arm

TF-M and Amazon FreeRTOS Integration update

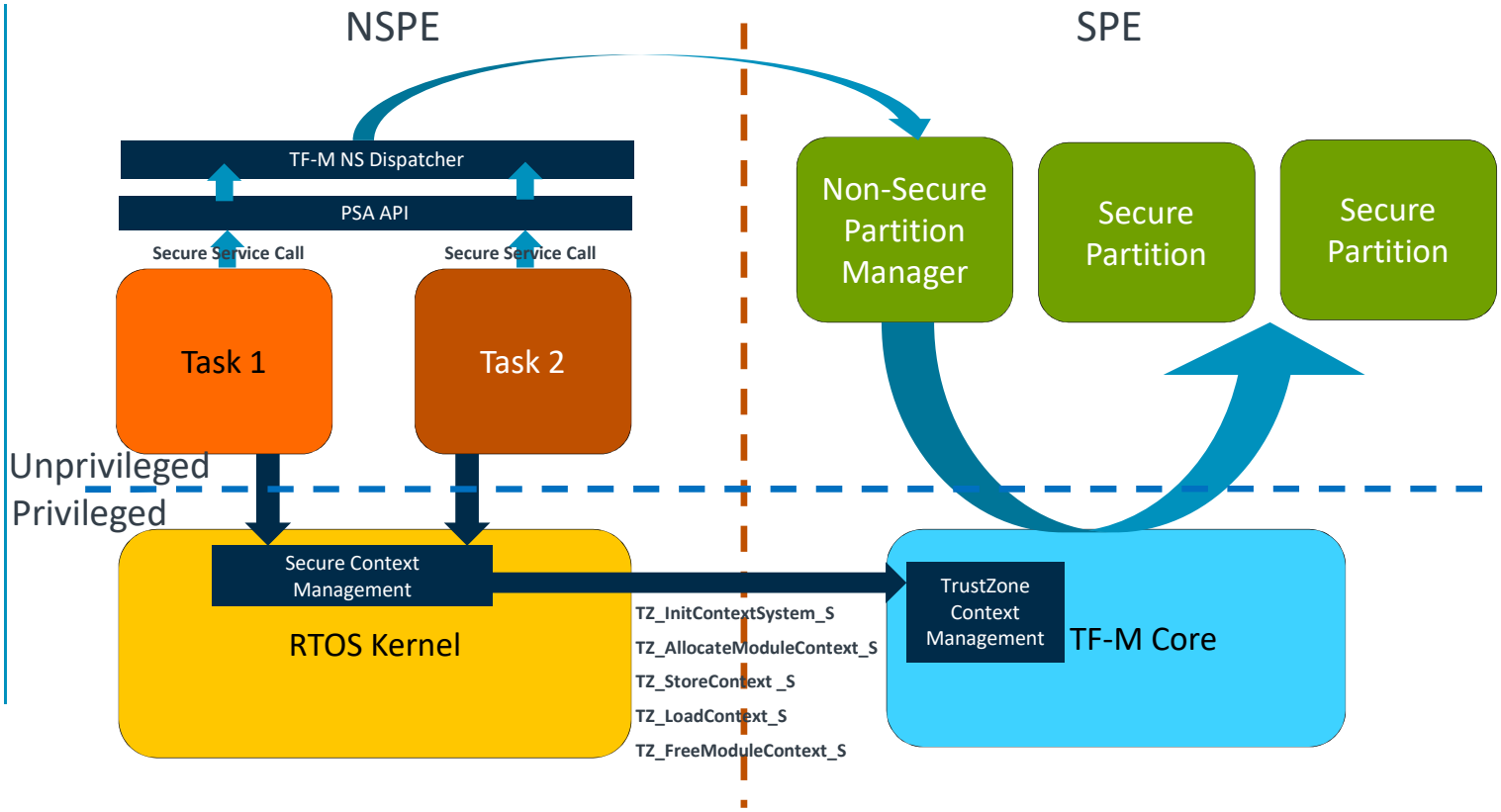
David Wang

19 Dec 2019

RTOS Enablement

General Design

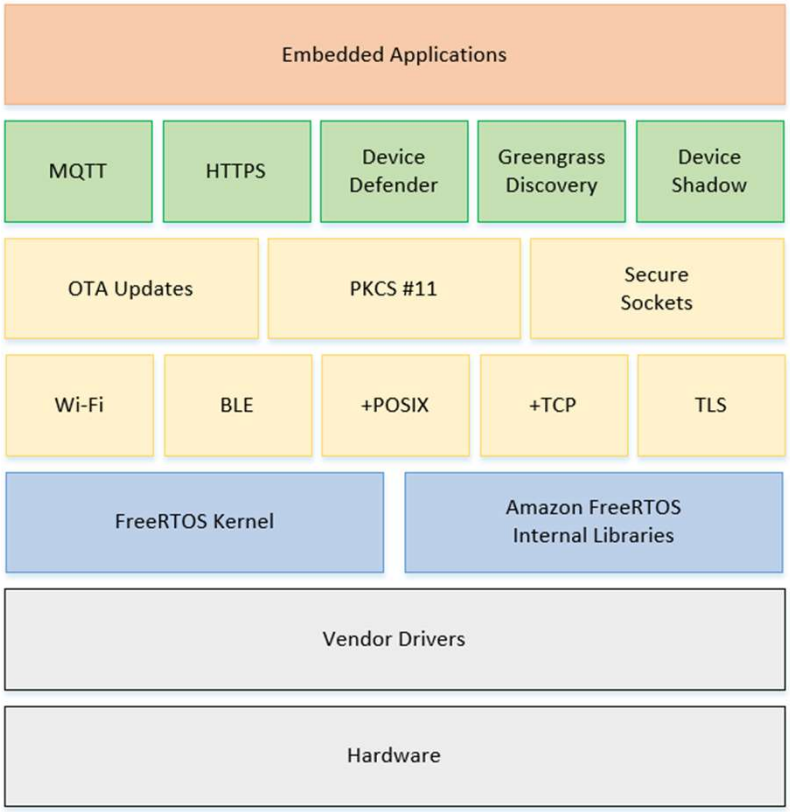
- RTOS Kernel manages the Secure Context (if needed) for each task
- Task calls PSA API through the TF-M NS Dispatcher
- Dispatcher forwards the Secure Service Call to TF-M
- The Secure Partition contains the called Secure Service will be activated to serve

