_pdu, 532
__init__, 534
check_response, 534
codes, 535
description, 535
endElement, 534
exceptions, 535
status, 535
toXML, 535
rpki::up_down::issue_pdu, 536
class_name, 539
endElement, 538
pkcs10, 539
query, 538
req_resource_set_as, 539
req_resource_set_ipv4, 539
req_resource_set_ipv6, 539
serve_pdu, 538
startElement, 538
toXML, 539
rpki::up_down::issue_response_pdu, 540
check_response, 542
rpki::up_down::list_pdu, 542
query, 544
serve_pdu, 544
toXML, 544
rpki::up_down::list_response_pdu, 545
rpki::up_down::message_pdu, 546
__str__, 548
log_query, 548
make_query, 548
name2type, 550
payload, 550
recipient, 550
sender, 550
serve_error, 549
serve_top_level, 549
startElement, 549
toXML, 549
type, 550
type2name, 550
version, 551
rpki::up_down::multi_uri, 551
__init__, 552
__str__, 553
rsync, 553
rpki::up_down::revoke_pdu, 553
class_name, 556
get_SKI, 555
query, 555
serve_pdu, 555
ski, 556
rpki::up_down::revoke_response_pdu, 556
rpki::up_down::revoke_syntax, 558

class_name, 559
ski, 559
startElement, 559
toXML, 559
rpki::up_down::sax_handler, 560
name, 562
pdu, 562
version, 562
rpki::x509
_find_xia_uri, 98
calculate_SKI, 98
POWify_OID, 98
rpki::x509::CMS_object, 562
content, 566
debug_cms_certs, 566
DER, 567
dump_on_verify_failure, 567
econtent_oid, 567
extract, 565
formats, 567
get_content, 565
get_DER, 565
get_POW, 565
other_clear, 567
pem_converter, 568
POW, 568
print_on_der_error, 568
require_crls, 568
set_content, 566
sign, 566
verify, 566
rpki::x509::CRL, 569
DER, 572
formats, 572
generate, 570
get_DER, 570
get_POW, 571
get_POWpkix, 571
getIssuer, 571
getNextUpdate, 571
getThisUpdate, 571
pem_converter, 572
POW, 572
POWpkix, 572
rpki::x509::DeadDrop, 573
__init__, 574
dump, 574
maildir, 574
pid, 574
rpki::x509::DER_CMS_object, 575
content, 576
decode, 576
encode, 576
rpki::x509::DER_object, 577
__cmp__, 579
__init__, 579
clear, 579
DER, 584
dumpasn1, 579
empty, 579
formats, 584
from_sql, 580
gAKI, 580
get_3779resources, 580
get_AIA, 580
get_aia_uri, 580
get_AKI, 581
get_Base64, 581
get_basicConstraints, 581
get_DER, 581
get_PEM, 581
get_SIA, 582
get_sia_directory_uri, 582
get_sia_manifest_uri, 582
get_SKI, 582
gSKI, 582
hAKI, 583
hSKI, 583
is_CA, 583
other_clear, 584
pem_converter, 584
set, 583
to_sql, 583
rpki::x509::PEM_converter, 585
__init__, 586
b, 587
e, 587
looks_like_PEM, 586
to_DER, 586
to_PEM, 586
rpki::x509::PKCS10, 587
check_valid_rpki, 589

create, 589
create_ca, 589
DER, 590
formats, 590
get_DER, 590
get_POWpkix, 590
getPublicKey, 590
pem_converter, 591
POWpkix, 591
rpki::x509::ROA, 591
build, 593
content_class, 593
econtent_oid, 593
pem_converter, 593
rpki::x509::RSA, 594
DER, 597
formats, 597
generate, 596
get_DER, 596
get_POW, 596
get_public_DER, 597
get_RSApublic, 597
get_SKI, 597
pem_converter, 598
POW, 598
rpki::x509::RSApublic, 598
DER, 601
formats, 601
get_DER, 600
get_POW, 600
get_SKI, 600
pem_converter, 601
POW, 601
rpki::x509::SignedManifest, 602
build, 603
content_class, 604
econtent_oid, 604
getNextUpdate, 603
getThisUpdate, 603
pem_converter, 604
rpki::x509::X509, 604
cross_certify, 606
DER, 609
expired, 607
formats, 609
get_DER, 607
get_POW, 607
get_POWpkix, 607
getIssuer, 607
getNotAfter, 607
getNotBefore, 608
getPublicKey, 608
getSerial, 608
getSubject, 608
issue, 608
normalize_chain, 609
pem_converter, 609
POW, 610
POWpkix, 610
rpki::x509::XML_CMS_object, 610
content, 614
decode, 612
dump_inbound_cms, 614
dump_outbound_cms, 614
dump_to_disk, 612
econtent_oid, 614
encode, 612
pretty_print_content, 613
schema_check, 613
unwrap, 613
wrap, 613
rpki::xml_utils::base_elt, 614
__str__, 616
attributes, 618
booleans, 618
elements, 618
endElement, 616
make_b64elt, 617
make_elt, 617
make_pdu, 617
read_attrs, 617
startElement, 617
toXML, 618
rpki::xml_utils::data_elt, 619
endElement, 621
make_reply, 621
make_reply_clone_hook, 621
serve_create, 622
serve_destroy, 622
serve_destroy_hook, 622
serve_dispatch, 622
serve_fetch_one, 622

