Trusted Firmware Community Project

TrustedFirmware.org

TrustedFirmware
.org

Collaborative Security

Reference
Secure
Software

Complexity
solved once
for all

Governing
bodies:
Board & TSC

Shared
Ownership

Security at
Scale

Current members

Diamond Members

arm

Google

Platinum Members

Linaro

NXP

RENESAS

General Members

Partners

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

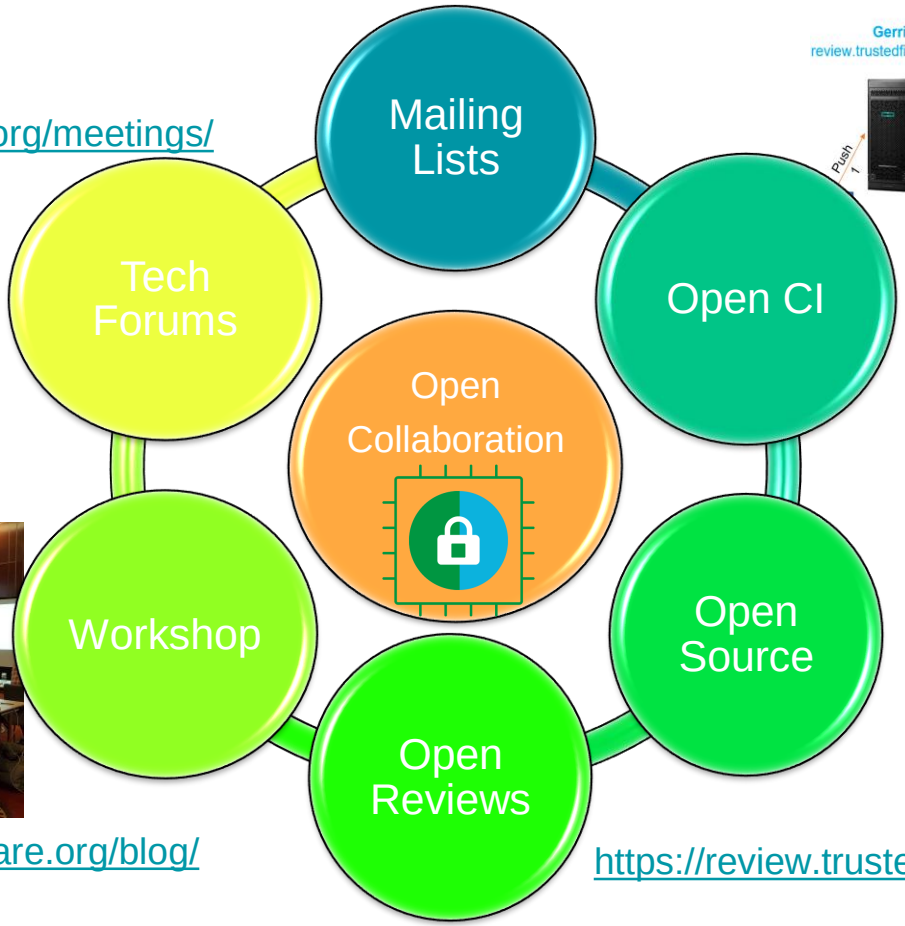
Refer “Membership Structure” slide for details on membership tiers and benefits

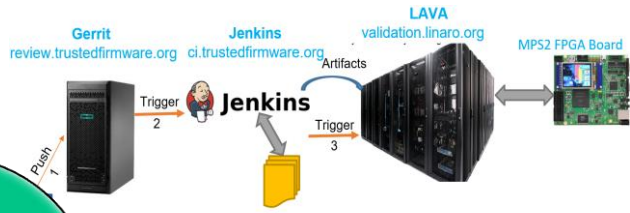
TrustedFirmware.org

The Virtuous Circle Of Collaboration!

