

The ARM logo is displayed in a white, lowercase, sans-serif font. It is positioned on the left side of the slide, set against a background of a blue-toned, stylized circuit board with glowing orange and yellow points of light. The background also features a grid of small white plus signs.

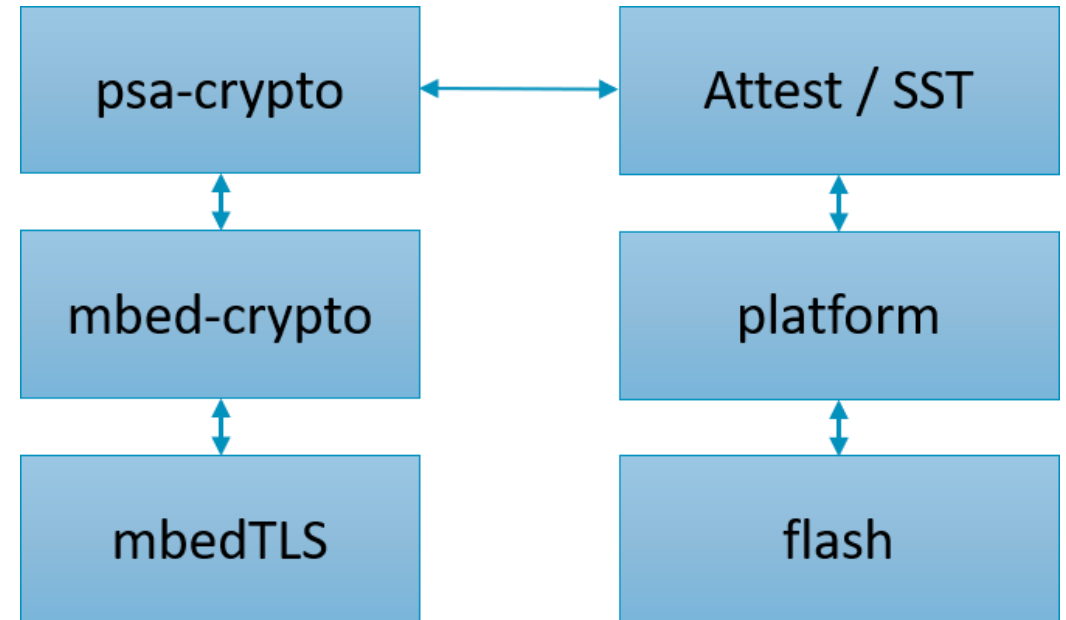
arm

Crypto HW Integration

Tamas Ban
2019.10.31

TF-M SW only crypto

- MbedTLS is used in MCUBoot
- Mbed-crypto is used in TF-M runtime
- Abstraction layer for retrieving keys from platform
- Just example implementation crypto keys are hard-coded in *.c file
- Keys are part of the secure image, stored on flash

