



**TrustedFirmware**

**OPEN SOURCE SECURE SOFTWARE**

[Trusted Firmware](#) Community Project



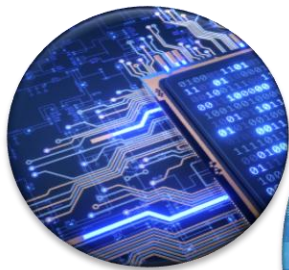
**TrustedFirmware**  
.org



**TrustedFirmware**  
.org

# Collaborative Security

Complexity  
solved once  
for all



Reference  
Secure  
Software



Governing  
bodies:  
Board & TSC

Open  
Governance  
Community  
Project



Shared  
Ownership



Security at  
Scale



# Current members

## Diamond Members

The ARM logo is the word "arm" in a lowercase, blue, sans-serif font.The Google logo is the word "Google" in its multi-colored, sans-serif font.

## Platinum Members

The Linaro logo features the word "Linaro" in a grey, sans-serif font, with a graphic of colored squares (purple, green, yellow) to its left.The NXP logo consists of the letters "NXP" in a stylized, blocky font with a color gradient from orange to green.The RENESAS logo is the word "RENESAS" in a blue, italicized, sans-serif font.The ST logo features a stylized blue "ST" monogram, with the text "life.augmented" in a smaller, blue, sans-serif font below it.

## General Members

The FUTUREWEI Technologies logo includes a red circular graphic of dots on the left, followed by the word "FUTUREWEI" in red and "Technologies" in grey.The NXM logo features the letters "NXM" in a bold, black, sans-serif font, with the "X" in red.The NORDIC SEMICONDUCTOR logo shows a blue geometric icon to the left of the words "NORDIC" and "SEMICONDUCTOR" in a black, sans-serif font.

## Partners

The bugSeng logo features the word "bugSeng" in a red, sans-serif font, with the "S" in a grey circle.The TrustedFirmware.org logo includes a green square icon with a white padlock on the left, followed by the text "TrustedFirmware.org" in a black, sans-serif font.

# Member Benefits: Highlights



Governing Board seat driving strategic direction and investments

(Budget, Marketing Initiatives, explore new investment areas)



Part of Technical Steering Committee driving technical direction of project

(Define Release process, Security Incident Handling process, Roadmaps reviews & influence)



Add and maintain platforms in Open CI (**Refer to the “Open CI & Board Farm” slide**)



Opportunity for close engineering collaboration with other members



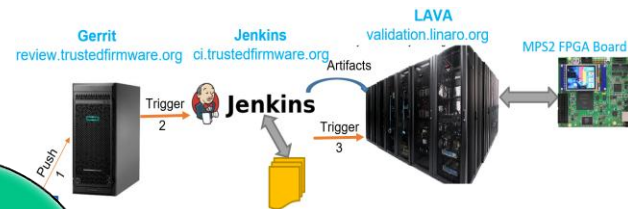
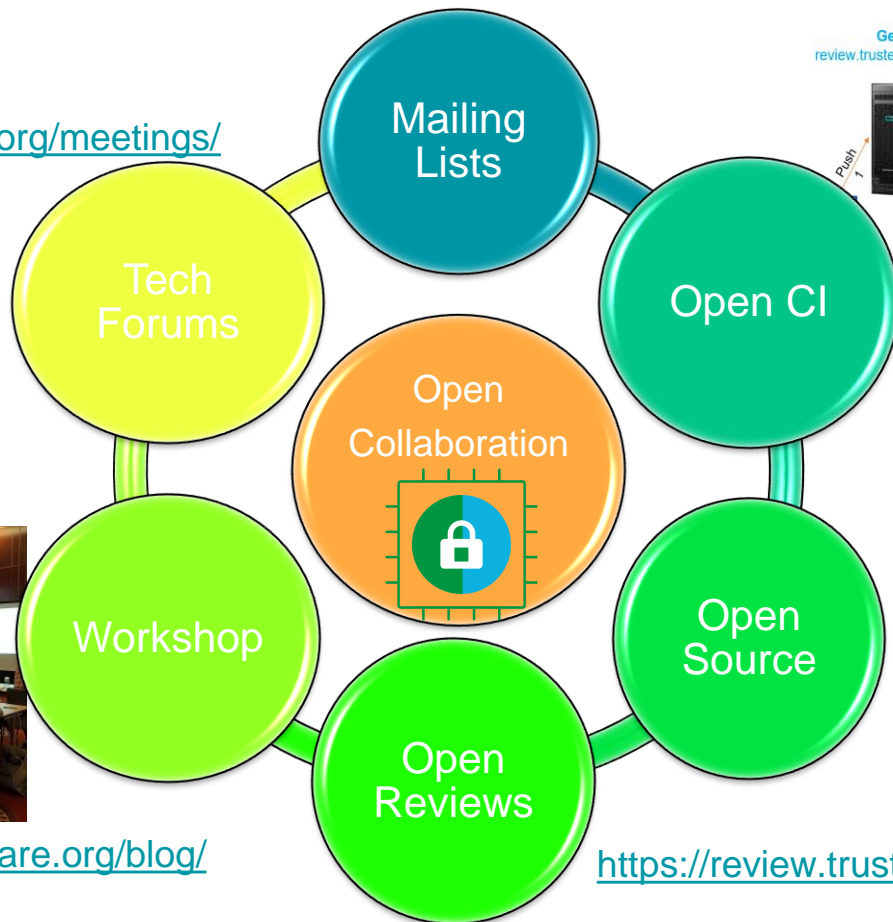
**Refer “Membership Structure” slide for details on membership tiers and benefits**



