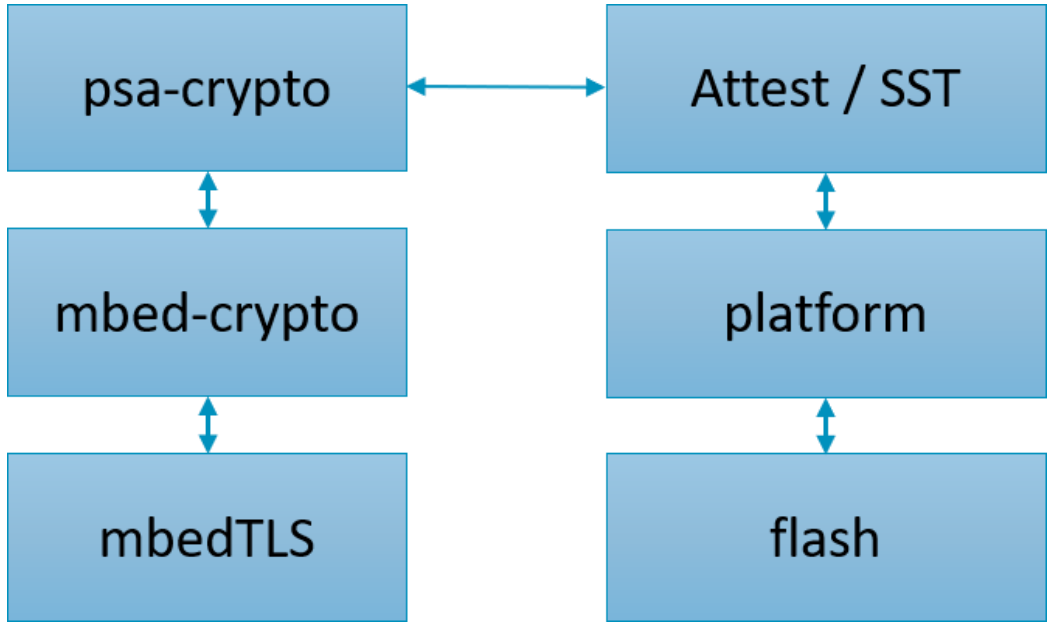
Crypto HW Integration

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 retreving keys from platform
- Just example implementation crypto keys are hard-coded in *.c file
- Keys are part of the secure image, stored on flash