serve_get, 623
serve_list, 623
serve_post_save_hook, 623
serve_pre_save_hook, 623
serve_set, 623
toXML, 624
unimplemented_control, 624
rpki::xml_utils::msg, 624
__str__, 626
endElement, 626
is_query, 626
is_reply, 626
query, 626
reply, 627
startElement, 627
toXML, 627
type, 627
version, 627
rpki::xml_utils::sax_handler, 628
__init__, 629
characters, 629
create_top_level, 630
endElement, 630
endElementNS, 630
result, 631
saxify, 630
stack, 631
startElement, 630
startElementNS, 631
text, 631
rpki::xml_utils::text_elt, 632
endElement, 633
text_attribute, 633
toXML, 633
rpki_base_uri
rootd, 63
rpki_class_name
rootd, 64
rpki_content_type
rpki::https, 77
rpki_engine.py(3107), 649
rpki_root_cert
rootd, 64
rpki_root_cert_file
rootd, 64
rpki_root_cert_uri
rootd, 64
rpki_root_crl
rootd, 64
rpki_root_dir
rootd, 64
rpki_root_key
rootd, 64
rpki_root_manifest
rootd, 65
rpki_subject_cert
rootd, 65
rpki_subject_lifetime
rootd, 65
rpki_subject_pkcs10
rootd, 65
rpki_subject_regen
rootd, 65
rpkid, 99
cfg_file, 100
main, 100
profile, 100
rpkid.py(2913), 649
rpkid_cert
irdbd, 56
rpki::rpki_engine::rpkid_context, 490
rpkid_key
rpki::rpki_engine::rpkid_context, 490
rsync
rpki::up_down::multi_uri, 553
run_debug
rpki::async::timer, 182
run_deferred
rpki::async, 68
runq
rpki::async::timer, 180

saxify
irbe_cli::left_right_cms_msg, 121
irbe_cli::publication_cms_msg, 136
rootd::cms_msg, 158
rpki::left_right::cms_msg, 305
rpki::publication::cms_msg, 367
rpki::up_down::cms_msg, 532
rpki::xml_utils::sax_handler, 630