**TrustedFirmware**  
.org

# The Virtuous Circle Of Collaboration!

<https://www.trustedfirmware.org/meetings/>



<https://ci.trustedfirmware.org/>

<https://git.trustedfirmware.org/>

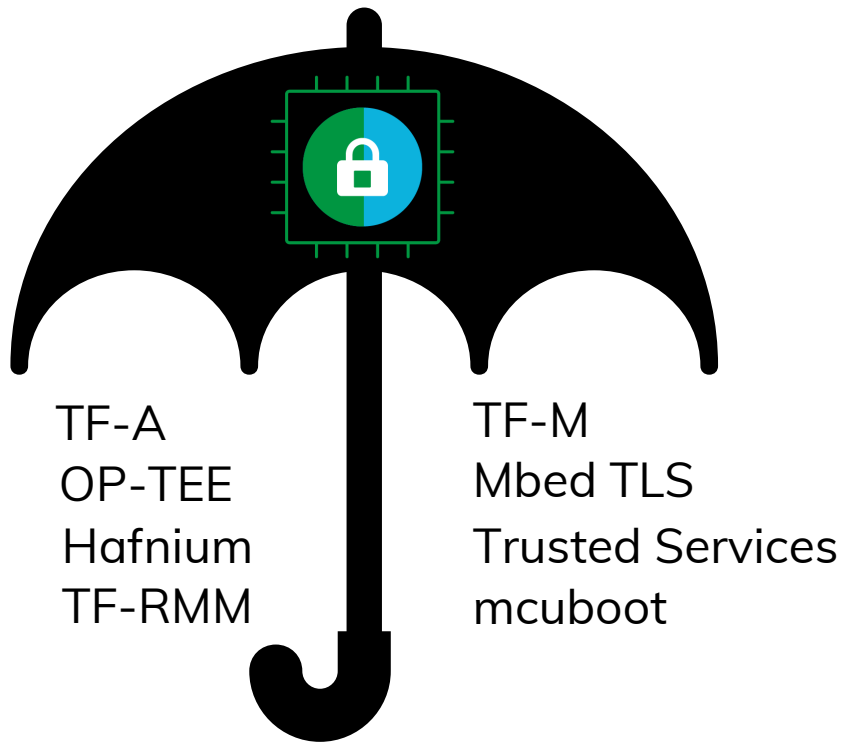
<https://review.trustedfirmware.org/>

<https://www.trustedfirmware.org/blog/>

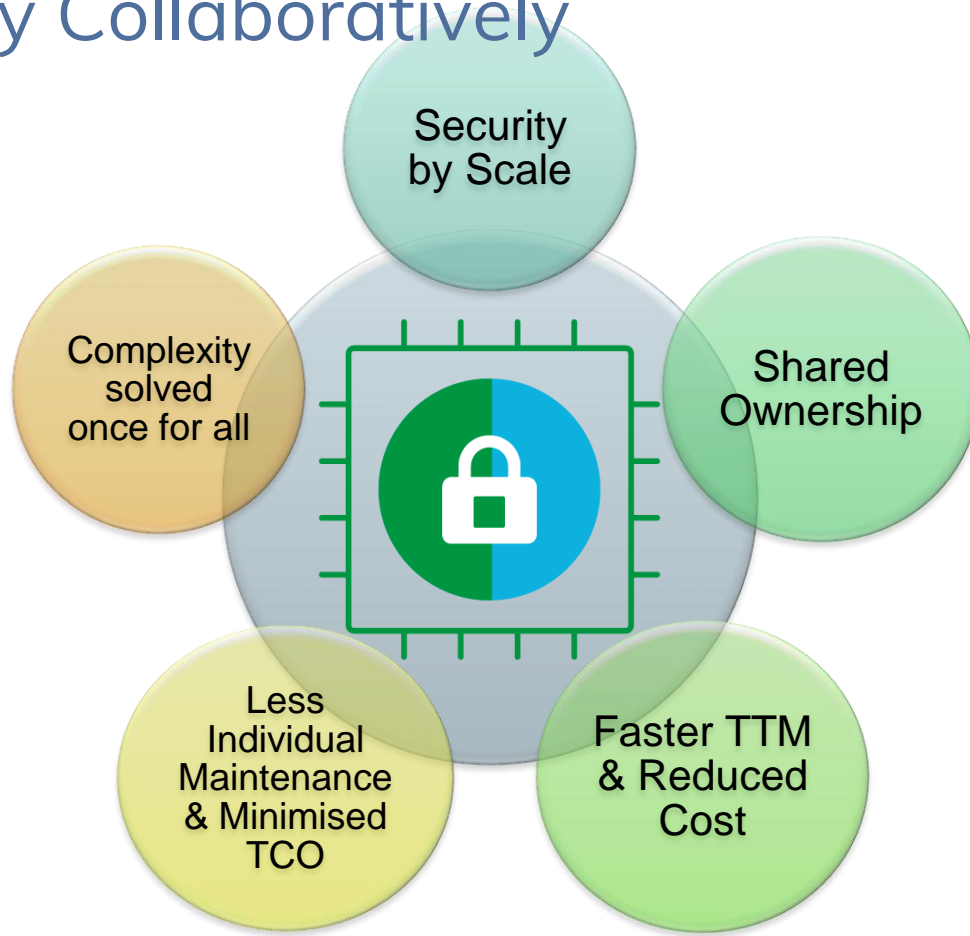


**TrustedFirmware**  
.org

# Current Projects



# Build Security Collaboratively



# All market segments

Devices

IoT/Mobile/Auto/Laptop



Embedded  
Edge

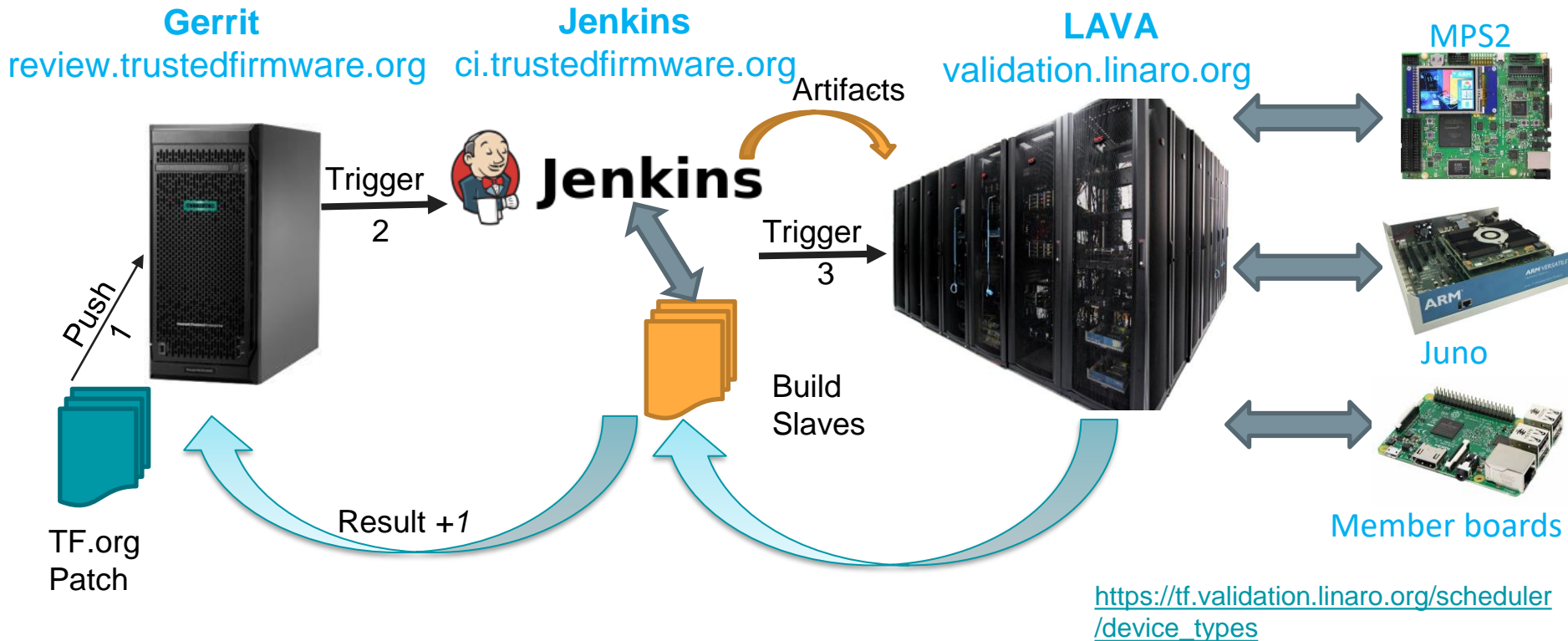


Cloud  
Server



**TrustedFirmware**  
.org

# Open CI & Board Farm



# Trusted Firmware Security Center

New centralized Security incident process

[https://developer.trustedfirmware.org/w/collaboration/security\\_center/](https://developer.trustedfirmware.org/w/collaboration/security_center/)

