arm

Trusted Services

May'21

PSA Certified Framework

psacertified™

Trustedfirmware.org
Reference Implementations

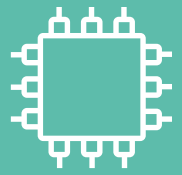
Analyze

Threat models
& security analyses

Architect

Hardware & firmware
architect specifications

Implement



Firmware
source code

Certify

Independently
tested

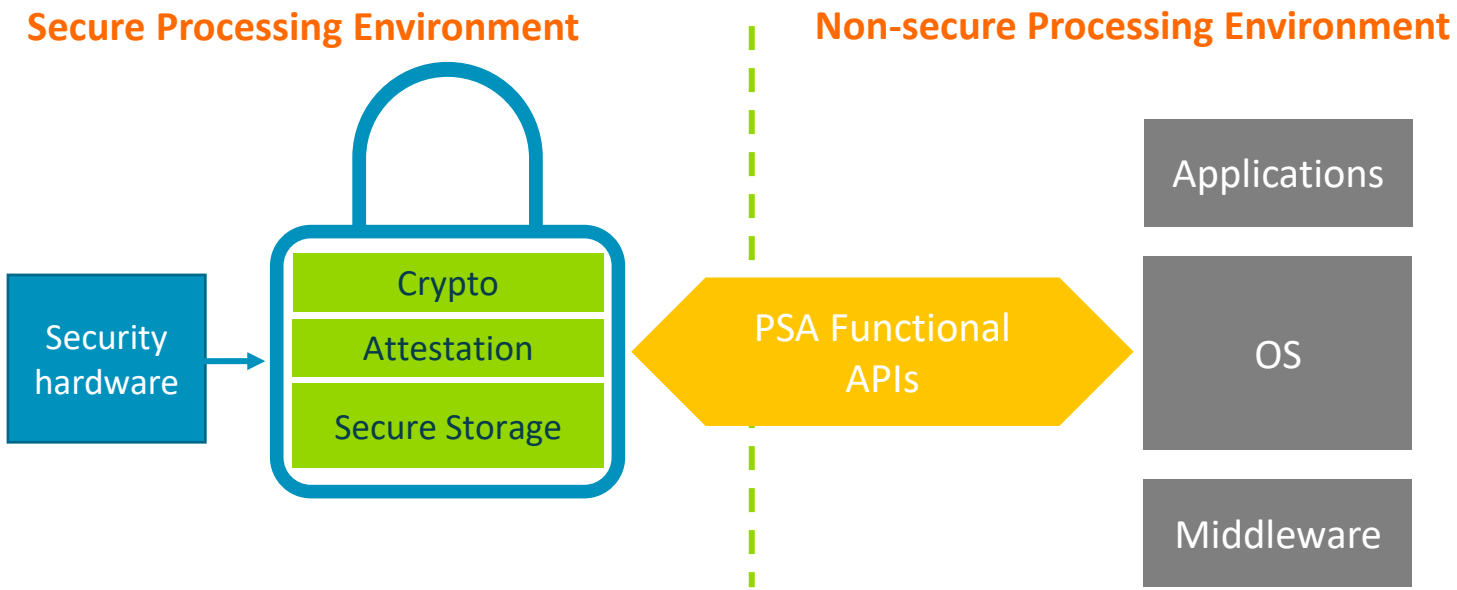
arm

PSA Functional APIs Makes Security Easier to Use

Fast time-to-market by abstracting security complexities

Reduced fragmentation by using widely available security APIs

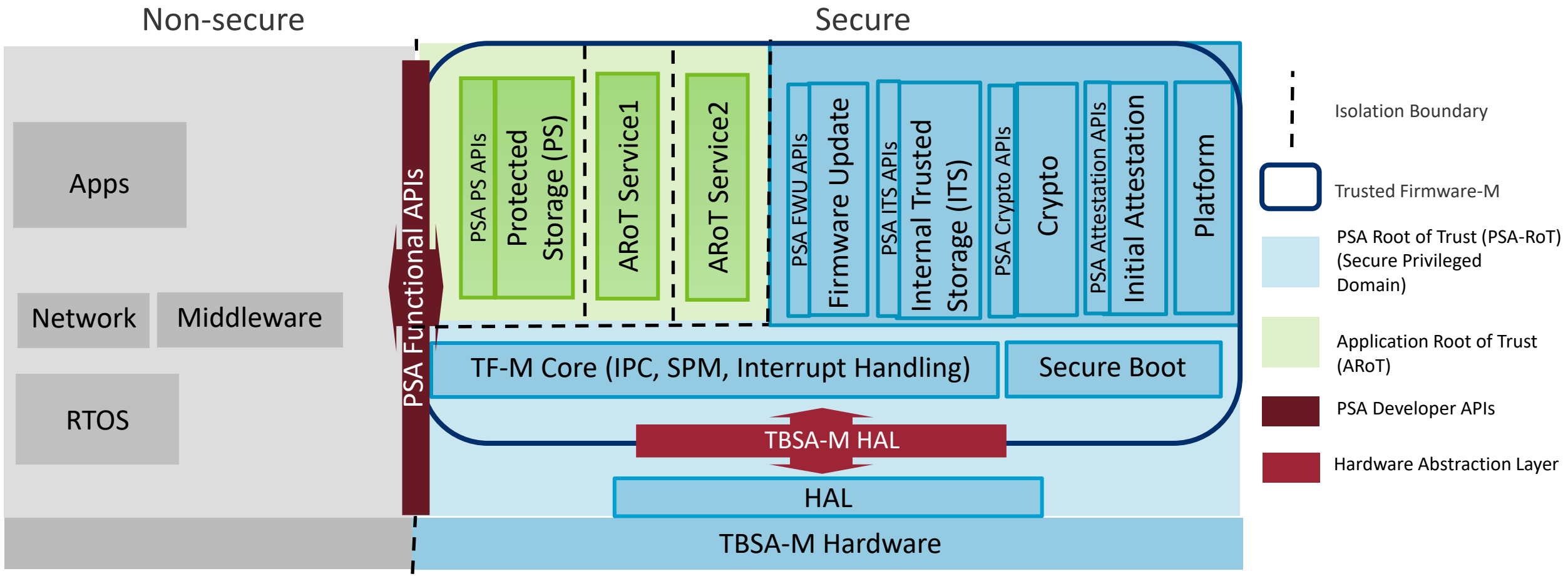
Lower total cost of ownership, maximizing ROI through re-use of APIs