schema
rpki::left_right::cms_msg, 305
rpki::publication::cms_msg, 367
rpki::up_down::cms_msg, 532
schema_check
rpki::x509::XML_CMS_object, 613
seconds_until_wakeup
rpki::async::timer, 180
select
rpki::sql::template, 506
self
rpki::left_right::data_elt, 307
rpki::rpki_engine::roa_obj, 480
self_handle
rpki::left_right::data_elt, 309
rpki::left_right::report_error_elt, 335
self_id
rpki::left_right::data_elt, 309
rpki::rpki_engine::roa_obj, 482
send
rpki::https::http_stream, 286
send_error
rpki::https::http_server, 277
send_message
rpki::https::http_server, 277
send_reply
rpki::https::http_server, 277
send_request
rpki::https::http_client, 255
rpki::https::http_queue, 267
sender
rpki::up_down::message_pdu, 550
Sequence, 634
SequenceOf, 634
serial
rpki::rpki_engine::revoked_cert_obj, 475
serve_create
rpki::xml_utils::data_elt, 622
serve_destroy
rpki::xml_utils::data_elt, 622
serve_destroy_hook
rpki::left_right::child_elt, 301
rpki::xml_utils::data_elt, 622
serve_dispatch
rpki::left_right::list_published_-objects_elt, 313
rpki::left_right::list_received_-resources_elt, 316
rpki::publication::control_elt, 374
rpki::publication::publication_-object_elt, 385
rpki::xml_utils::data_elt, 622
serve_error
rpki::up_down::message_pdu, 549
serve_fetch_all
rpki::left_right::data_elt, 308
rpki::left_right::self_elt, 346
rpki::publication::client_elt, 363
serve_fetch_handle
rpki::left_right::data_elt, 308
rpki::left_right::self_elt, 347
serve_fetch_one
rpki::xml_utils::data_elt, 622
serve_fetch_one_maybe
rpki::left_right::data_elt, 308
rpki::left_right::self_elt, 347
rpki::publication::client_elt, 363
rpki::publication::config_elt, 369
serve_get
rpki::xml_utils::data_elt, 623
serve_list
rpki::xml_utils::data_elt, 623
serve_pdu
rootd::issue_pdu, 160
rootd::list_pdu, 162
rootd::revoke_pdu, 166
rpki::up_down::base_elt, 520
rpki::up_down::issue_pdu, 538
rpki::up_down::list_pdu, 544
rpki::up_down::revoke_pdu, 555
serve_post_save_hook
rpki::left_right::child_elt, 301
rpki::left_right::parent_elt, 329
rpki::left_right::self_elt, 347
rpki::publication::client_elt, 363
rpki::xml_utils::data_elt, 623
serve_pre_save_hook
rpki::left_right::bsc_elt, 296
rpki::left_right::data_elt, 308
rpki::xml_utils::data_elt, 623

serve_publish
rpki::publication::publication_-object_elt, 385
serve_publish_world_now
rpki::left_right::self_elt, 347
serve_rekey
rpki::left_right::parent_elt, 329
rpki::left_right::self_elt, 348
serve_revoke
rpki::left_right::parent_elt, 329
rpki::left_right::self_elt, 348
serve_revoke_forgotten
rpki::left_right::parent_elt, 329
rpki::left_right::self_elt, 348
serve_run_now
rpki::left_right::self_elt, 348
serve_set
rpki::publication::config_elt, 370
rpki::xml_utils::data_elt, 623
serve_top_level
rpki::left_right::msg, 325
rpki::publication::msg, 380
rpki::up_down::message_pdu, 549
serve_up_down
rpki::left_right::child_elt, 301
serve_withdraw
rpki::publication::publication_-object_elt, 385
server
rpki::https, 75
server_cert
irdbd, 56
rootd, 65
rpki::https::caller, 251
server_ta
rpki::https::caller, 251
set
rpki::async::timer, 180
rpki::x509::DER_object, 583
set_content
rpki::x509::CMS_object, 566
set_errback
rpki::async::timer, 181
set_global_flags
rpki::config::parser, 191
set_handler
rpki::async::timer, 181
set_state
rpki::https::http_client, 255
set_subject_cert
rootd, 61
set_subject_pkcs10
rootd, 61
set_trace
rpki::log, 81
sia_uri
rpki::rpki_engine::ca_obj, 464
sign
rpki::x509::CMS_object, 566
signing_cert
irbe_cli::bsc_elt, 104
rpki::left_right::bsc_elt, 297
signing_cert_crl
irbe_cli::bsc_elt, 104
rpki::left_right::bsc_elt, 298
ski
rpki::up_down::revoke_pdu, 556
rpki::up_down::revoke_syntax, 559
software_name
rpki::https::http_message, 264
sql
pubd::pubd_context, 156
rpki::rpki_engine::rpkid_context, 490
sql.py(2895), 650
sql_debug
rpki::sql::sql_persistent, 502
sql_decode
rpki::rpki_engine::ca_detail_obj, 454
rpki::sql::sql_persistent, 498
sql_delete
rpki::sql::sql_persistent, 499
sql_delete_hook
rpki::rpki_engine::roa_obj, 480
rpki::sql::sql_persistent, 499
sql_deleted
rpki::sql::sql_persistent, 502
sql_encode
rpki::sql::sql_persistent, 499
sql_fetch
rpki::sql::sql_persistent, 499