- Have you found a security vulnerability in Trusted Firmware?  
→ Report it here: [security@lists.trustedfirmware.org](mailto:security@lists.trustedfirmware.org)
- Coordinated disclosure with Trusted Stakeholders and ESS
  - [https://developer.trustedfirmware.org/w/collaboration/security\\_center/trusted\\_stakeholder\\_registration/](https://developer.trustedfirmware.org/w/collaboration/security_center/trusted_stakeholder_registration/)
- Per-project security email aliases
  - [https://developer.trustedfirmware.org/w/collaboration/security\\_center/mailing\\_aliases/](https://developer.trustedfirmware.org/w/collaboration/security_center/mailing_aliases/)



# TF-A very first LTS release!

- A TF.org community effort to create and maintain the first TF-A LTS release!
  - LTS v2.8.0 launched in February (based on TF-Av2.8 release)
  - Already 6 maintenance releases produced with urgent bugfix (latest LTS v2.8.6)
  - Dedicated mailing list [tfa-lts@lists.trustedfirmware.org](mailto:tfa-lts@lists.trustedfirmware.org)
- Commitment to keep it supported for 5 years
  - First year effort sustained by community members from interested companies
  - Seeking for wider engagement and contributions to achieve the LTS requirements
- Ideally a new LTS release will be created again next year, aligned with autumn TF-A release (subject to community interest and engagement)
- Full LTS requirements and proposal can be found [here](#)



# Trusted Firmware-A

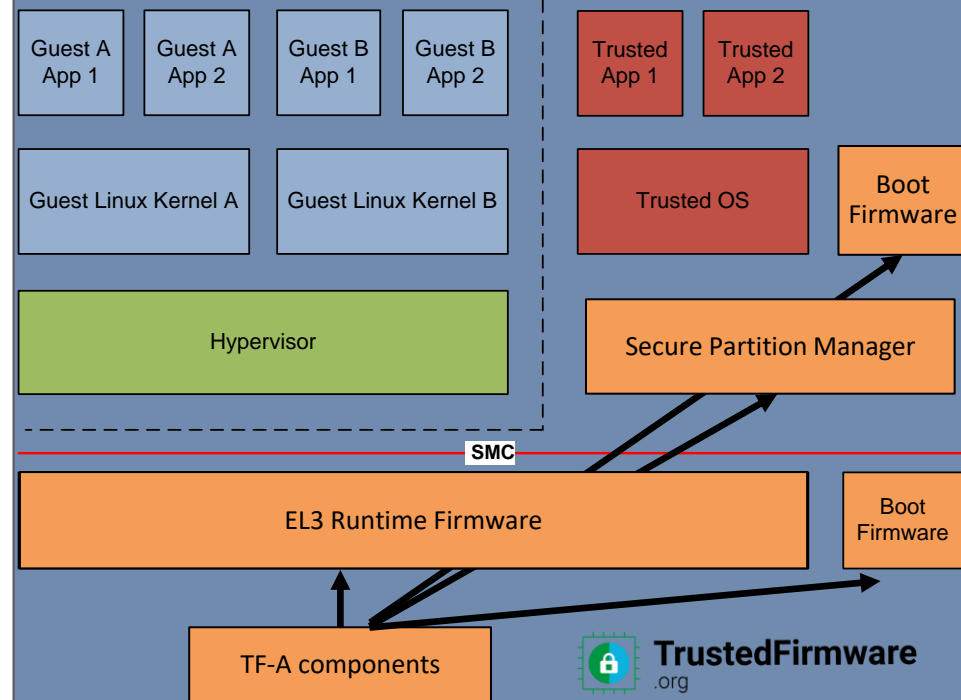
<https://trustedfirmware-a.readthedocs.io/en/latest/>

Secure world reference software for all Arm Cortex-A & Neoverse processors across all market segments.

