
arm
PSA Secure Partitions/OP-TEE

OSS Reference Implementation: PSA RoT

Analyze

Threat models
& security analyses

Methodically
developed

Architect

Hardware & firmware
architect specifications

Open
architecture

Implement

Firmware
source code

Open Source

Certify

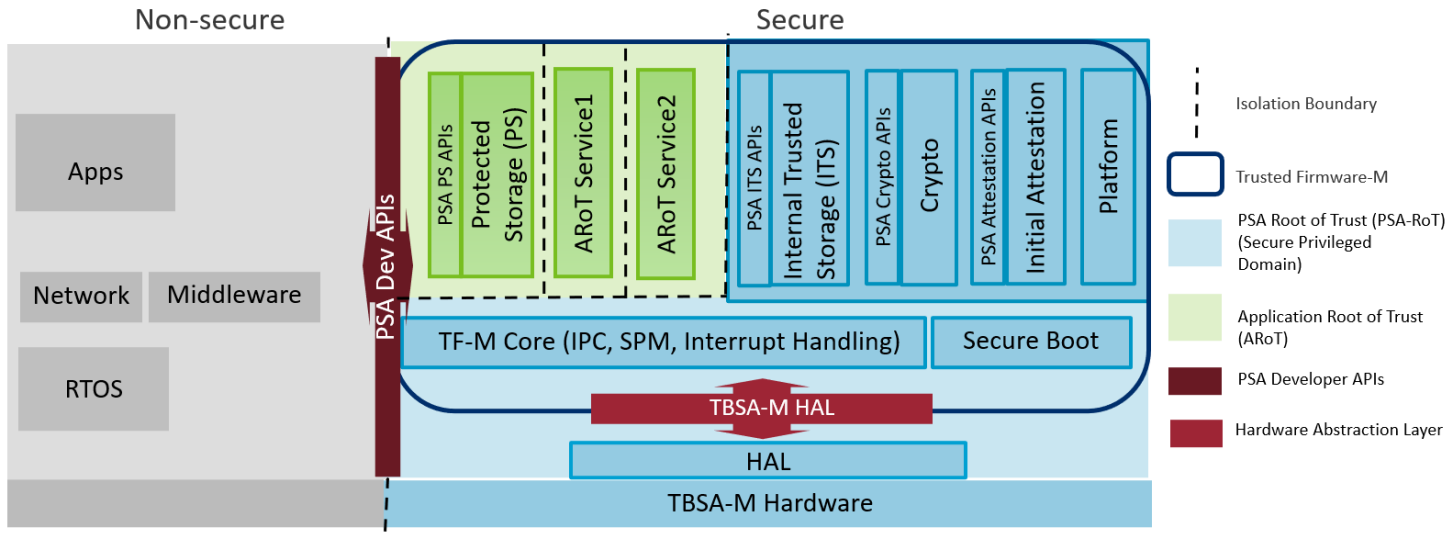
Independently
tested

psacertified™

Enabling
trust

TF-M v1.2: For PSA Level1, Level2 and Functional API Certification

- Enabled on several Cortex-M platforms
  - 6 PSA L2 certification
  - Corstone-300 (v8.1-M)
- 4-Monthly Releases – PSA and Regression tested on all platforms
- Enabled PSA L3 isolation, Profiles, mcuboot fault injection mitigations
- RTOS Integrations
- Open Test System under Trustedfirmware.org