sql_fetch_all
rpki::sql::sql_persistent, 500
sql_fetch_hook
rpki::rpki_engine::roa_obj, 480
rpki::sql::sql_persistent, 500
sql_fetch_where
rpki::sql::sql_persistent, 500
sql_fetch_where1
rpki::sql::sql_persistent, 500
sql_in_db
rpki::sql::sql_persistent, 503
sql_init
rpki::sql::sql_persistent, 500
sql_insert_hook
rpki::rpki_engine::roa_obj, 480
rpki::sql::sql_persistent, 501
sql_is_dirty
rpki::sql::sql_persistent, 501
sql_mark_clean
rpki::sql::sql_persistent, 501
sql_mark_deleted
rpki::sql::sql_persistent, 501
sql_mark_dirty
rpki::sql::sql_persistent, 501
sql_store
rpki::sql::sql_persistent, 502
sql_template
rpki::left_right::bsc_elt, 298
rpki::left_right::child_elt, 303
rpki::left_right::parent_elt, 331
rpki::left_right::repository_elt, 340
rpki::left_right::self_elt, 350
rpki::publication::client_elt, 364
rpki::publication::config_elt, 371
rpki::rpki_engine::ca_detail_obj, 457
rpki::rpki_engine::ca_obj, 464
rpki::rpki_engine::child_cert_obj, 469
rpki::rpki_engine::revoked_cert_obj, 475
rpki::rpki_engine::roa_obj, 482
sql_update_hook
rpki::sql::sql_persistent, 502
stack
rpki::xml_utils::sax_handler, 631
start
rpki::https::http_client, 255
start_cron
rpki::rpki_engine::rpkid_context, 487
startElement
rpki::left_right::list_resources_elt, 319
rpki::left_right::list_roa_requests_-elt, 322
rpki::publication::config_elt, 370
rpki::up_down::base_elt, 520
rpki::up_down::certificate_elt, 522
rpki::up_down::class_elt, 526
rpki::up_down::class_response_-syntax, 529
rpki::up_down::issue_pdu, 538
rpki::up_down::message_pdu, 549
rpki::up_down::revoke_syntax, 559
rpki::xml_utils::base_elt, 617
rpki::xml_utils::msg, 627
rpki::xml_utils::sax_handler, 630
startElementNS
rpki::xml_utils::sax_handler, 631
startup_msg
irdbd, 56
state
rpki::https::http_client, 257
rpki::rpki_engine::ca_detail_obj, 457
status
rpki::up_down::error_response_pdu, 535
suggested_sia_head
rpki::up_down::class_elt, 527
sundial.py(3191), 650
supported_address_families
rpki::https, 77
sweep
rpki::sql::session, 494
symmetric_difference
rpki::resource_set::resource_set, 415

ta
rpki::https::http_client, 257
rpki::https::http_listener, 260

rpki::https::http_queue, 268
table
rpki::sql::template, 506
tag
rpki::left_right::report_error_elt, 335
rpki::log, 83
rpki::publication::report_error_elt, 391
test
rpki::sundial, 94
test1
rpki::resource_set, 90
test2
rpki::resource_set, 90
text
rpki::xml_utils::sax_handler, 631
text_attribute
rpki::left_right::list_published_-objects_elt, 314
rpki::left_right::report_error_elt, 335
rpki::publication::report_error_elt, 391
rpki::xml_utils::text_elt, 633
textwrap::TextWrapper, 634
thisUpdate
rpki::manifest::Manifest, 358
threshold
rpki::async::gc_summary, 169
timeout
rpki::https::http_client, 257
rpki::https::http_server, 279
timer
rpki::async::gc_summary, 169
rpki::https::http_stream, 287
tls
rpki::https::http_client, 257
rpki::https::http_server, 279
rpki::https::http_stream, 288
tls_accept
rpki::https::http_server, 277
tls_connect
rpki::https::http_client, 255
to_bytes
rpki::ipaddrs::v4addr, 289
rpki::ipaddrs::v6addr, 292
to_DER
rpki::x509::PEM_converter, 586
to_PEM
rpki::x509::PEM_converter, 586
to_resource_bag
rpki::up_down::class_elt, 526
to_resource_range
rpki::resource_set::roa_prefix, 428
to_resource_set
rpki::resource_set::roa_prefix_set, 435
to_rfc3779_tuple
rpki::resource_set::resource_range_-as, 403
rpki::resource_set::resource_range_-ip, 406
rpki::resource_set::resource_set_as, 417
rpki::resource_set::resource_set_ip, 420
to_roa_tuple
rpki::resource_set::roa_prefix, 428
rpki::resource_set::roa_prefix_set, 436
to_sql
rpki::sundial::datetime, 510
rpki::x509::DER_object, 583
toASN1tuple
rpki::sundial::datetime, 511
toGeneralizedTime
rpki::sundial::datetime, 511
top_opts
irbe_cli, 51
totimestamp
rpki::sundial::datetime, 511
toUTCTime
rpki::sundial::datetime, 511
toXML
rpki::left_right::list_resources_elt, 319
rpki::publication::publication_-object_elt, 386
rpki::up_down::certificate_elt, 522
rpki::up_down::class_elt, 526
rpki::up_down::class_response_-syntax, 529