Trusted boot flow and runtime firmware providing standard implementation of Arm specifications:

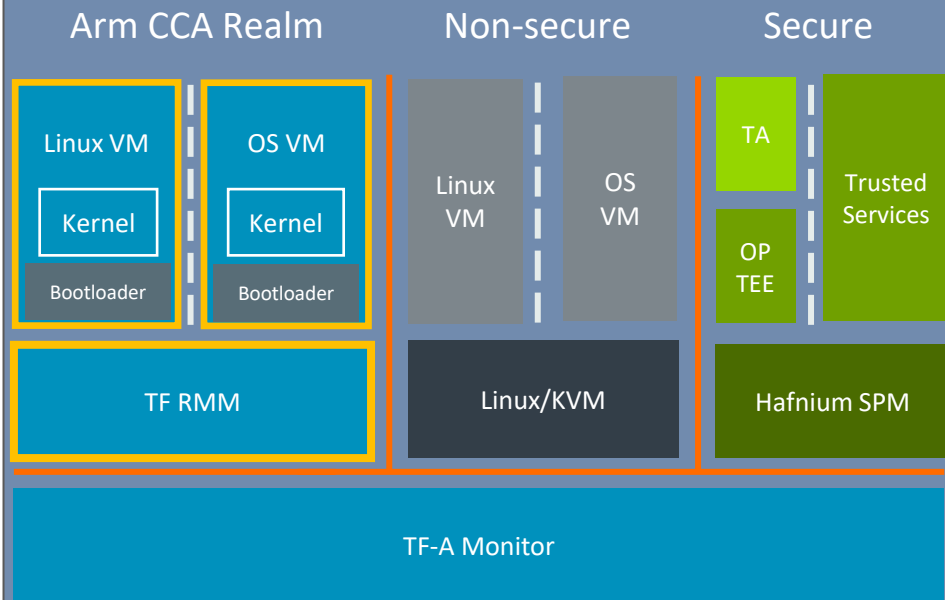
- SMCCC (SMC Calling Convention)
- TBBR (Trusted Board Boot Requirements)
- PSCI (Power State Coordination Interface)
- SCMI (System Control & Management Interface)
- FF-A (Firmware Framework for A-Profile)

## Cortex-A/Neoverse



# TF-RMM (Arm CCA)

- Reference implementation of the Arm Realm Management Monitor (RMM) [specification](#) for the Arm Confidential Compute Architecture (Arm CCA)



# TF-A-Tests

<https://trustedfirmware-a-tests.readthedocs.io/en/latest/>

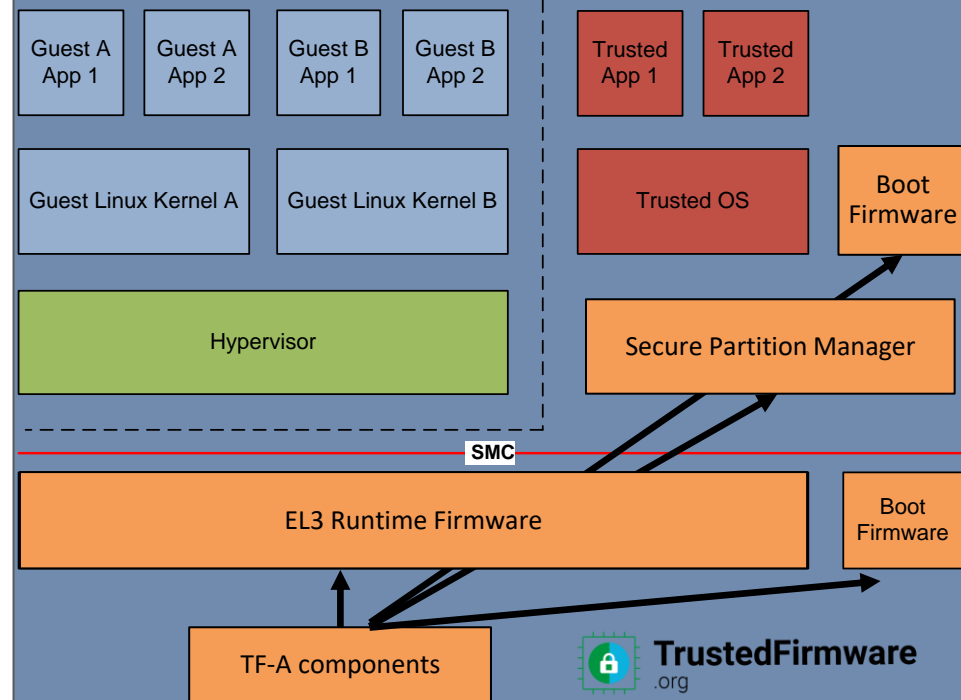
A suite of bare-metal functional tests to exercise TF-A features from the Normal World, without dependencies on a Rich OS