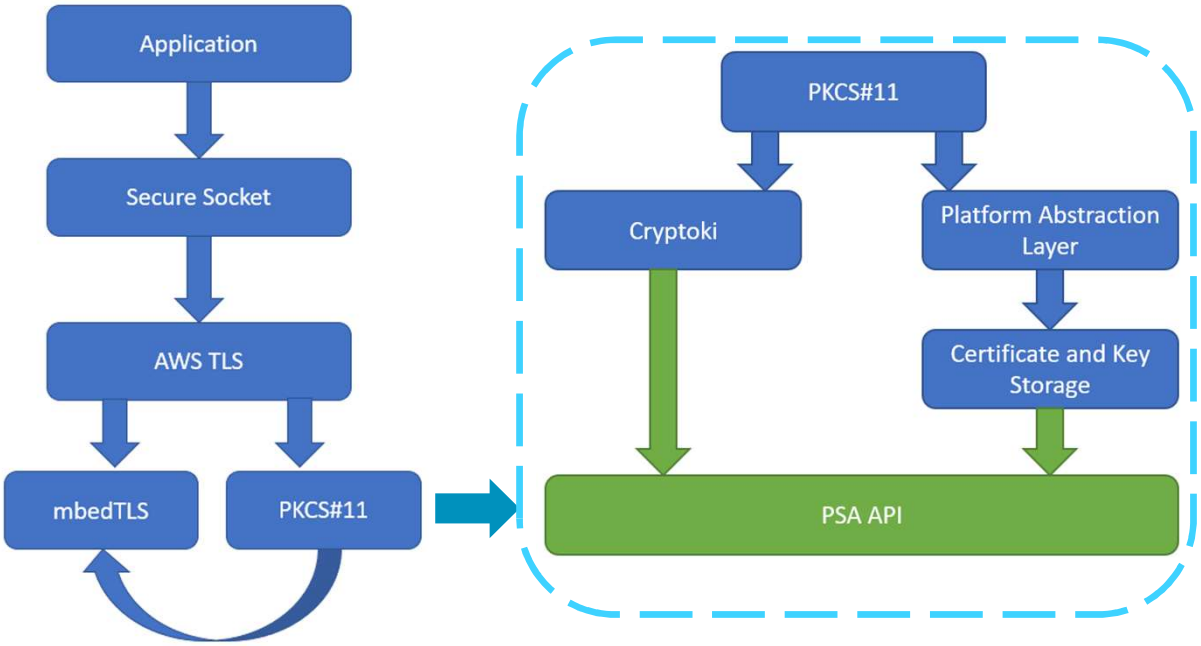


arm

IoT Cloud Security Enablement – PKCS#11

Amazon FreeRTOS TLS integration



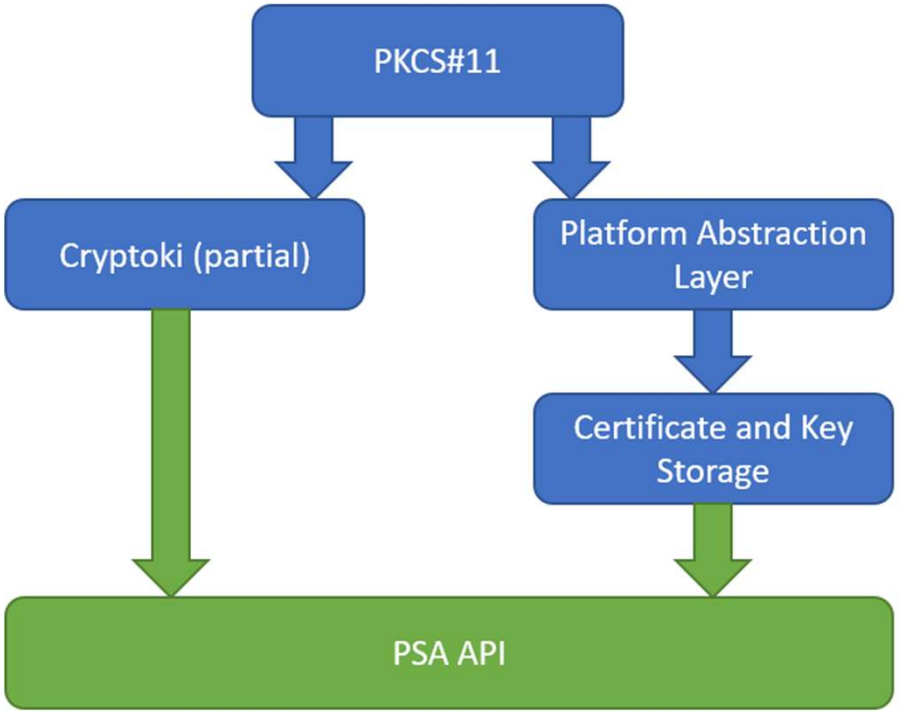


arm

PSA Dev API + PKCS#11 Integration Design

Integrate with PKCS#11

- The PAL of PKCS#11
  - Store the Certificate by PSA Storage API – Protected with integrity
  - Store the Keys by PSA Cryptography API
- Cryptoki - Call PSA Cryptography API
  - Digest
  - Sign/Verify
  - Generate key
  - Generate random



arm

Patches are ready for review

- In Linaro Github now
  - https://github.com/Linaro/amazon-freertos
- Enable TF-M in Amazon FreeRTOS
  - https://github.com/Linaro/amazon-freertos/pull/1
- PKCS#11 TF-M shim layer
  - https://github.com/Linaro/amazon-freertos/pull/2
  - Got a lot of comments from Amazon and partners

arm

Thank You
Danke
Merci
谢谢
ありがとう
Gracias
Kiitos
감사합니다
धन्यवाद
شكرًا
תודה