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

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





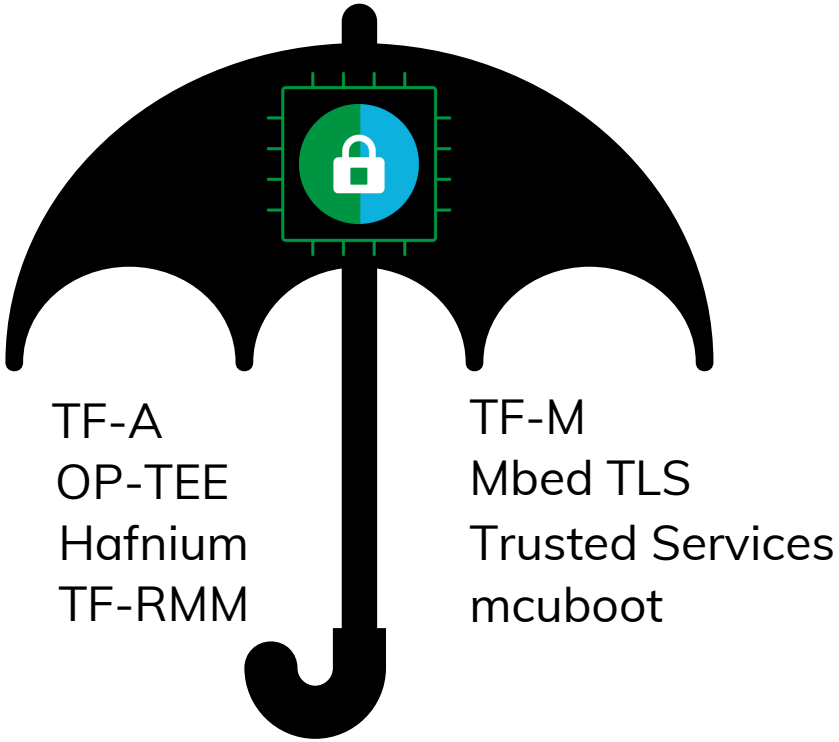
https://ci.trustedfirmware.org/

https://git.trustedfirmware.org/

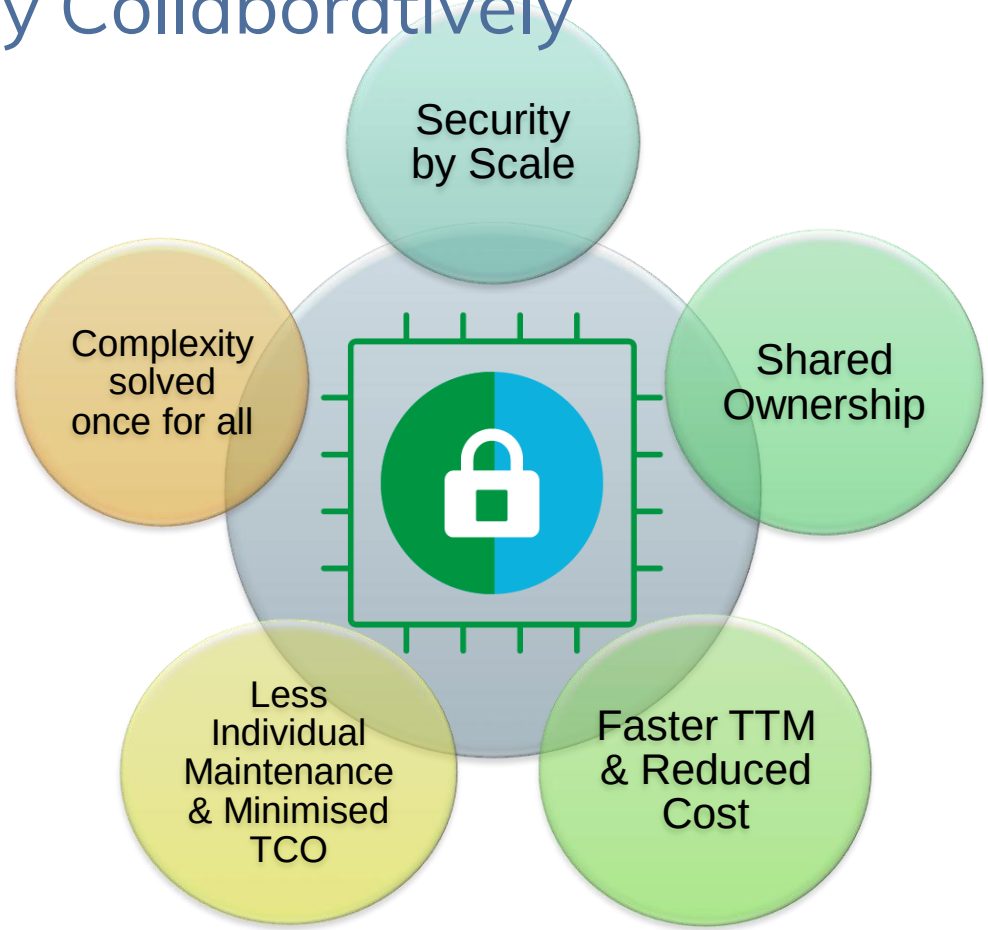
https://review.trustedfirmware.org/

TrustedFirmware.org

Current Projects



Build Security Collaboratively



TrustedFirmware.org

All market segments

Devices

IoT/Mobile/Auto/Laptop

Embedded

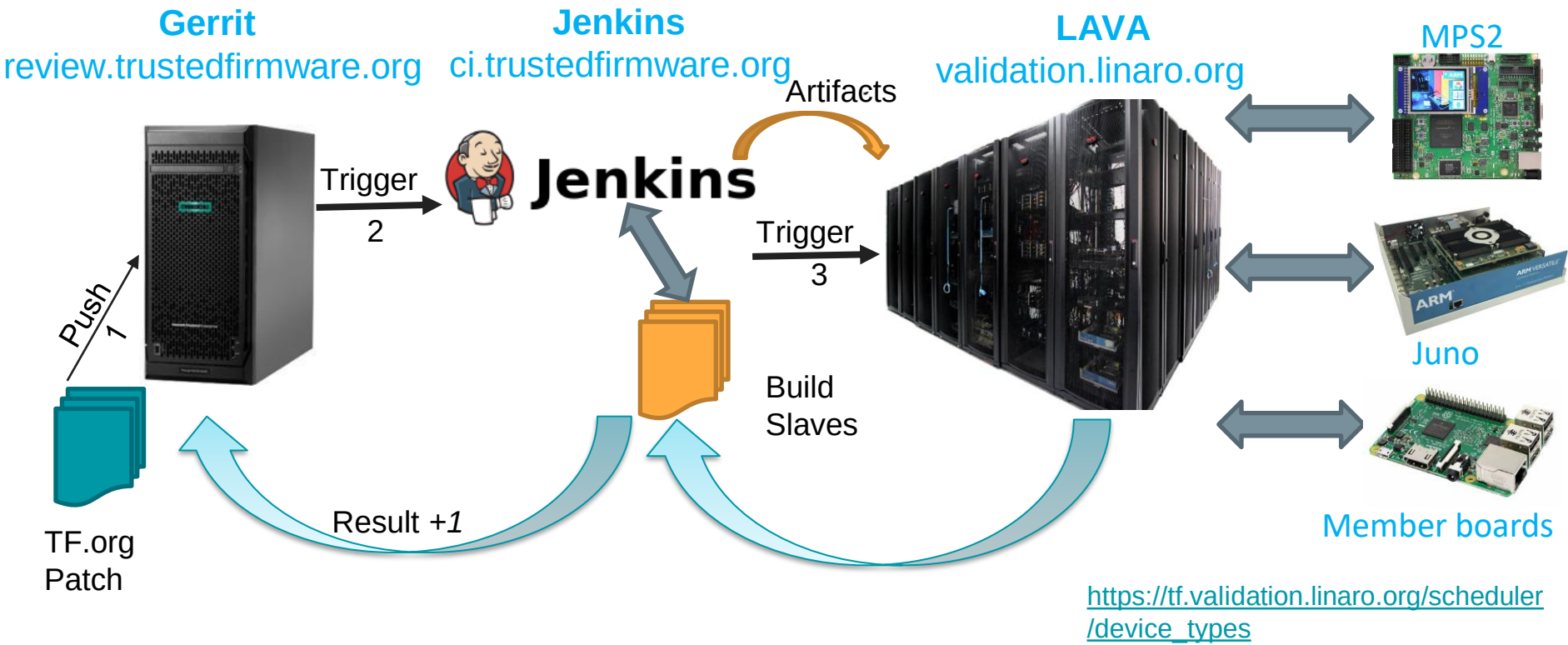
Edge

Cloud

Server

TrustedFirmware.org

Open CI & Board Farm



https://tf.validation.linaro.org/scheduler/device_types

Trusted Firmware Security Center

New centralized Security incident process

https://developer.trustedfirmware.org/w/collaboration/security_center/

- Have you found a security vulnerability in Trusted Firmware?

  → **Report it here: security@lists.trustedfirmware.org**

- Coordinated disclosure with Trusted Stakeholders and ESS
  - 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/