arm

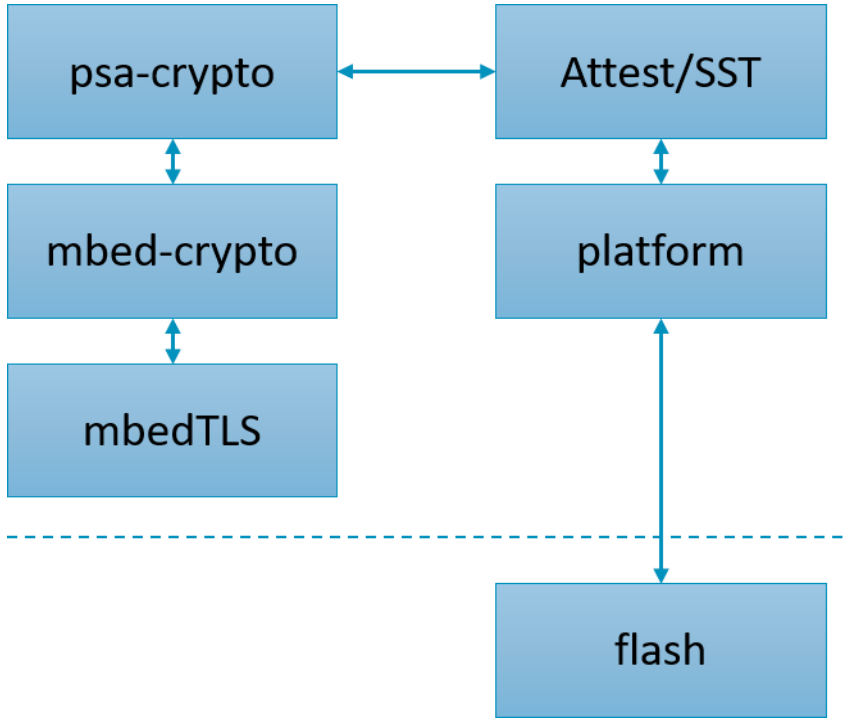
Musca-B1 HW crypto capability

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

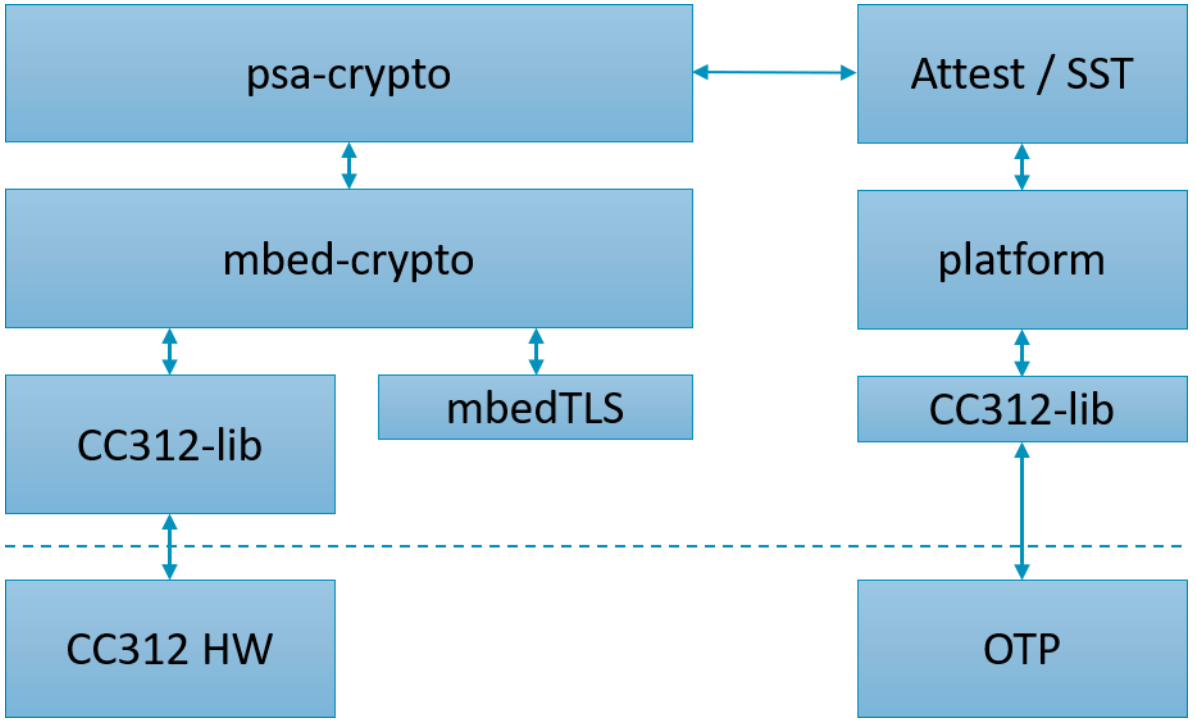
arm

TF-M and CC312 integration

SW only



HW accelrated



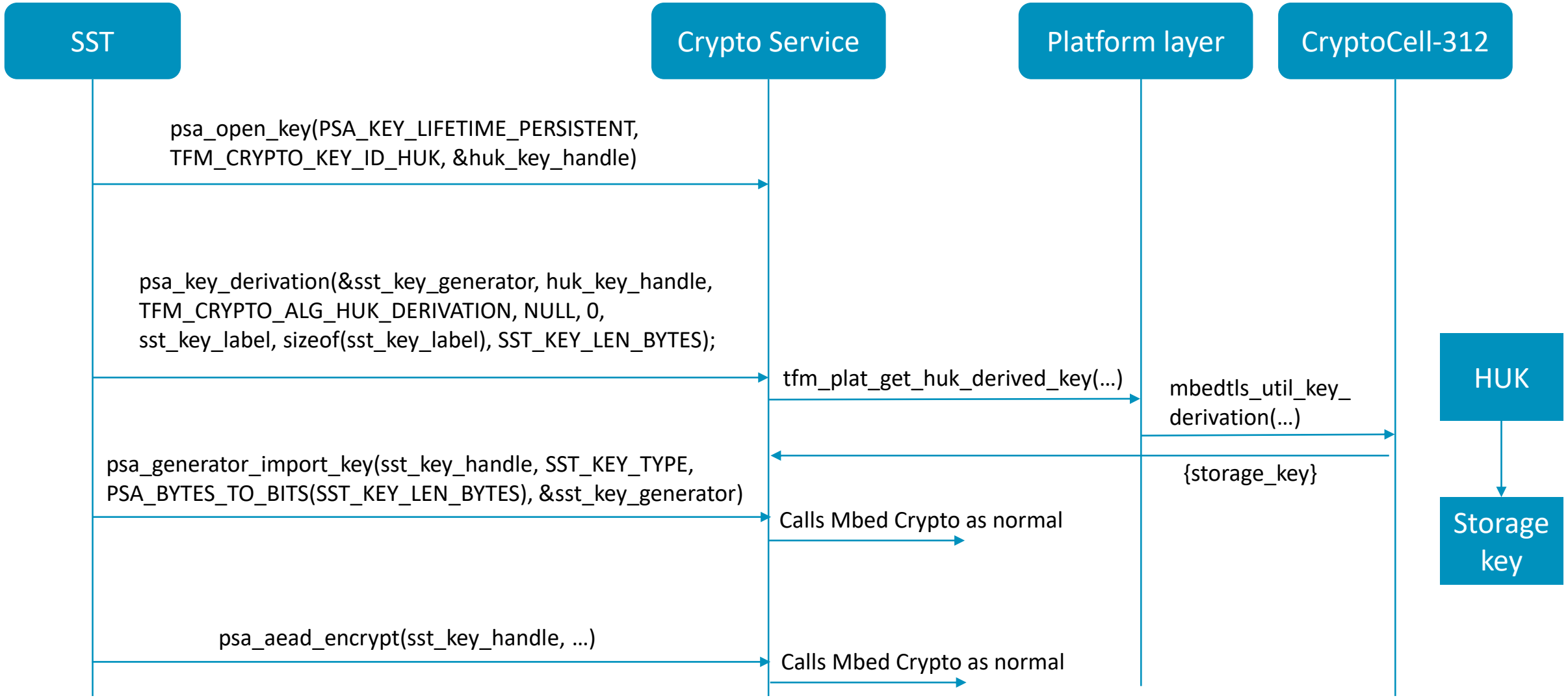
arm

OTP provisoning

- Manufacturing utility libraries

