**Embedded Security Showcase on PSoC64(ESSOP)**

Mbed TLS Library

|  |  |
| --- | --- |
| **Author:** | Aadarsh Kumar Singh, Embedded Systems and Microelectronics |
| **Status:** | released |

|  |  |  |  |
| --- | --- | --- | --- |
| Revision | Date | Editor | Reason |
| 1.0 | 05.01.2020 | Aadarsh Kumar Singh | [ESSOP-21](https://aadarsh.atlassian.net/browse/ESSOP-21) - Check the Mbed TLS library uses Hardware accelerator present in PSoC64 Board |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[1. Security APIs on mbed-OS 1](#_Toc42434501)

[2. Algorithms that uses crypto-hardware accelerator on PSoC64 1](#_Toc42434502)

[3. Useful links: 1](#_Toc42434503)

# Security APIs on mbed-OS

* The PSoC64 uses Arm Platform Security Architecture (PSA).
* The cryptographic interface for PSA is implemented in the mbed-crypto library for the MCUs (like PSoC64) which supports PSA platforms.
* As per the documentation on the mbed OS [website](https://os.mbed.com/docs/mbed-os/v6.0/apis/security.html) , mbed-crypto library is integrated with mbed-OS.
* The version of Mbed Crypto integrated with Mbed OS implements PSA Crypto [API](https://armmbed.github.io/mbed-crypto/PSA_Cryptography_API_Specification.pdf) v1.0b1.
* The development of Mbed Crypto has moved to Mbed TLS.
* Mbed TLS and Mbed Crypto have the same APIs, and the same build system.
* The mbed-OS library used in the project repository uses the mbed-TLS library.

# Algorithms that uses crypto-hardware accelerator on PSoC64

* The mbed TLS library supports many cryptographic algorithms for encryption/decryption, signature generation/verification, hashing, key generation, storage and exchange.
* Supported Algorithms that use Hardware – Crypto modules on PSoC 64 are:
* AES - Encryption/ decryption
* ECDSA – Signature Generation / Verification
* SHA-1, SHA-256, SHA-512 – Hashing
* ECP - Elliptic curve generation (Elliptic Curve Cryptography Cipher Suites

for Transport Layer Security)

* We incorporated the reference implementation for all the security services in the project using the Makefile and debugged the code, In case the hardware accelerator support was available for the device(in our case PSoC64) it used lower level API’s for triggering the hardware accelerator (like Cy\_Crypto\_Core\_Aes\_Ecb()) otherwise it used to perform the security options using the software APIs.

# Useful links:

* mbed-OS security APIs - <https://os.mbed.com/docs/mbed-os/v5.15/apis/security.html>
* Getting started mbed-Crypto : <https://github.com/ARMmbed/mbed-crypto/blob/development/docs/getting_started.md>
* PSA Cryptographic APIs link : <https://armmbed.github.io/mbed-crypto/psa/#application-programming-interface>
* PSA Reference manual link : <https://armmbed.github.io/mbed-crypto/PSA_Cryptography_API_Specification.pdf>
* Mbed-OS link : <https://github.com/ARMmbed/mbed-os/#b6370b4c37f3d4665ed1cdcb1afea85396bba1b3>