TrustedFirmware.org

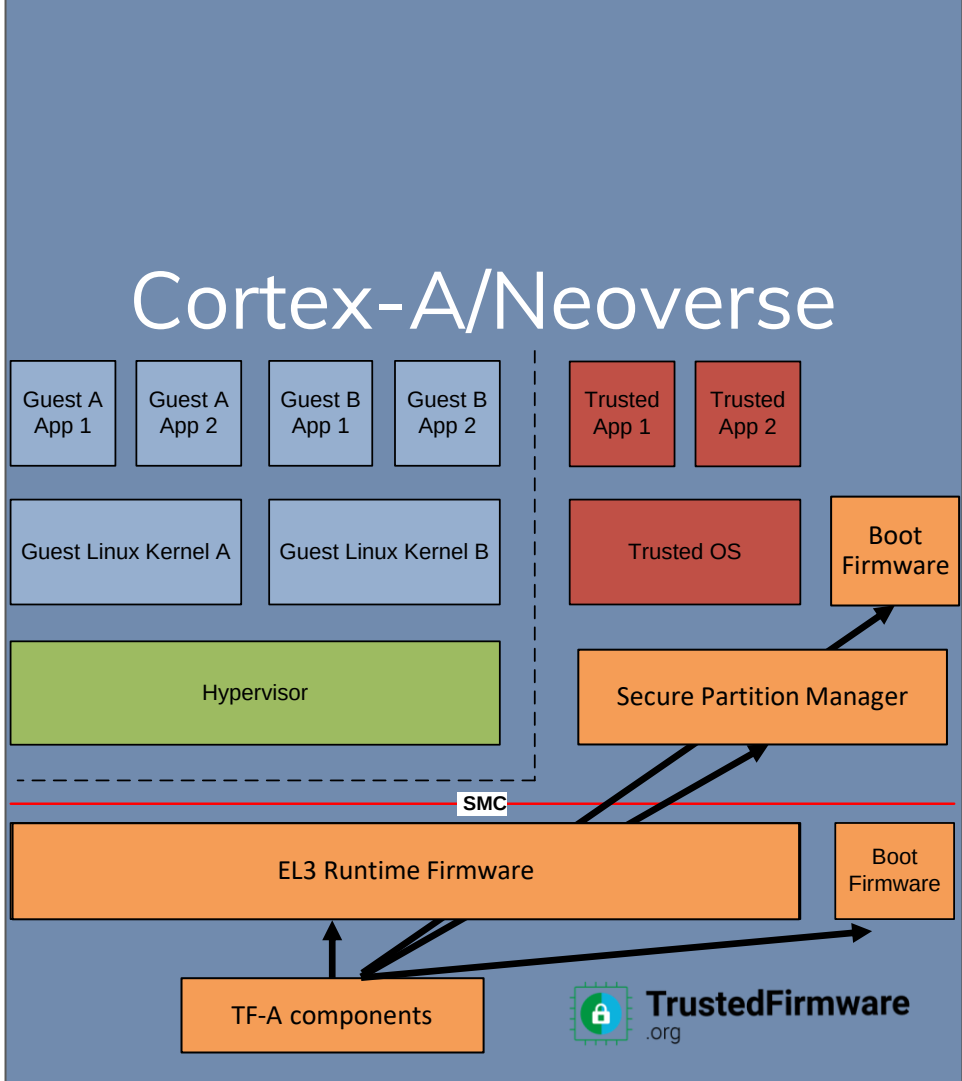
Trusted Firmware-A

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

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

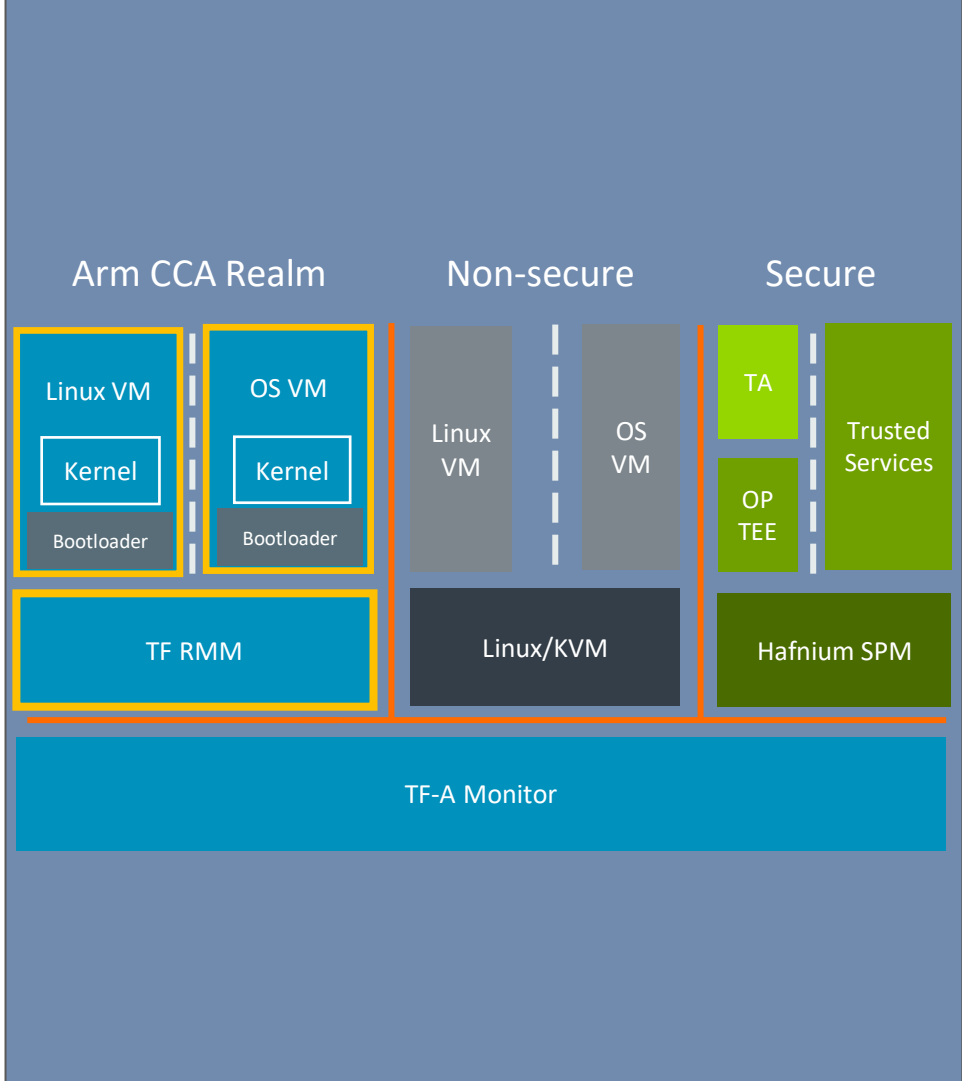
Trusted boot flow and runtime firmware providing standard implementation of Arm specifications:

- 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)