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

SST integration with CryptoCell-312



arm

TF-M Crypto service integration with CryptoCell

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

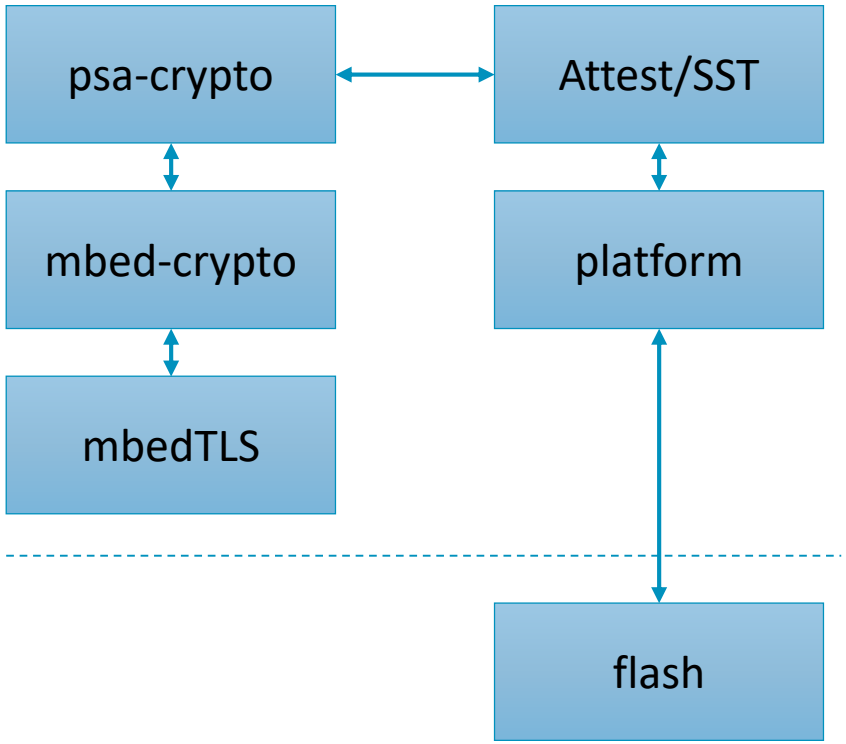
Use ‘alt’ implementation feature to replace Mbed Crypto software implementations