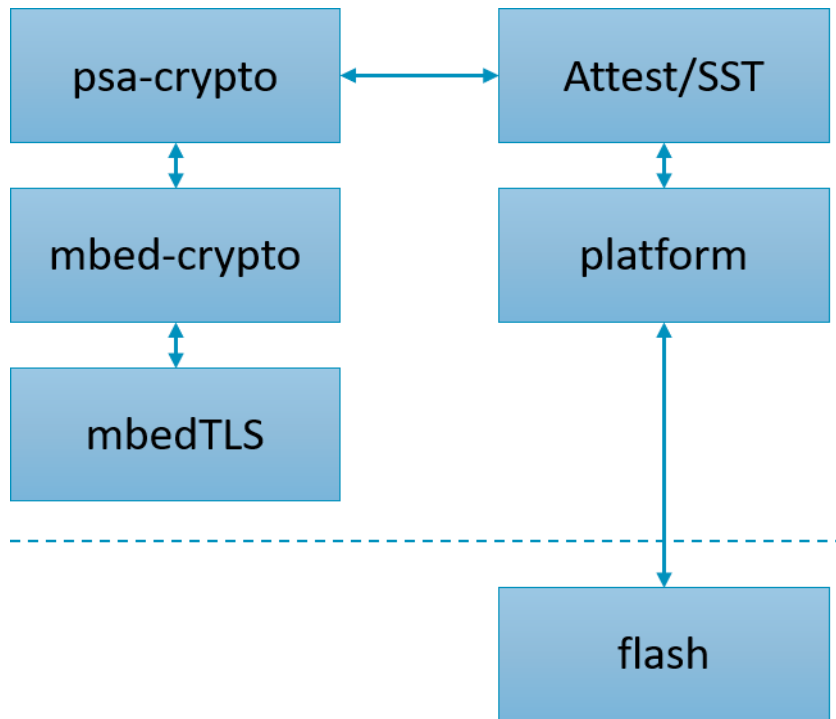


Musca-B1 HW crypto capability

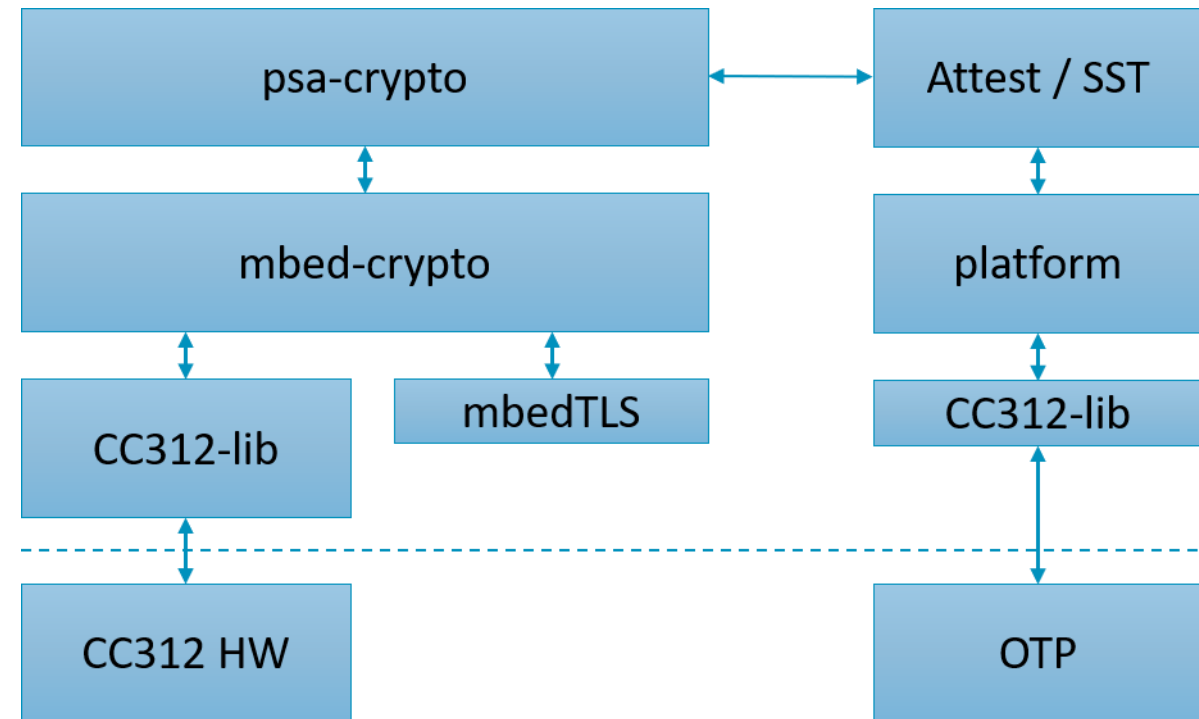
- Crypto Island:
 - M0+ core
 - CC312
- CryptoCell-312 (CC312):
 - Crypto HW accelerator
 - OTP memory
- SW support for CC312
 - Using [open source](#) Runtime library
 - mbedTLS aligned API
 - Tools in the library used to provision OTP