It provides a strong basis for TF-A developers to validate their own platform ports and add their own test cases, interacting with TF-A through its SMC interface

Features currently tested include:

- SMC Calling Convention
- Power State Coordination Interface (PSCI)
- Software Delegated Exception Interface (SDEI)
- Performance Measurement Framework (PMF)
- Trusted Board Boot Requirements (TBBR)
- Secure Partition Manager (SPM) ... and lots more!

## Cortex-A/Neoverse

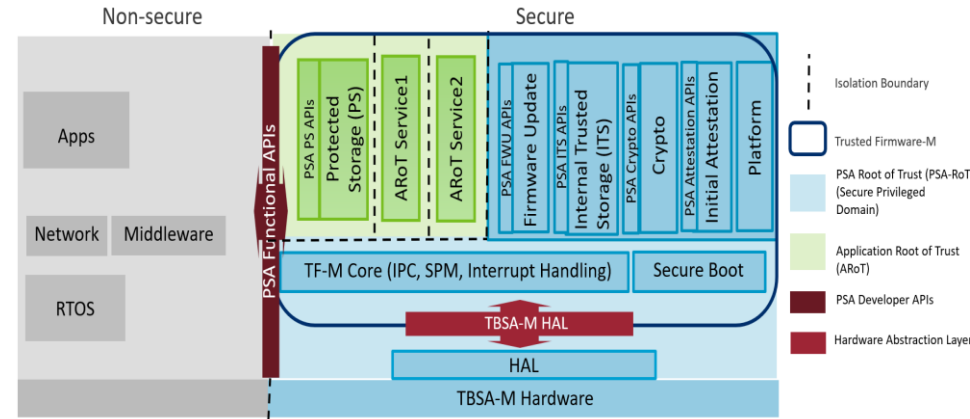


# Trusted Firmware-M

Implements the Secure Processing Environment (SPE) for Armv8-M, Armv8.1-M architectures. It is the platform security architecture reference implementation aligning with PSA Certified guidelines.

It consists of Secure Boot and a set of Secure Services such as Secure Storage, Crypto, Attestation, Firmware update. Applications accessible via PSA Functional APIs.