PSA-RoT is the foundation for all secure operations in the system

arm

Trusted Firmware-M Available on Several MCU platforms

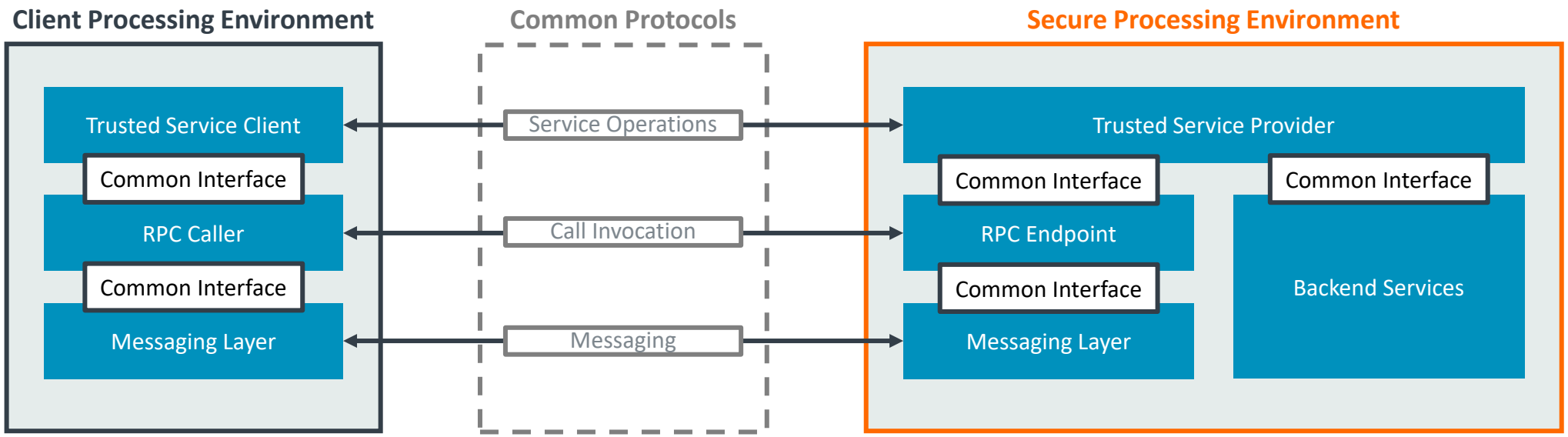


Extending to Linux IoT Devices

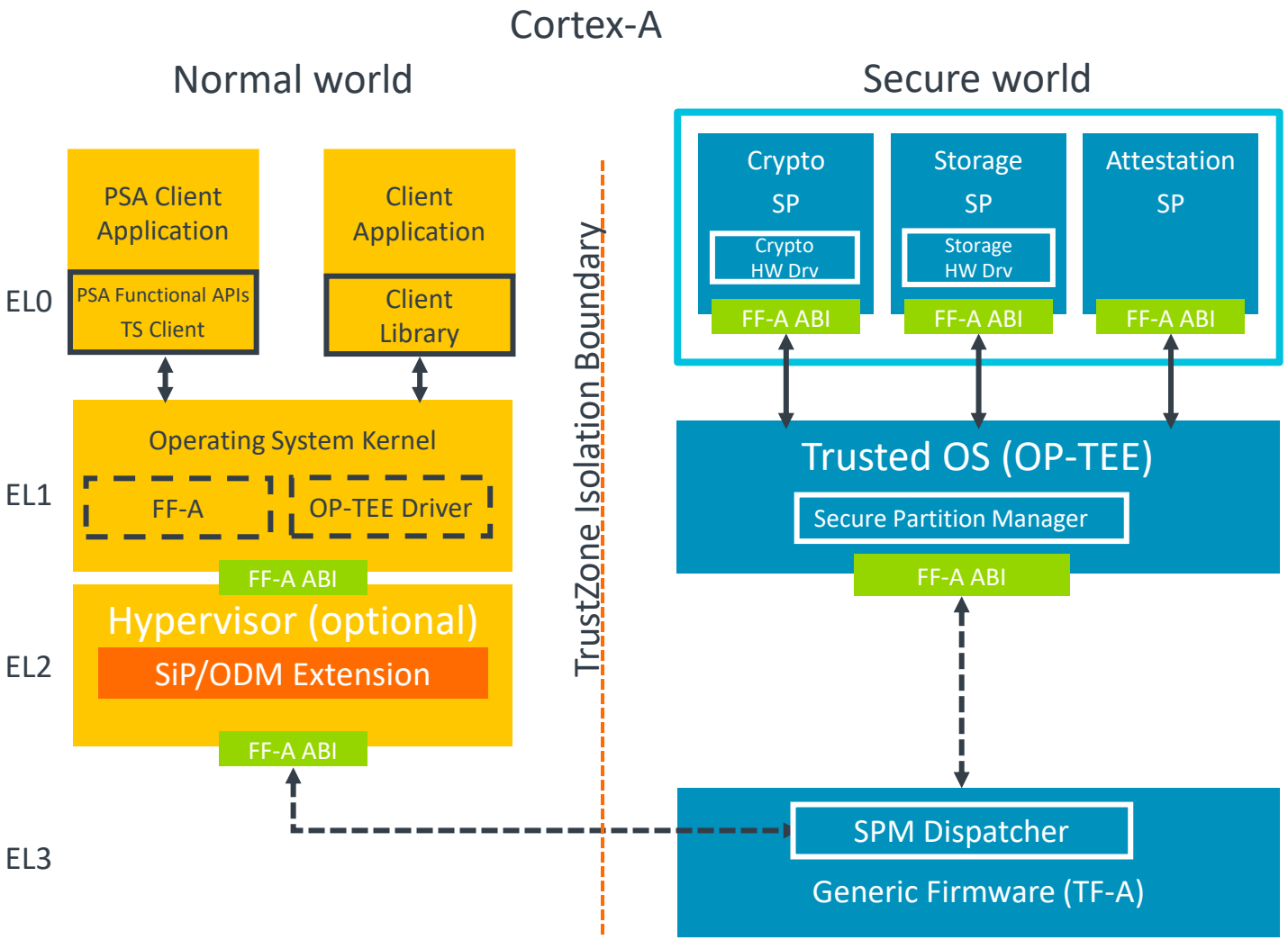
- PSA-RoT For Rich IoT, Edge Devices