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

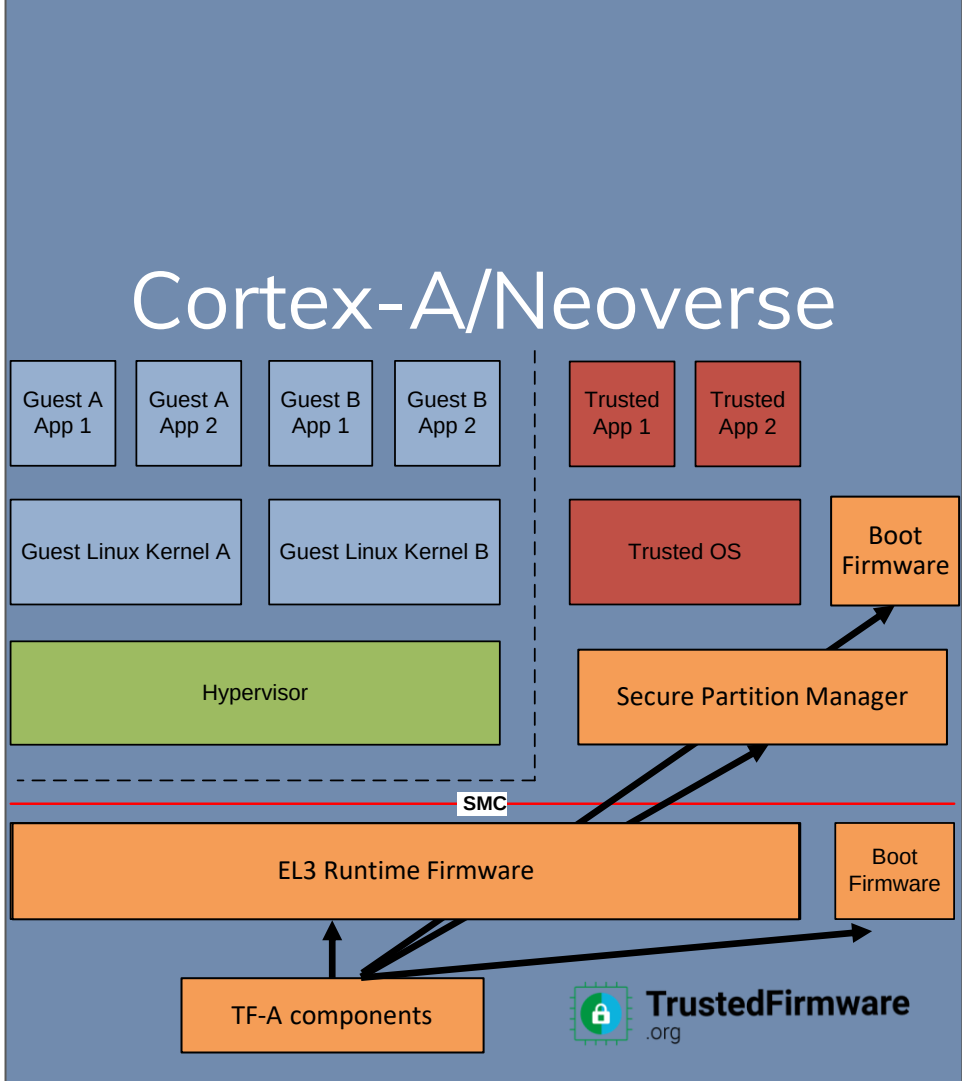
https://trustedfirmware-a-tests.readthedocs.io/en/latest/

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!

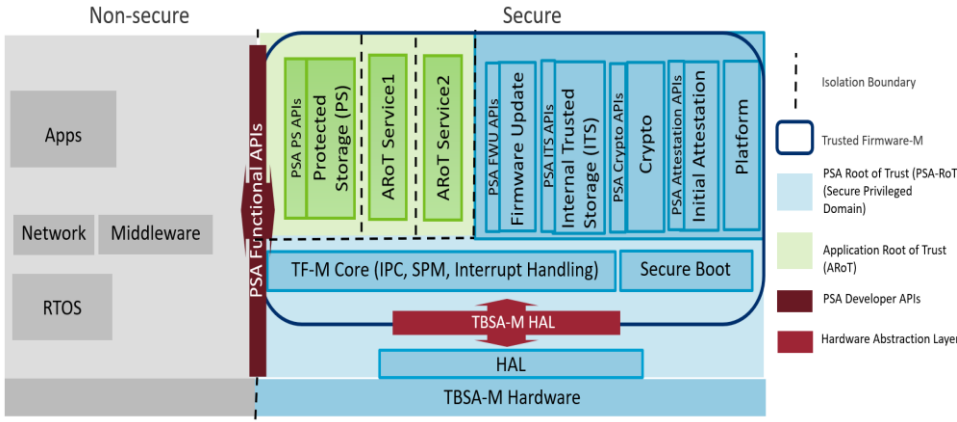


Trusted Firmware-M

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 . for Applications accessible via PSA Functional APIs.