## Cortex-M

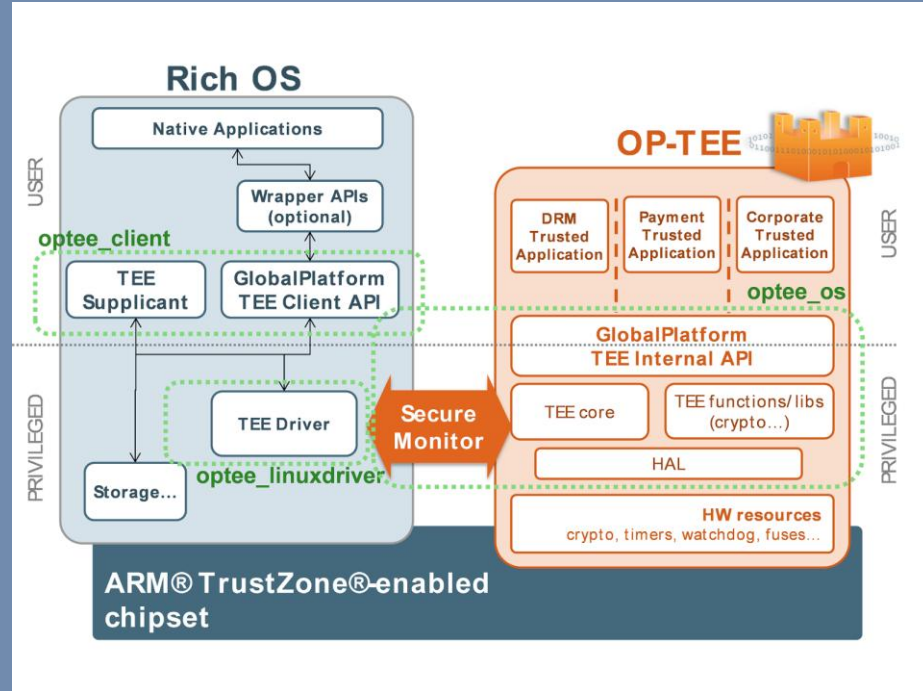


**TrustedFirmware**  
.org

# OP-TEE

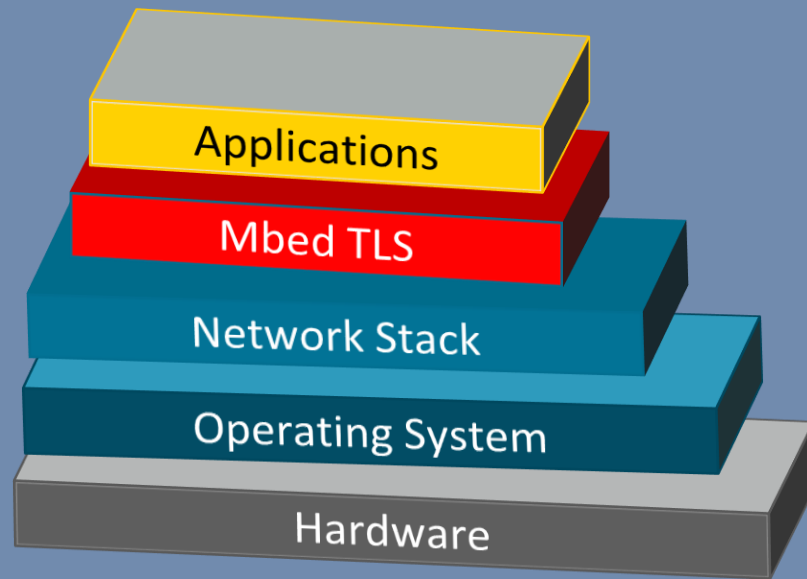
A reference implementation of a Trusted Execution Environment (TEE), designed as companion to a non-secure Linux kernel running on Arm Cortex-A cores using the TrustZone technology.

Implements [TEE Internal Core API](#) v1.1.x and the [TEE Client API](#) v1.0, as defined in the [GlobalPlatform API](#) specifications.



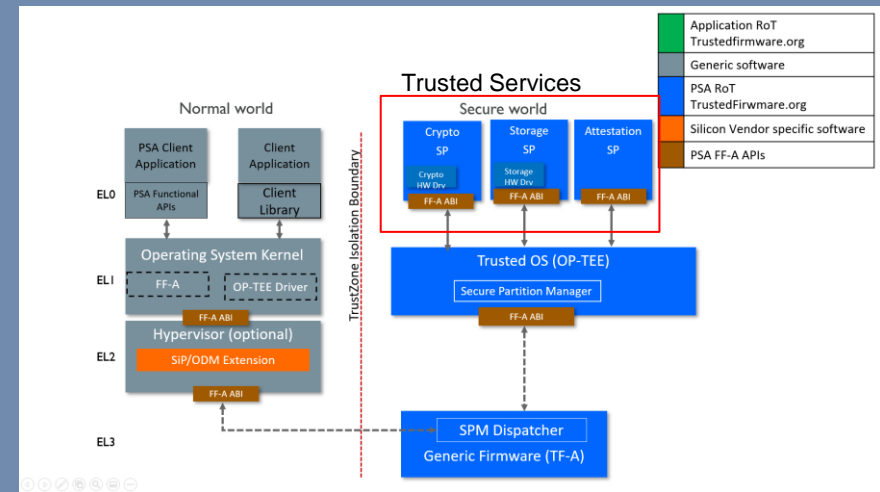
# Mbed TLS

- Portable, highly modular, easy-to-use TLS and X.509 library
- Extensively used in various market segments
- Distributed under Apache2.0 License
- Components –
  - Cryptography
  - Protocol (TLS, DTLS)
  - Certificates (X.509, PKI)
- PSA Crypto (Mbed Crypto), derived from Mbed TLS library, brings together Crypto primitives and makes them available via. PSA Crypto APIs.
- PSA Crypto also support driver interfaces to integrate with Secure Elements and Crypto Accelerators.