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

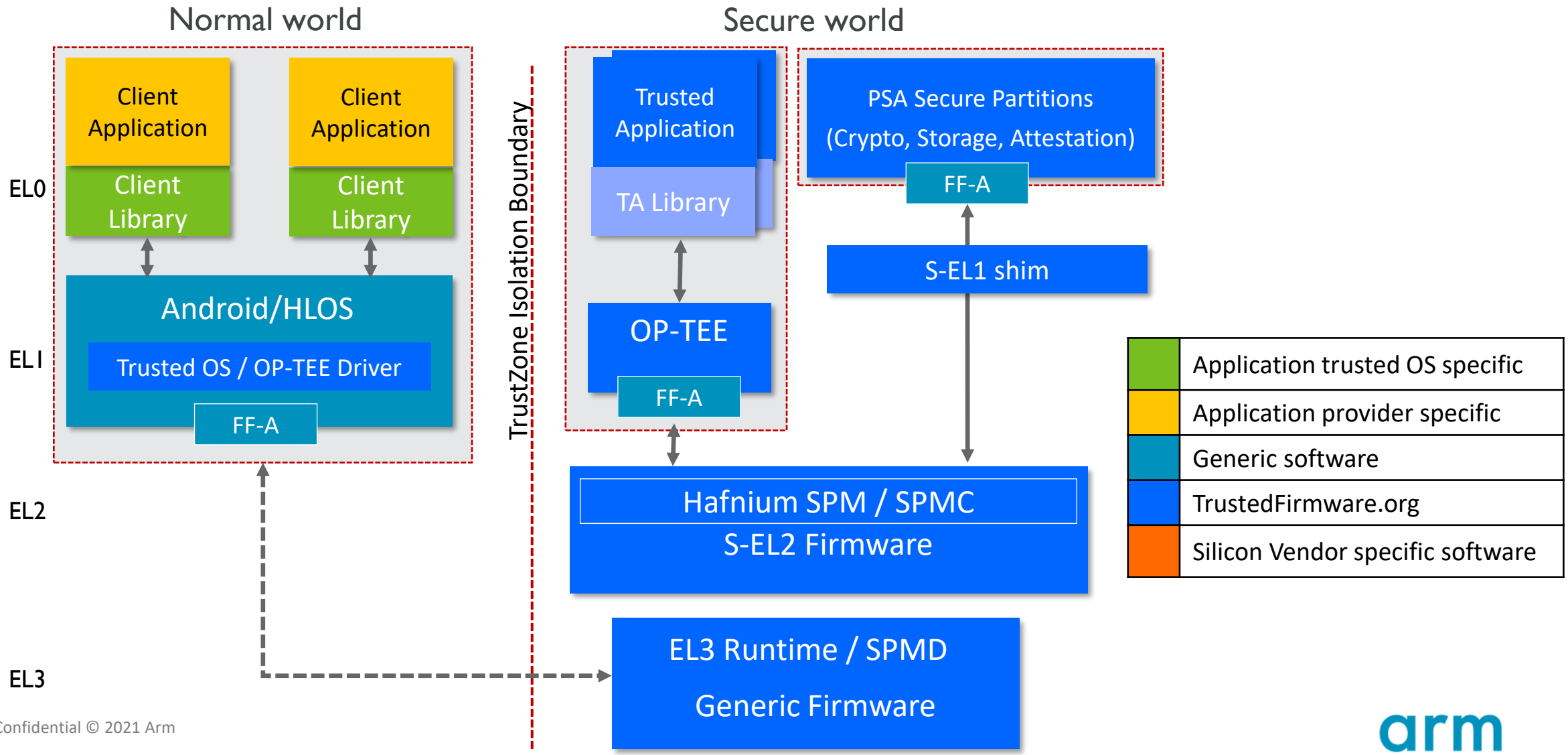


Trusted Services on pre-Armv8.4



	Application RoT Trustedfirmware.org
	Generic software
	PSA-RoT TrustedFirwmare.org
	Silicon Vendor specific software
	PSA FF-A APIs