TF-M and CC312 integration

SW only



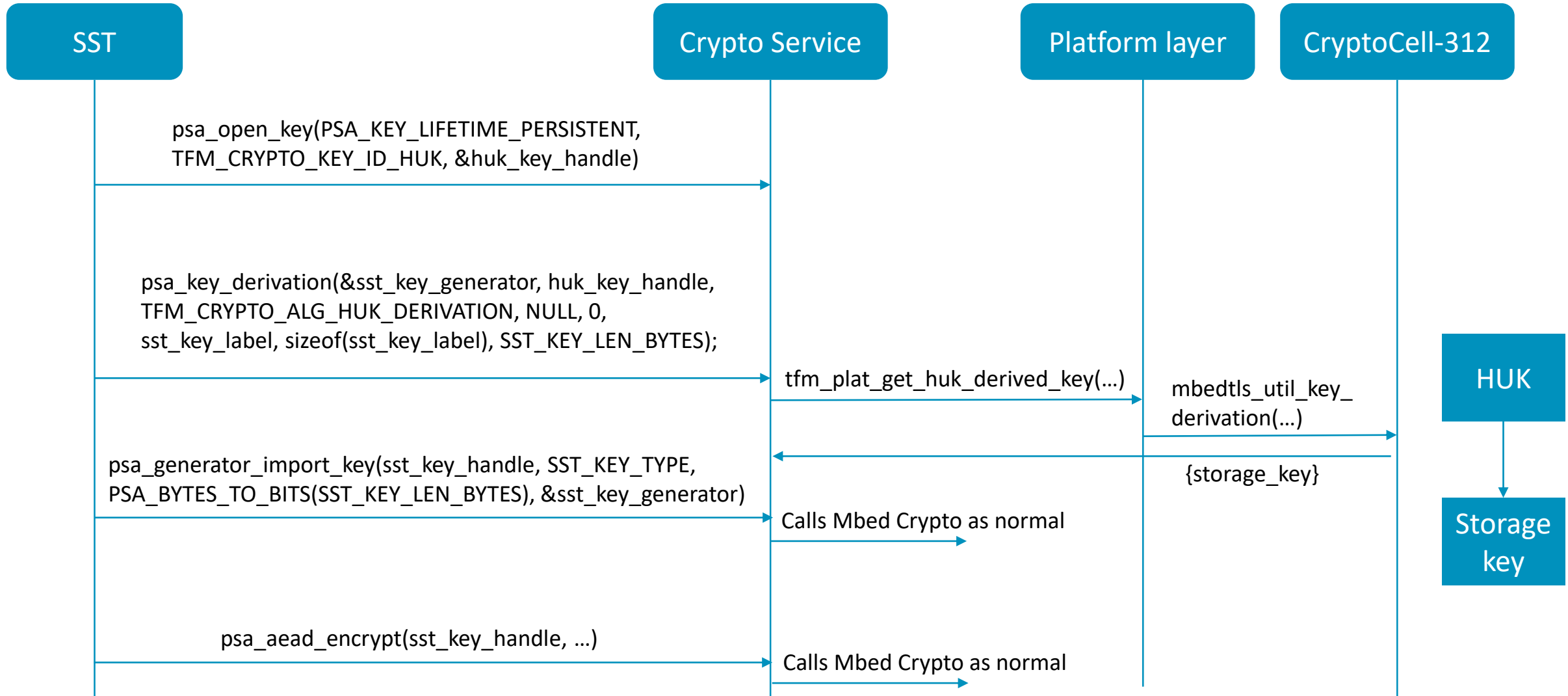
HW accelarated



OTP provisioning

- Manufacturing utility libraries
- They will be integrated with MCUBoot
 - Compile time option to link them to bootloader or not
- When OTP provisioned then newer DAPLink is necessary to reprogram the board because debug ports will be closed down
- Keys to be provisioned:
 - HUK
 - Hash of ROTPK
 - Attestation private key

SST integration with CryptoCell-312



TF-M Crypto service integration with CryptoCell

TF-M Crypto service uses Mbed Crypto to provide implementation of PSA Crypto APIs

Use 'alt' implementation feature to replace Mbed Crypto software implementations

- Alt implementations provided by CryptoCell repo to call the CryptoCell runtime library

Only change inside TF-M Crypto service code is to call initialisation function for CryptoCell-312

Mostly just changes to build system

- Build Mbed Crypto with alt implementations enabled
- Build & link the CryptoCell runtime library



The Arm trademarks featured in this presentation are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved. All other marks featured may be trademarks of their respective owners.

www.arm.com/company/policies/trademarks