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

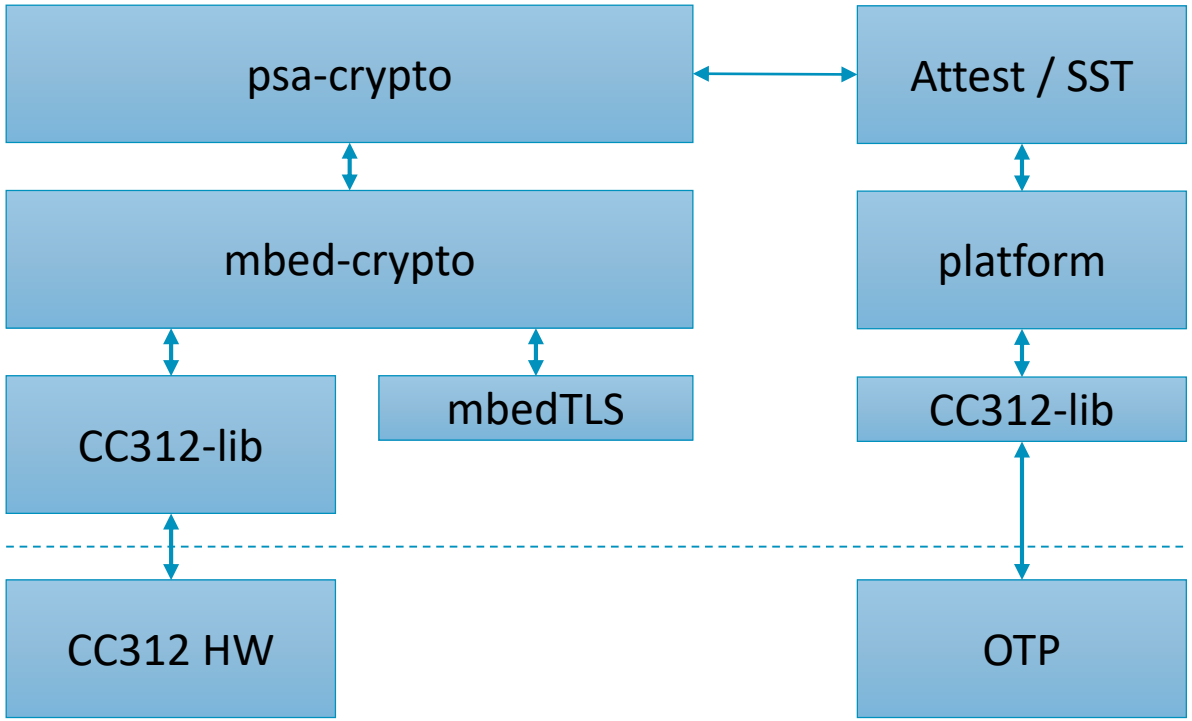
Only change inside TF-M Crypto service code is to call initialisation function for CryptoCell-312

Mostly just changes to build system

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



arm



arm