Cortex-M

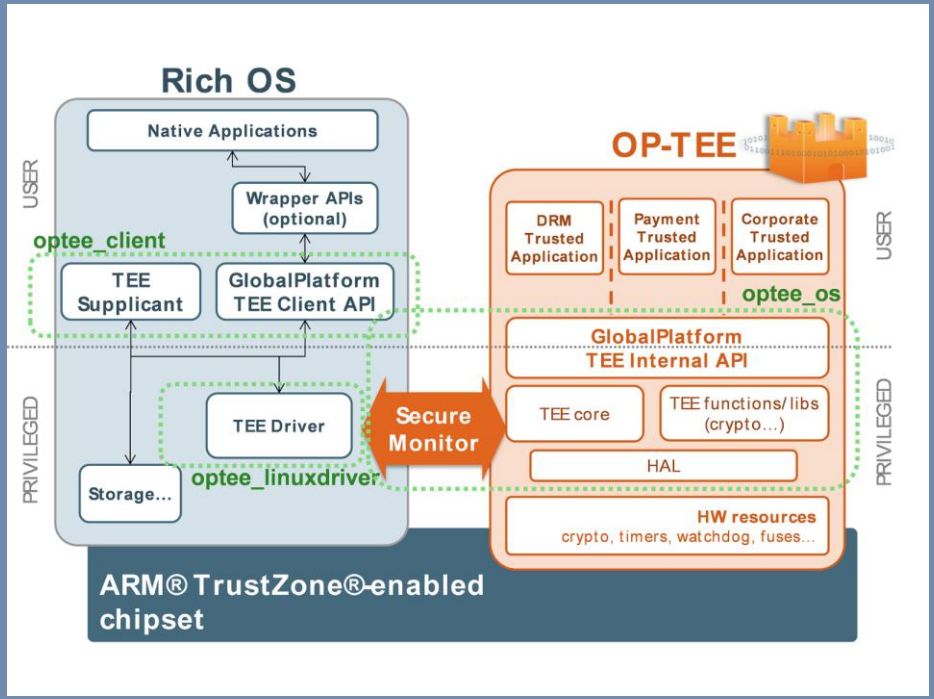


TrustedFirmware.org

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.

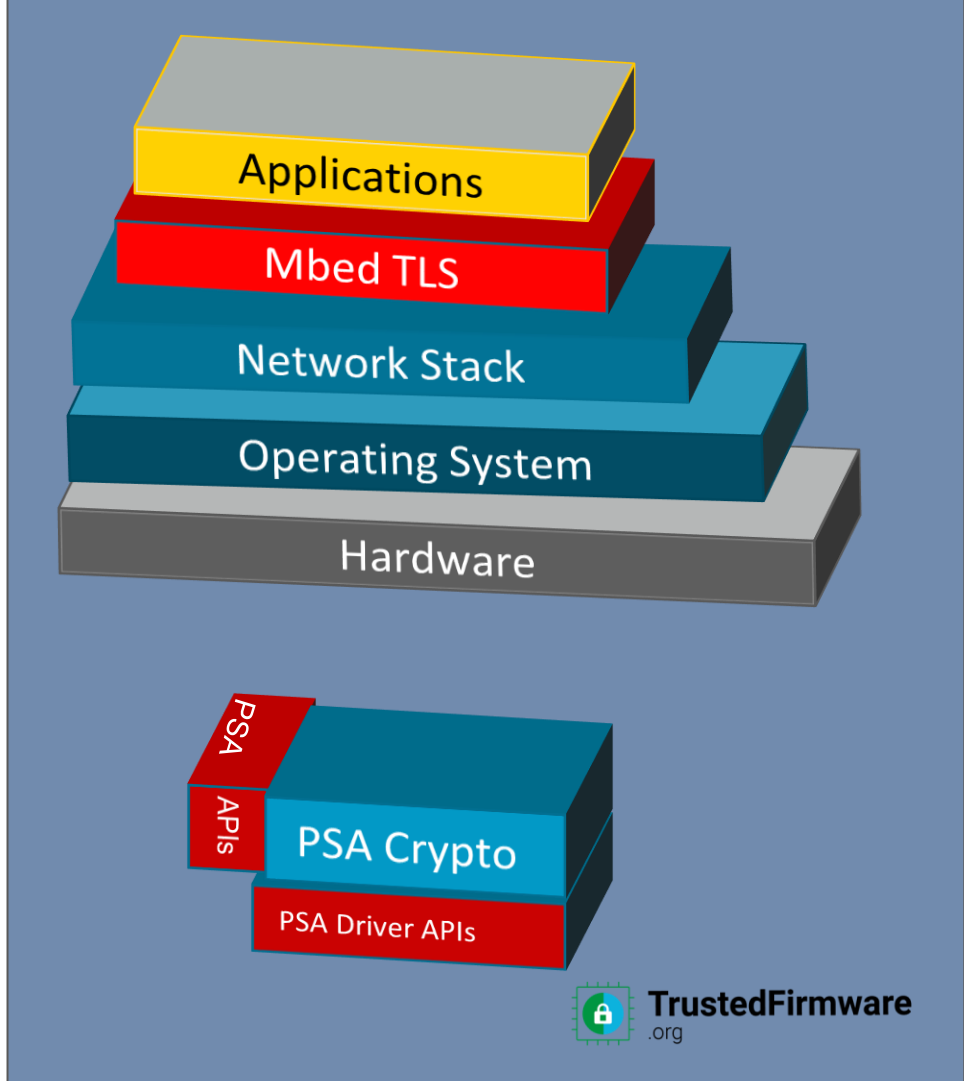
Implements TEE Internal Core API v1.1.x and the TEE Client APIv1.0, as defined in the GlobalPlatform API specifications.