rpki::up_down::error_response_pdu, 535
rpki::up_down::issue_pdu, 539
rpki::up_down::list_pdu, 544
rpki::up_down::message_pdu, 549
rpki::up_down::revoke_syntax, 559
rpki::xml_utils::base_elt, 618
rpki::xml_utils::data_elt, 624
rpki::xml_utils::msg, 627
rpki::xml_utils::text_elt, 633
toXMLtime
rpki::sundial::datetime, 511
trace
rpki::async::timer, 181
rpki::log, 82
traceback
rpki::log, 82
type
rpki::up_down::message_pdu, 550
rpki::xml_utils::msg, 627
type2name
rootd::message_pdu, 164
rpki::up_down::message_pdu, 550

u
irdbd, 56
undersized
rpki::resource_set::resource_bag, 398
unimplemented_control
rpki::xml_utils::data_elt, 624
union
rpki::resource_set::resource_bag, 399
rpki::resource_set::resource_set, 415
unwind_stack
rpki::async::iterator, 173
unwrap
rpki::x509::XML_CMS_object, 613
up_down
rpki::relaxng, 87
up_down.py(3162), 650
up_down_handler
rootd, 61
rpki::rpki_engine::rpkid_context, 488
up_down_url_regexp
rpki::rpki_engine::rpkid_context, 490
update
rpki::rpki_engine::ca_detail_obj, 454
rpki::rpki_engine::roa_obj, 481
rpki::sql::template, 506
update_children
rpki::left_right::self_elt, 348
update_roas
rpki::left_right::self_elt, 349
update_timeout
rpki::https::http_stream, 286
uri
rpki::rpki_engine::child_cert_obj, 467
rpki::rpki_engine::roa_obj, 481
uri_tail
rpki::rpki_engine::child_cert_obj, 468
rpki::rpki_engine::roa_obj, 481
uri_to_filename
rpki::publication::publication_-object_elt, 386
uris
rpki::rpki_engine::publication_-queue, 472
url
rpki::https::caller, 251
usage
irbe_cli, 50
irbe_cli::cmd_elt_mixin, 113
irbe_cli::cmd_msg_mixin, 116
usage_fill
irbe_cli, 52
use_hsm
rpki::left_right::self_elt, 351
use_internal_cron
rpki::rpki_engine::rpkid_context, 490
use_syslog
rpki::log, 83
username
rpki::sql::session, 495

v4
rpki::resource_set::resource_bag, 399
v6
rpki::resource_set::resource_bag, 399
valid_until
rpki::left_right::list_resources_elt, 320
rpki::resource_set::resource_bag, 399
verbose
irbe_cli, 52
verify
rpki::x509::CMS_object, 566
version
rpki::https::http_message, 264
rpki::left_right::msg, 325
rpki::left_right::sax_handler, 342
rpki::manifest::Manifest, 358
rpki::publication::msg, 380
rpki::publication::sax_handler, 395
rpki::roa::RouteOriginAttestation, 447
rpki::up_down::message_pdu, 551
rpki::up_down::sax_handler, 562
rpki::xml_utils::msg, 627

want_persistent_client
rpki::https, 77
want_persistent_server
rpki::https, 77
warn
rpki::log, 83
when
rpki::async::timer, 182
wired_in_config_id
rpki::publication::config_elt, 371
withdraw
rpki::rpki_engine::publication_queue, 472
wrap
rpki::x509::XML_CMS_object, 613
writeable
rpki::https::http_stream, 286
x509.py(3107), 651
xml::sax::handler::ContentHandler, 634
xml_utils.py(2836), 652
xmlns
rpki::left_right::left_right_namespace, 310
rpki::publication::publication_namespace, 382
rpki::up_down, 96

years_to_seconds
rpki::sundial::timedelta, 517
yes_or_no
rpki::cli, 69