Trusted Services on Armv8.4/Secure EL2



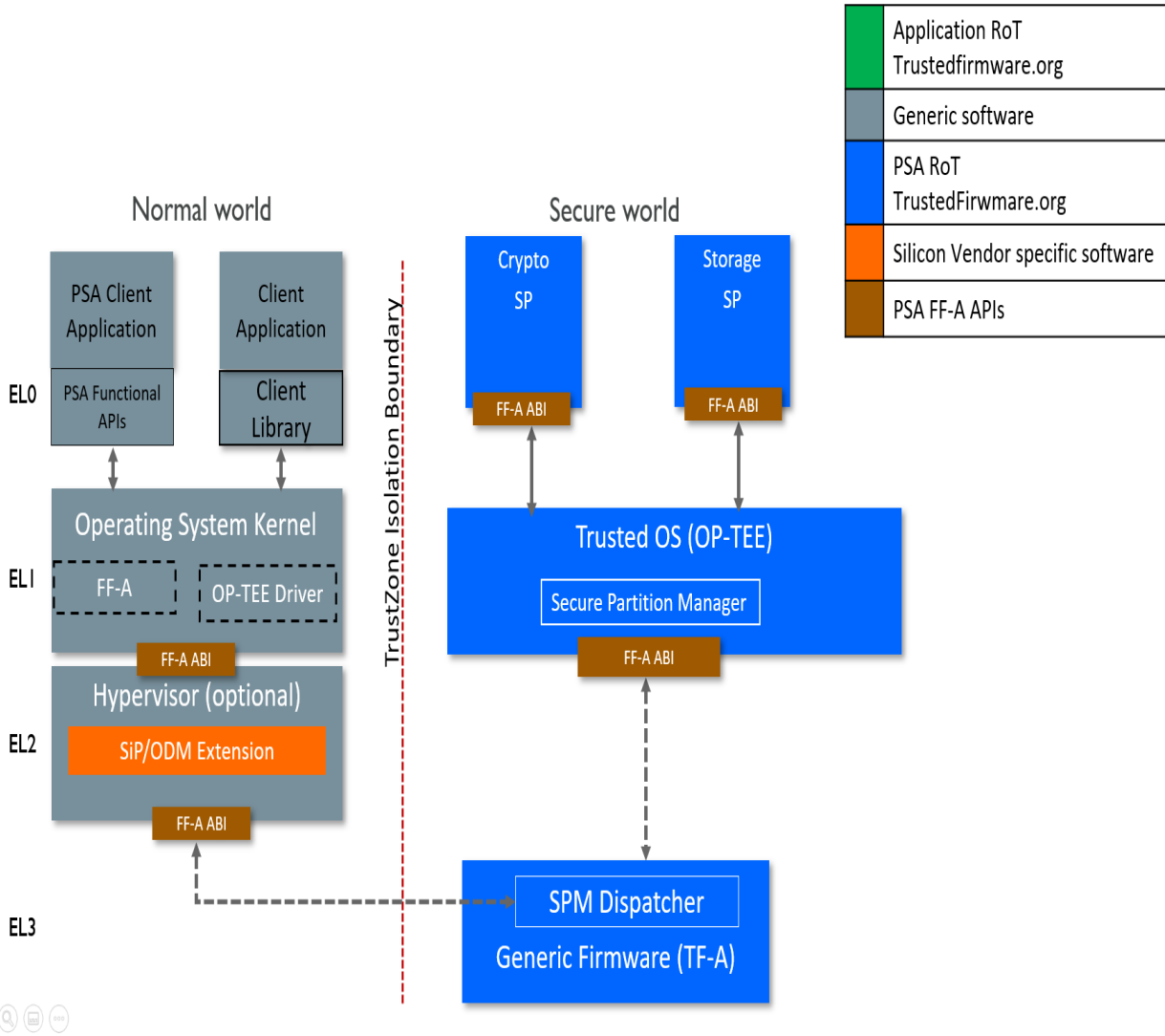
Roadmap

Released | Adv. Planning | Development | Concept | (L) … at Linaro | (C) … in Community

	Available	CY2021 Q2	CY2021 Q3	CY2021 Q4	
Trusted Services	• PSA Crypto SP • PSA Internal Trusted Storage (ITS) SP • Non-Secure Appln. Using PSA Crypto, ITS • Enable Crypto HW Integration • Hafnium/Crypto SP/ ITS SP Integration on Total Compute	• PSA Attest SP • PSA Protected Storage SP • FF-A Direct Messaging (routing extn.) • FIP based booting (earlier OP-TEE based)	• PSA Attest SP Contd. • StMM Updates (for compatibility with SPMC & co-exist with PSA SPs) • PSA Functional API Testing • 32bit Support SEL0/SP • Storage Backend Integration (nwd eMMC RPMB, secure flash)	• 32-bit Support SEL0/SP Contd. • Platform Security Firmware Update for A-profile • Meta-arm yocto support	• Shim layer for legacy TAs
OP-TEE	• SEL1: SP Loading & FF-A Message Routing	• OP-TEE SPMC – upstream contd. • StMM SPMC Implementation	• 32-bit Support (OP-TEE as monitor + SPMD) • Use upstream FF-A kernel driver	• Pass FF-A ACS • 32-bit Support (OP-TEE as monitor + SPMD) Contd. • Test suite for SPM (xtest adaptations)	• OpenCI

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



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