

arm

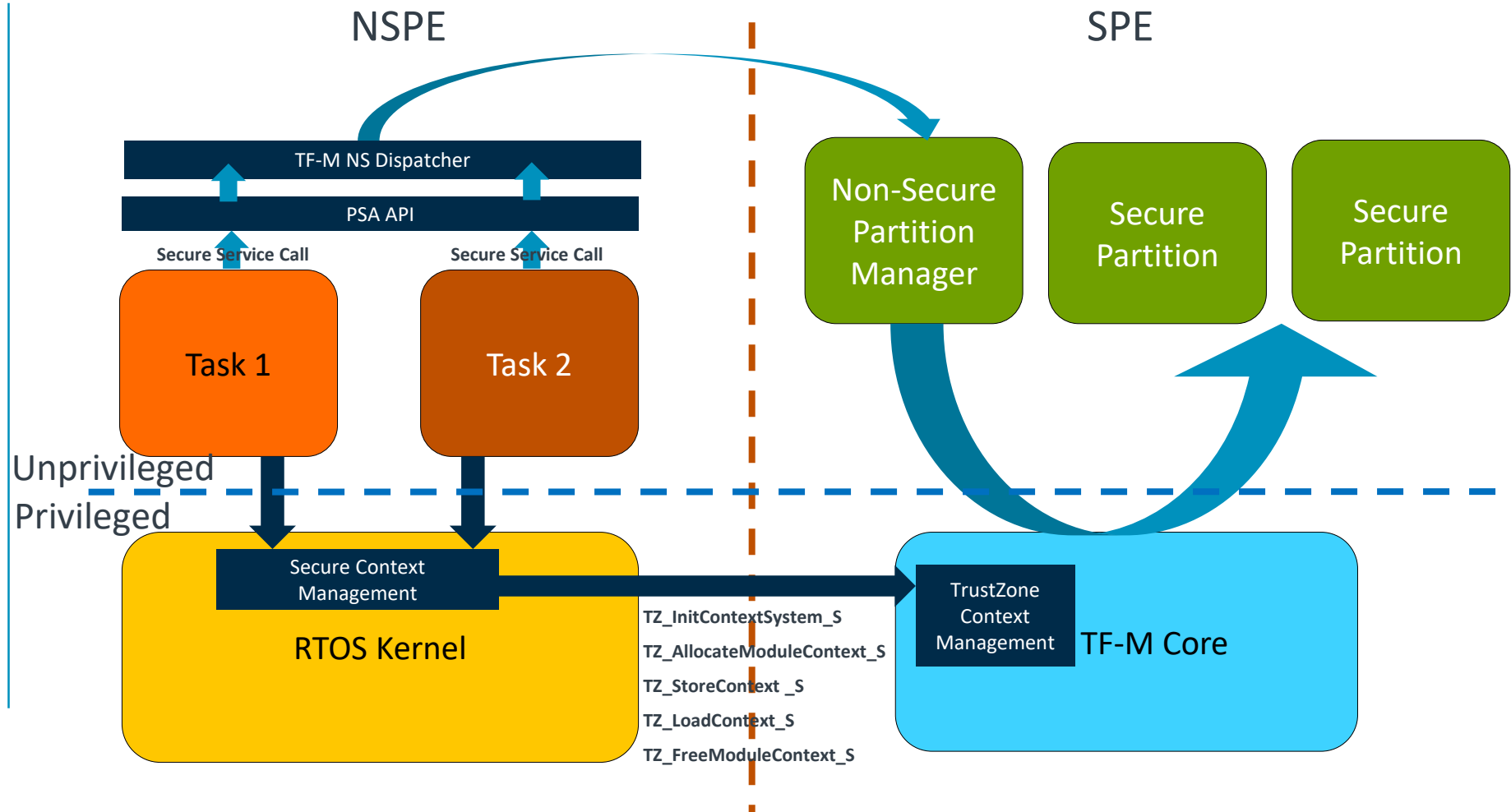
IoT Ecosystem Enablement for TF-M

David Wang
1 Nov 2019

RTOS Enablement

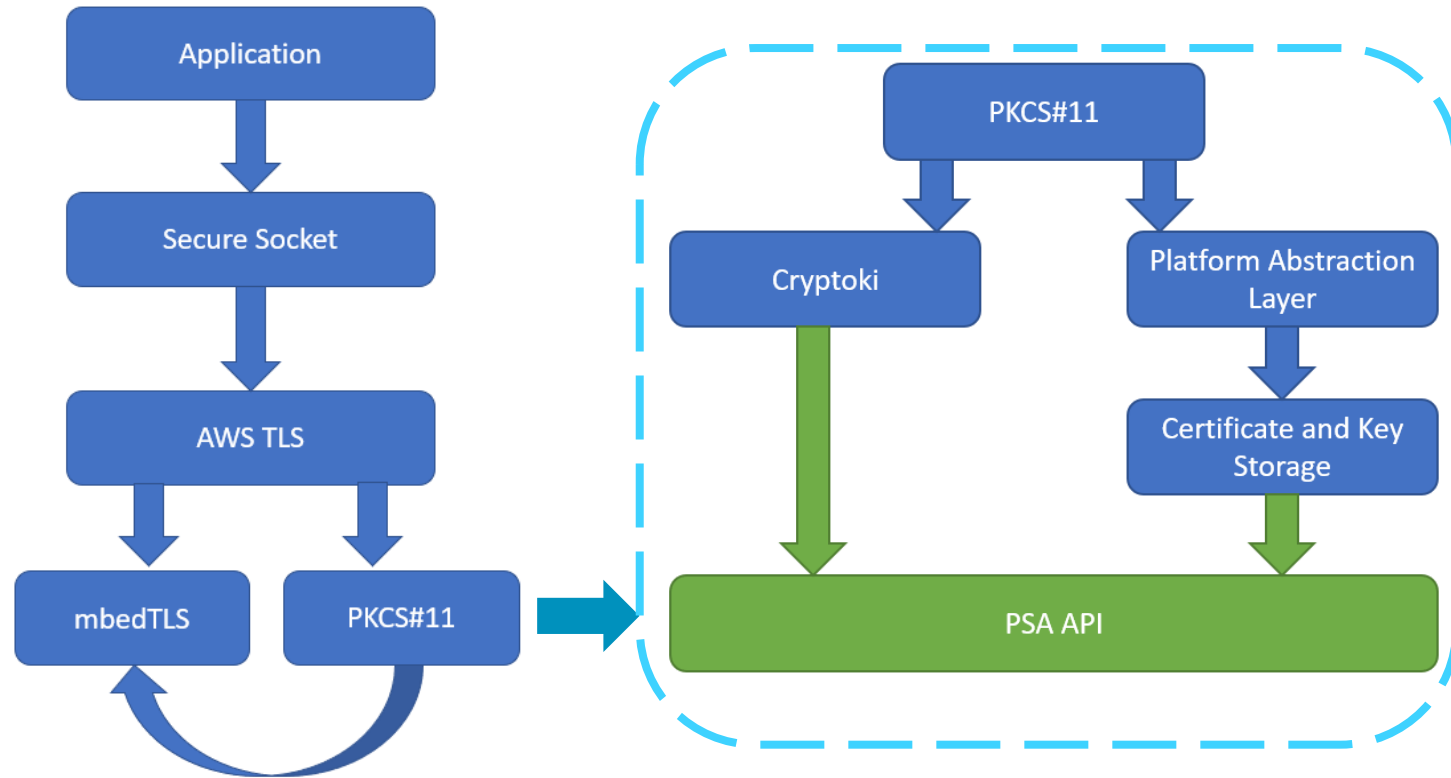
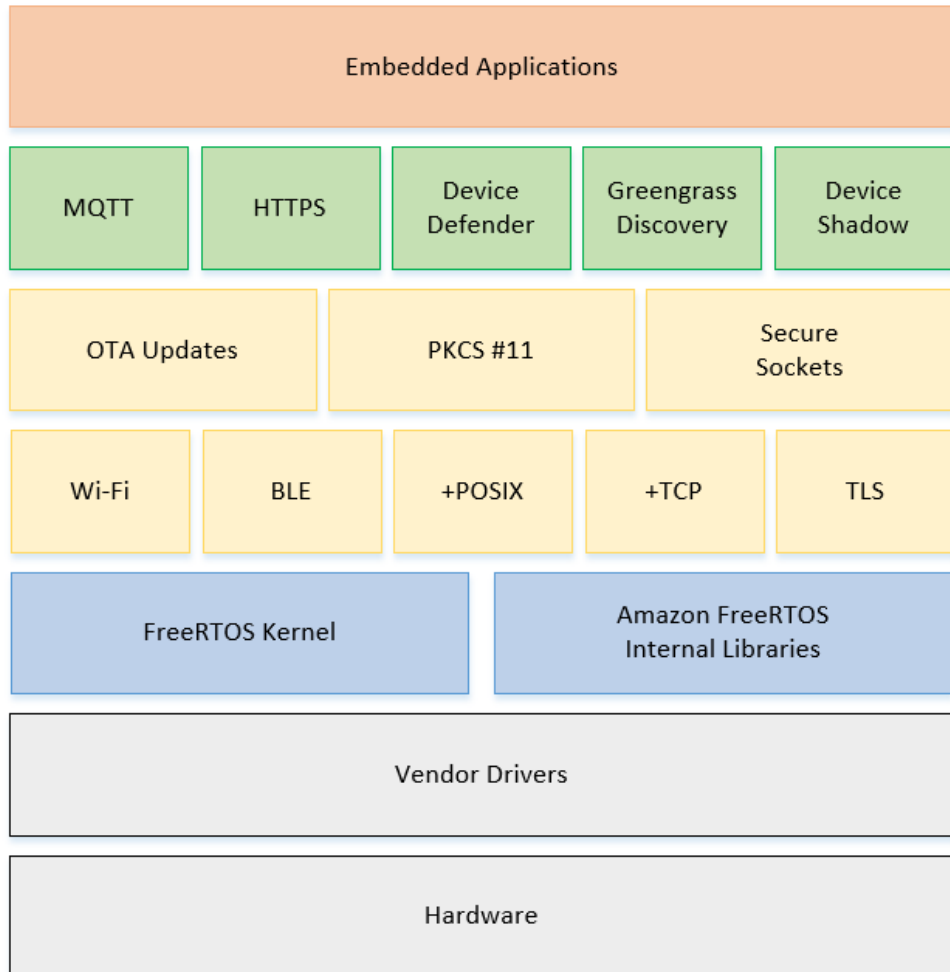
General Design

- RTOS Kernel manages the Secure Context 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



IoT Cloud Security Enablement – PKCS#11

Amazon FreeRTOS TLS integration



IoT Ecosystem Enablement

Discussion

- Build only secure FW
- One API for secure context switch
- Improve realtime ability – leave partition management to PendSV
- Reuse PKCS#11 shim layer