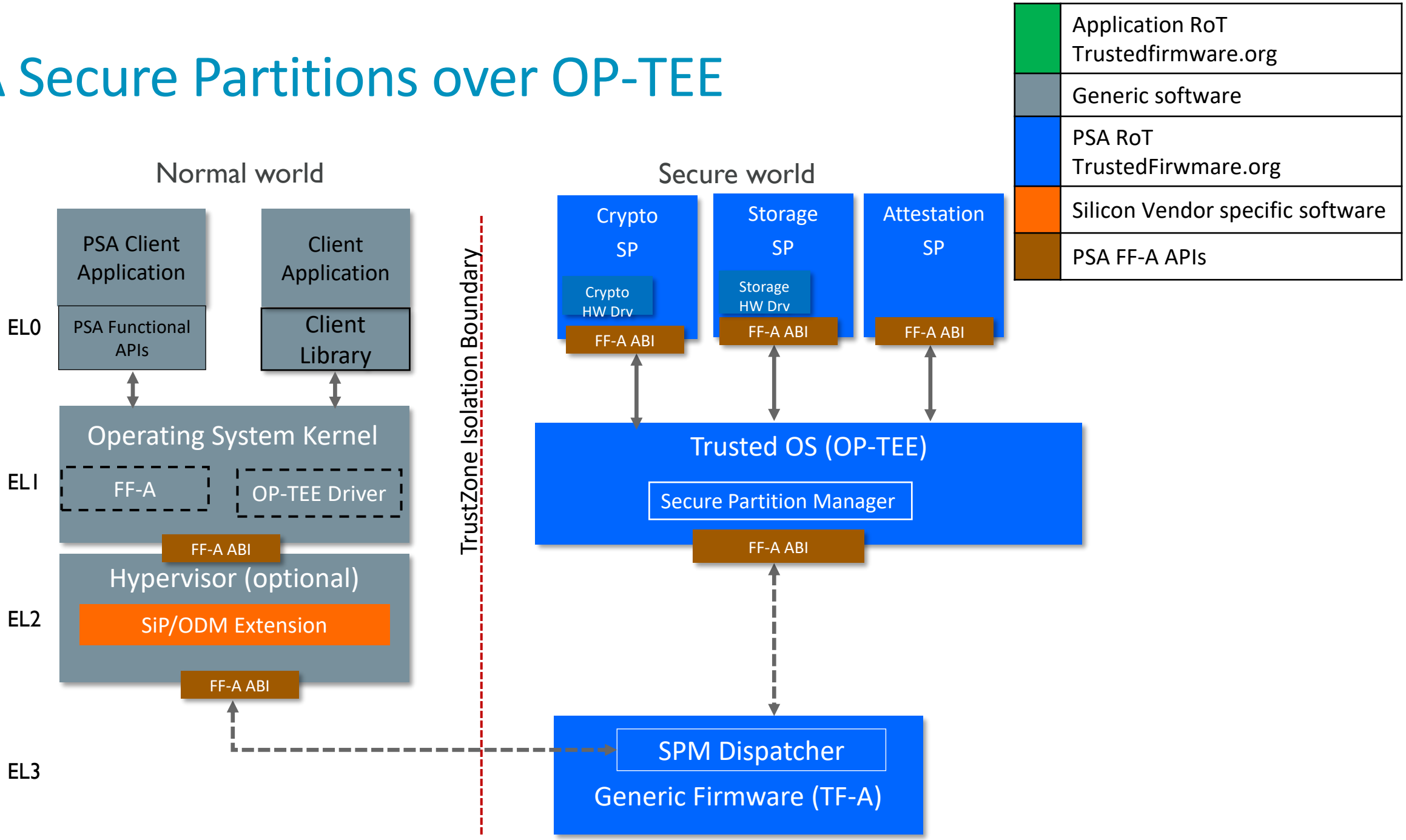
arm

PSA Extending to Cortex-A

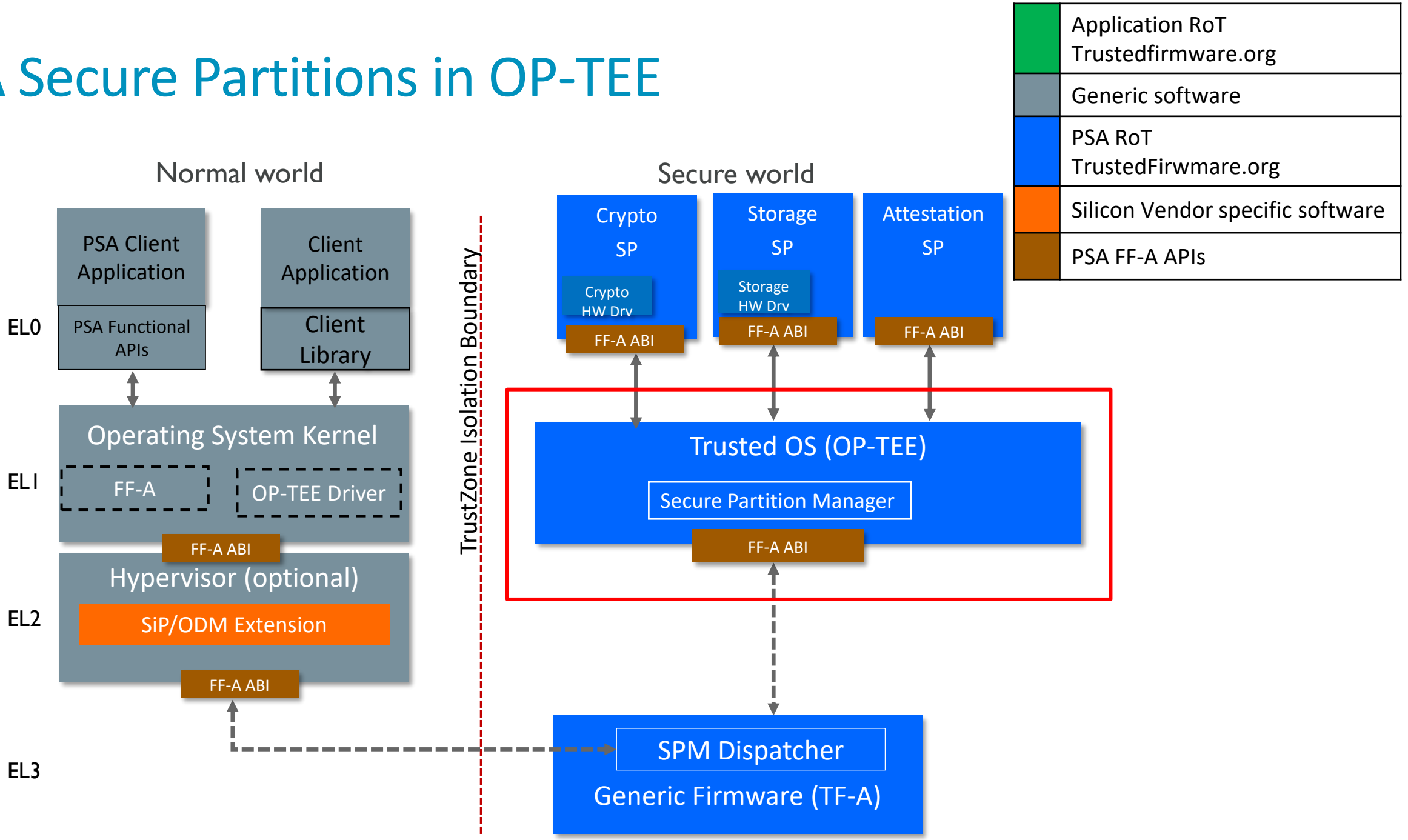
Goals

- Provide PSA RoT for Rich IoT, Edge Devices
- Providing Out of the Box Security & Enabling Platforms to be PSA Certified
- Use Firmware Framework-A (FF-A) for these standardization efforts
- Applicable to the Diverse Rich IoT/Edge deployment models