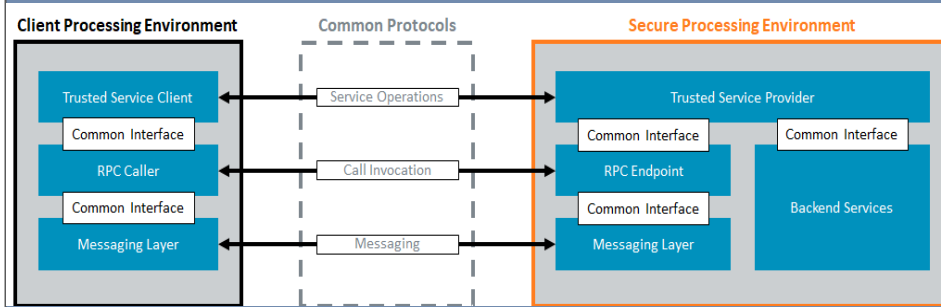


# Trusted Services

- Framework to develop Security related Services
- Deployable over range of Isolated Processing Environments (e.g., Secure EL0 Partitions under OP-TEE, Secure Partition under Hafnium.)
- Applications access Trusted Services for Security Operations via. a standardized service layer
- Includes PSA Trusted Services for Cryptography, Storage and Attestation and other Secure Services

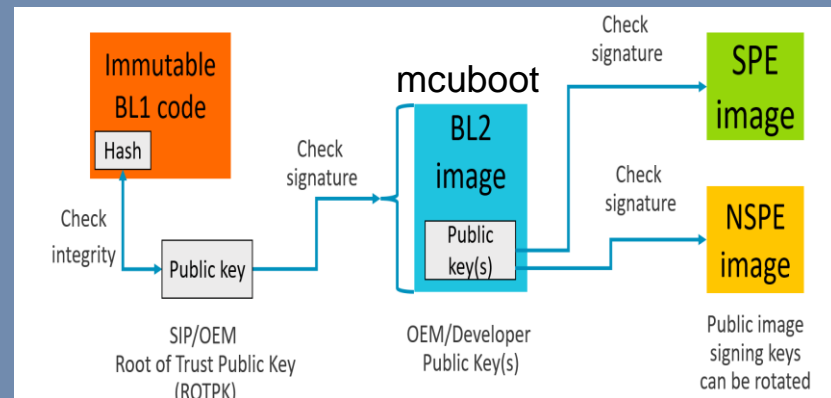


## Layered Model Of Trusted Services



# MCUBoot

- Secure bootloader
- Widely deployed secure boot solution
- Define a common infrastructure for the bootloader, system flash layout on microcontroller systems
- Enables simple software upgrades
- Used as BL2 bootloader in TF-M
- MCUboot is operating system and hardware independent and provides a hardware abstraction layer.



TF-M Boot flow



**TrustedFirmware**  
.org

# Membership Structure

**\*: Only for G2 & G3 General members**

G1: \$2.5K (0 to 50 empl. only)

G2: \$10k (0-499)

G3: \$25k (500+)

	Diamond	Platinum	General	Community (Uni/Non-profit)	Individual (invite only)	Non- Member
Code Access, Review Participation	Yes	Yes	Yes	Yes	Yes	Yes
Technical Forums	Yes	Yes	Yes	Yes	Yes	Yes
Logo and marketing recognition (scaled per tier)	Yes	Yes	Yes	Yes	N/A	No
Technical Steering Committee (TSC) seat + vote	Yes (2 votes each)	Yes (1 vote each)	Yes (1 vote every 5)	Yes (1 vote every 5)	Yes	No
Governing Board seat + vote	Yes (2 votes each)	Yes (1 vote each)	Yes* (1 vote every 5)*	Yes (1 vote every 5)	No	No
Boards in Open CI	2 new / year	1 new / year	No	No	No	No
Fees	\$100k	\$50k	G1: \$2.5K G2: \$10K G3: \$25K	\$2.5K	\$500	No

Additional benefits will be evaluated and revisited for future investment topics (MISRA, LTSs, ...) when it happens

Thank you

# Adopt Trusted Firmware to build your next secure platform

Visit [www.TrustedFirmware.org](http://www.TrustedFirmware.org) or email  
[enquiries@trustedfirmware.org](mailto:enquiries@trustedfirmware.org) for more information