TrustedFirmware.org

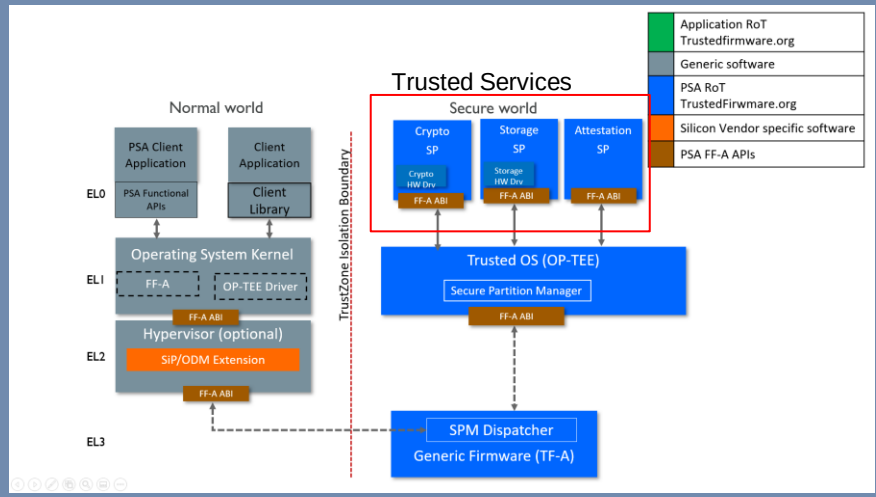
Mbed TLS

- 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.