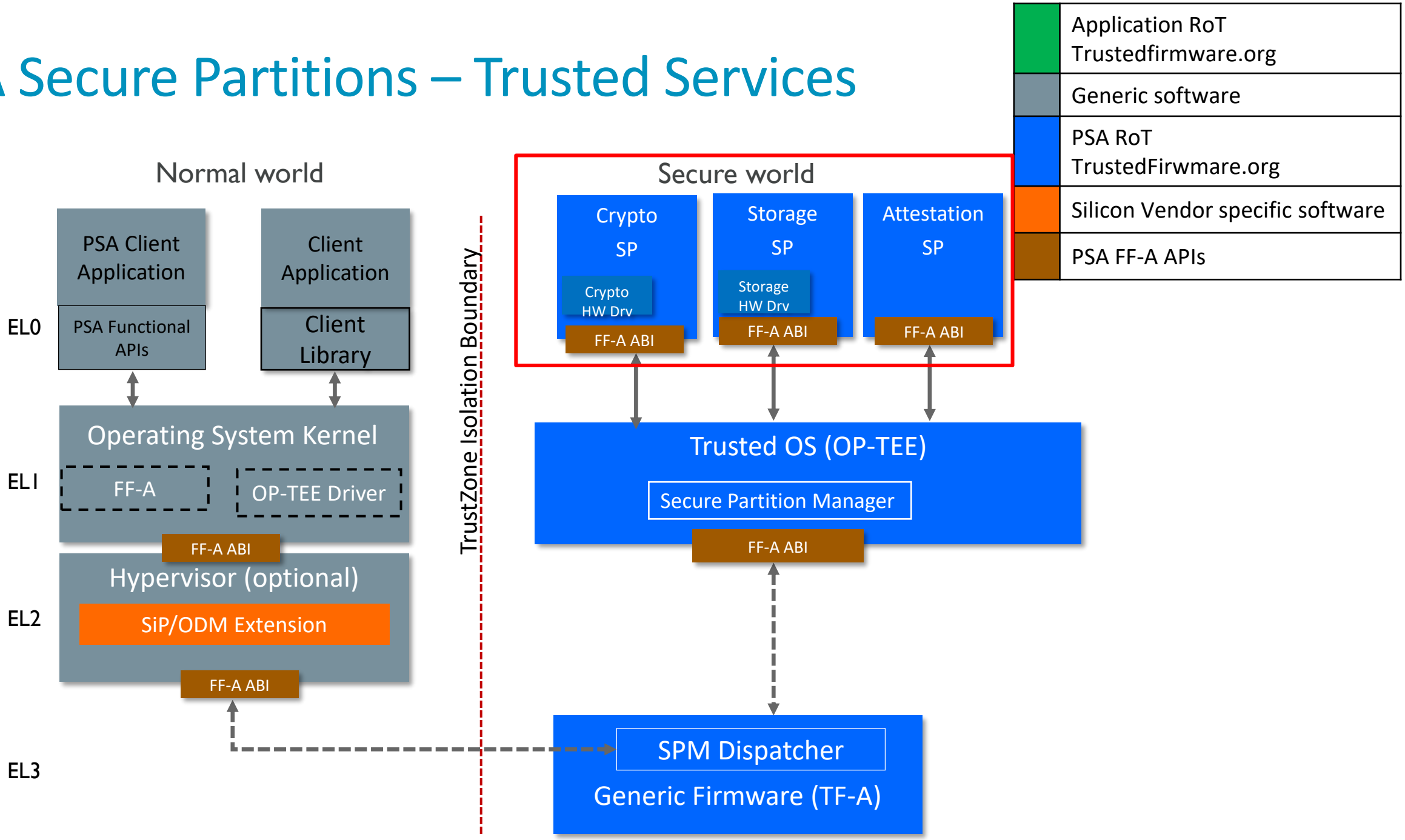
PSA Secure Partitions over OP-TEE



PSA Secure Partitions in OP-TEE

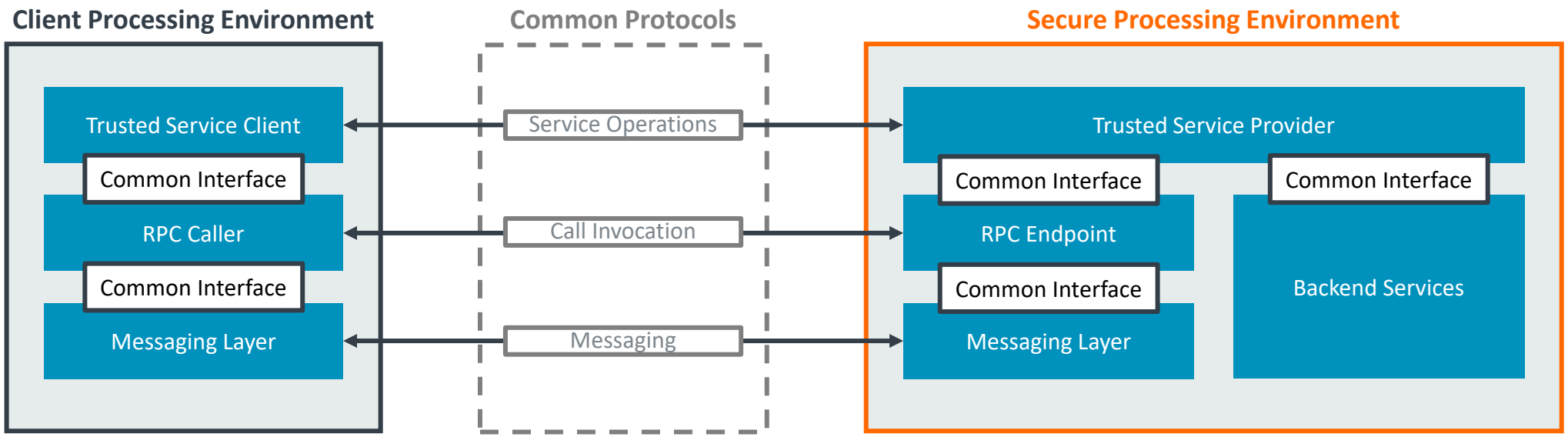


PSA Secure Partitions – Trusted Services



Trusted Services – A Layered Model

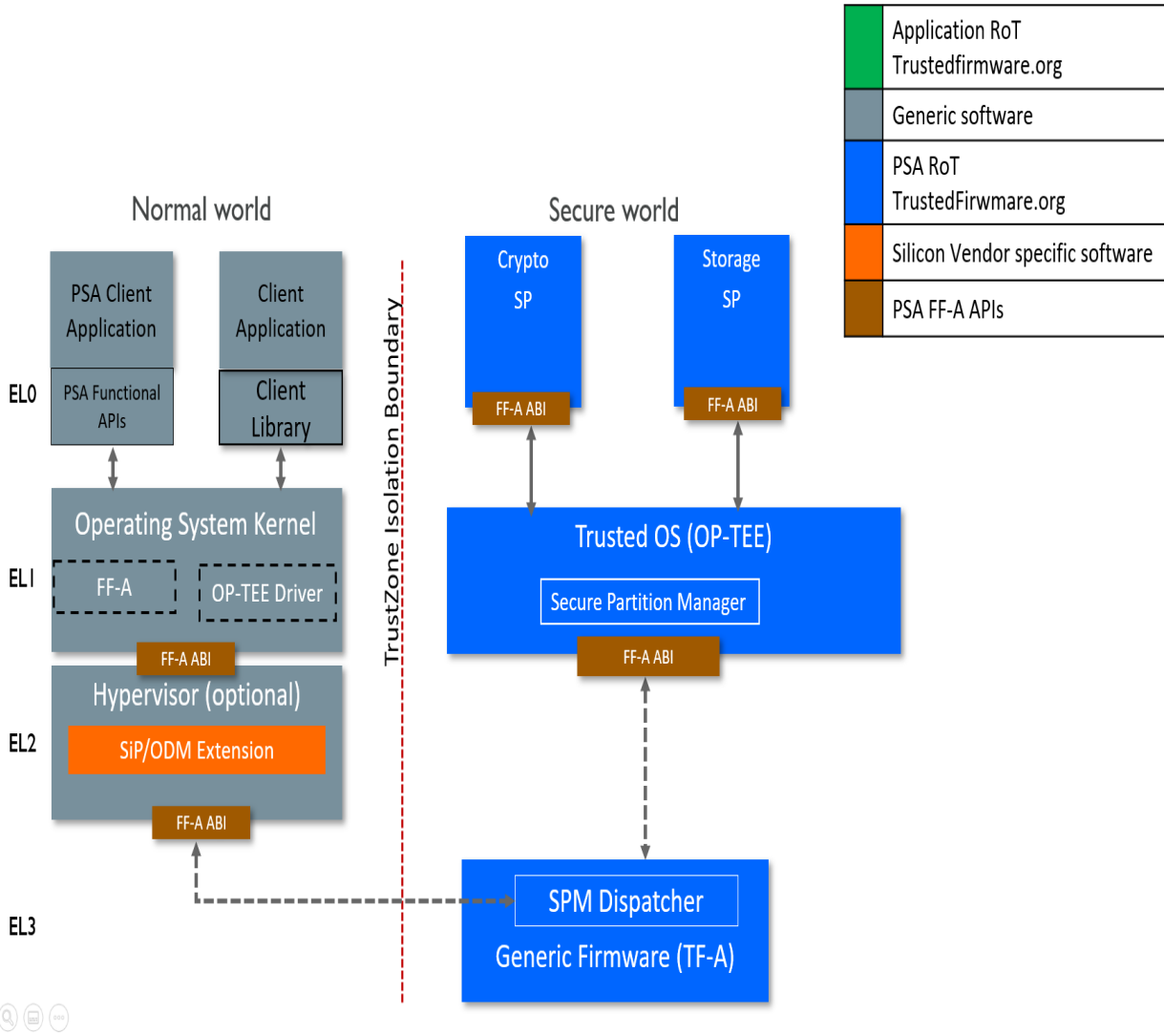
- Framework to develop Security related Services
- Deployable over range of Isolated Processing Environments
- Applications uses Trusted Services for Security Operations using client/server model
- Trusted Services for Cryptography, Storage and Attestation



arm

Work So Far…

- Initial OP-TEE, Crypto, Internal Trusted Storage Secure Partitions (SP), Normal World Test Application available.
- OP-TEE patches in trustedfirmware.org being upstreamed to OP-TEE github
- Crypto and Storage Services available in Trusted Services repository in TF.org
- PoC Linux driver that exposes FF-A operations to user space available



Roadmap

- Enhancing, Upstreaming OP-TEE OS SPM Implementation
- Linux kernel upstreaming
- SEL0 Access to Hardware
- Attestation and Protected Storage Service
- PSA Secure Partition over Secure-EL2/Hafnium
- 32-bit support

arm

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