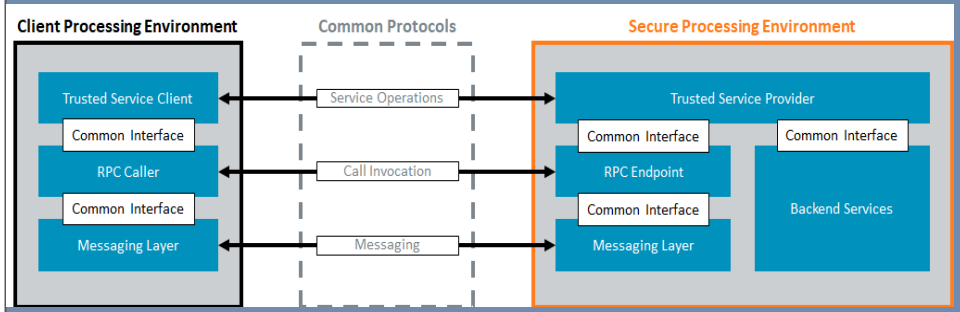


Trusted Services

- 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



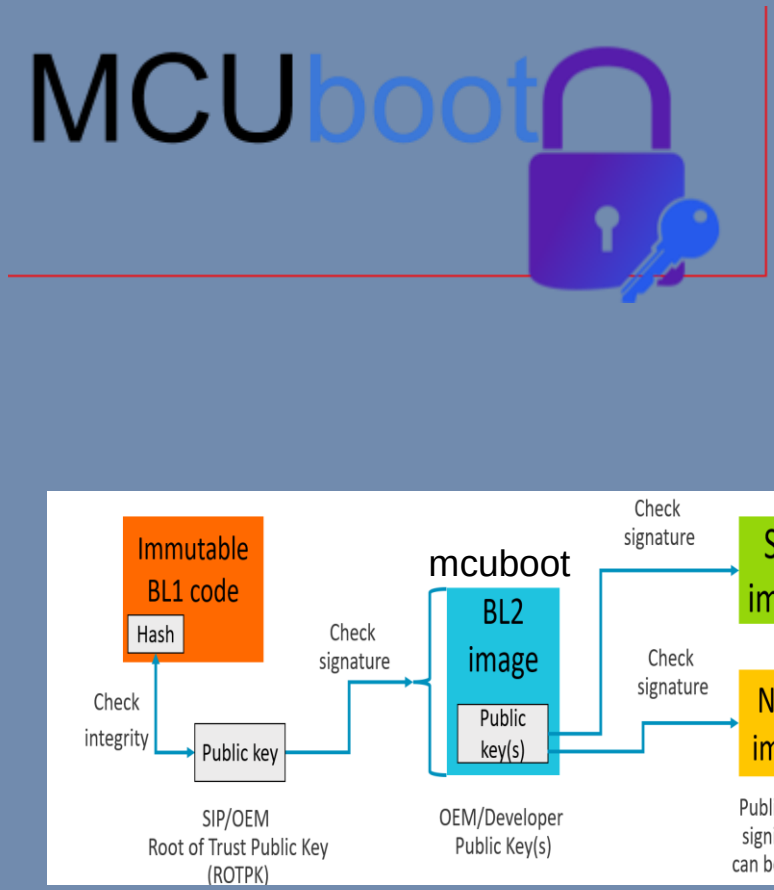
Layered Model Of Trusted Services



TrustedFirmware.org

MCUBoot

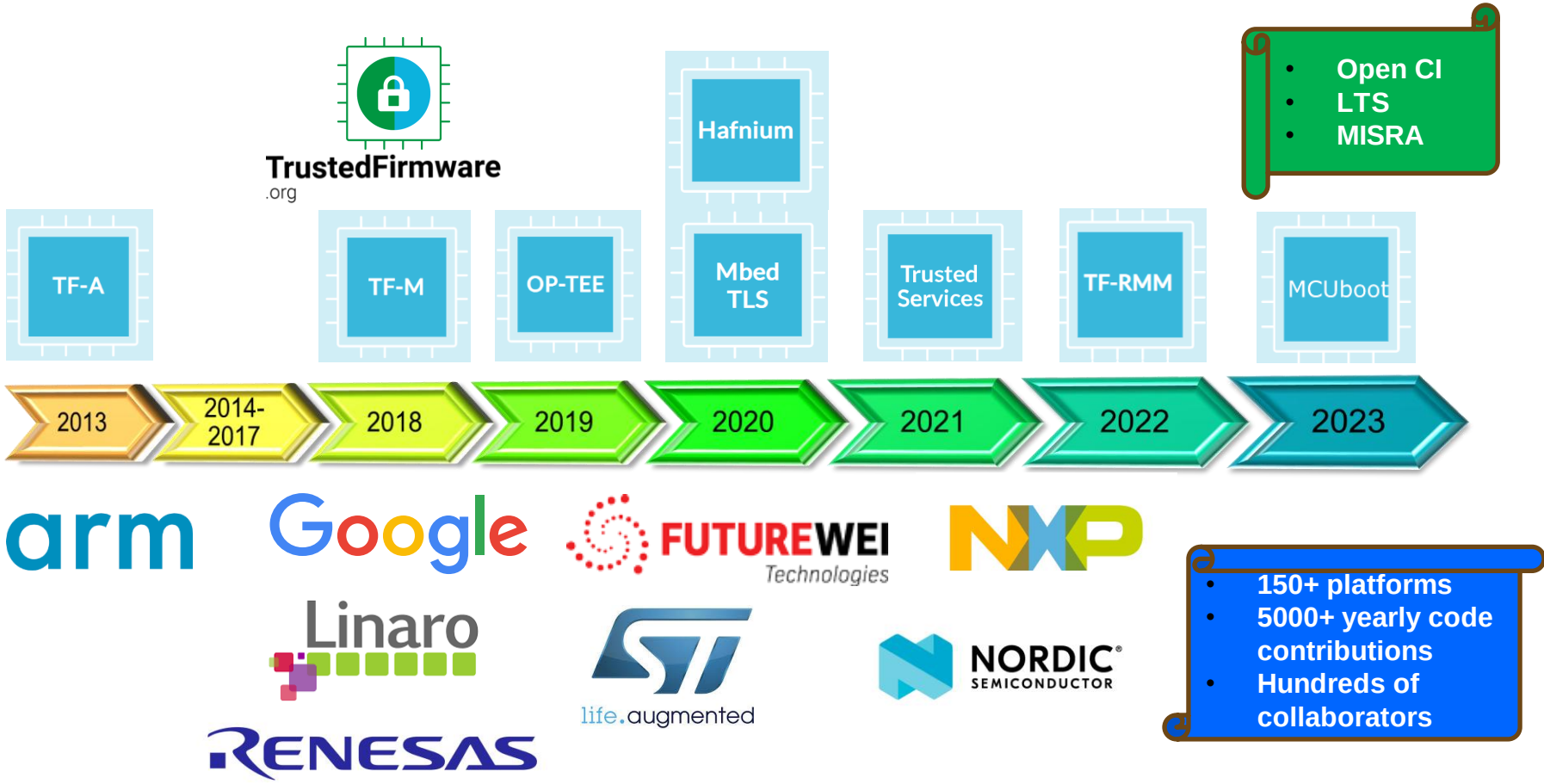
- Secure bootloader
- Widely deployed secure boot solution
- Define a common infrastructure for the bootloader, system flash layout on microcontroller systems
- Enables simple software upgrades
- Used as BL2 bootloader in TF-M
- MCUboot is operating system and hardware independent and provides a hardware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



TF-M Boot flow

TrustedFirmware.org

10yrs of growing collaboration in building security



Membership Structure

***: Only for G2 & G3 General members**
G1: $3K (0 to 50 empl. only)
G2: $12k (0-499)
G3: $30k (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	1 (D1) or 2 (D2) new / year	1 new / year	No	No	No	No
Fees	**D1: $100k D2: $120k**	**$60k**	**G1: $3K G2: $12K G3: $30K**	**$3K**	**$600**	No

Thank you

Adopt Trusted Firmware to build your next secure platform

Visit www.TrustedFirmware.org or email enquiries@trustedfirmware.org for more information