TrustedFirmware.org Community Project Overview

January 2024

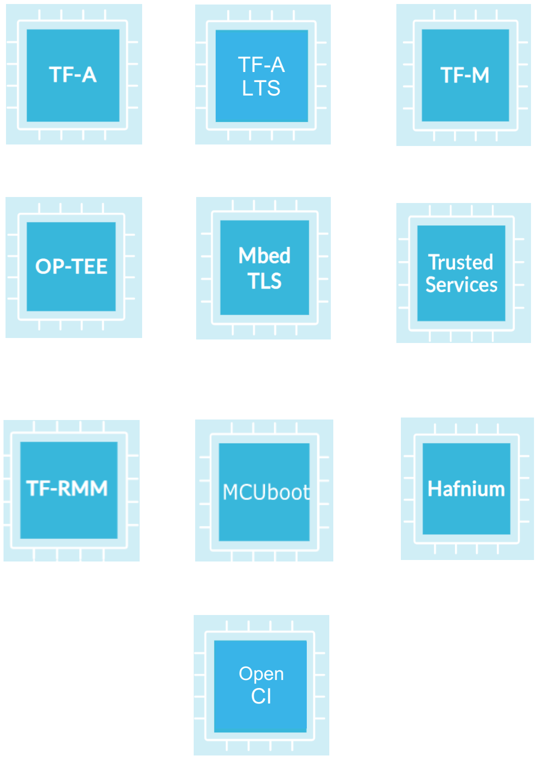
TrustedFirmware
.org

TrustedFirmware.org Overview

TrustedFirmware
.org

Trusted Firmware provides a reference implementation of secure software for, but not limited to, **Armv8-A, Armv9-A** and **Armv8-M** architectures. It provides SoC developers and OEMs with a reference trusted code base complying with the relevant Arm specifications.

- Provides the preferred software implementation of the Arm specifications allowing quick and easy porting to modern chips and platforms.
- Forms the foundations of a **Trusted Execution Environment (TEE)** on application processors, or the **Secure Processing Environment (SPE)** of microcontrollers.



TF-A

TF-A LTS

TF-M

OP-TEE

Mbed TLS

Trusted Services

TF-RMM

MCUboot

Hafnium

Open CI

Collaborative Security

Open Governance Community Project

Reference Secure Software

Governing bodies: Board & TSC

Security at Scale

Shared Ownership

Complexity solved once for all

Member Benefits: Highlights

TrustedFirmware.org

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

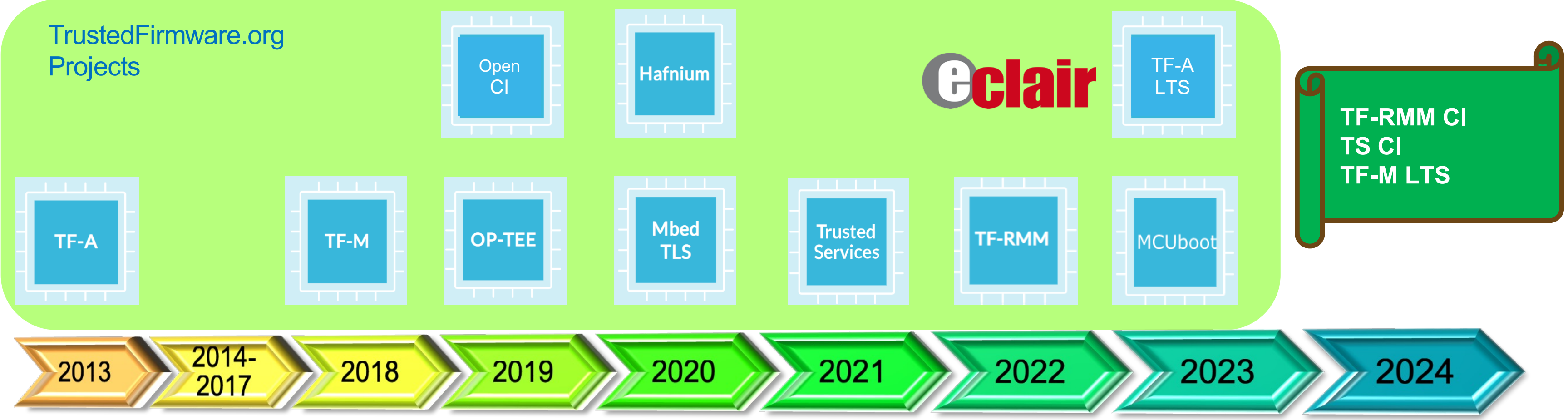
(Define Release process, Security Incident Handling process, Roadmaps reviews & influence)

Add and maintain platforms in Open CI (Refer to the “Open CI Summary” section below)

Opportunity for close engineering collaboration with other members

Refer to “Membership Structure & Benefits” slide below for more details

10yrs of growing collaboration in building security



TF-RMM CI
TS CI
TF-M LTS

arm

Google

FUTUREWEI Technologies

PROVENRUN

Linaro

ST life.augmented

NXP

NORDIC SEMICONDUCTOR

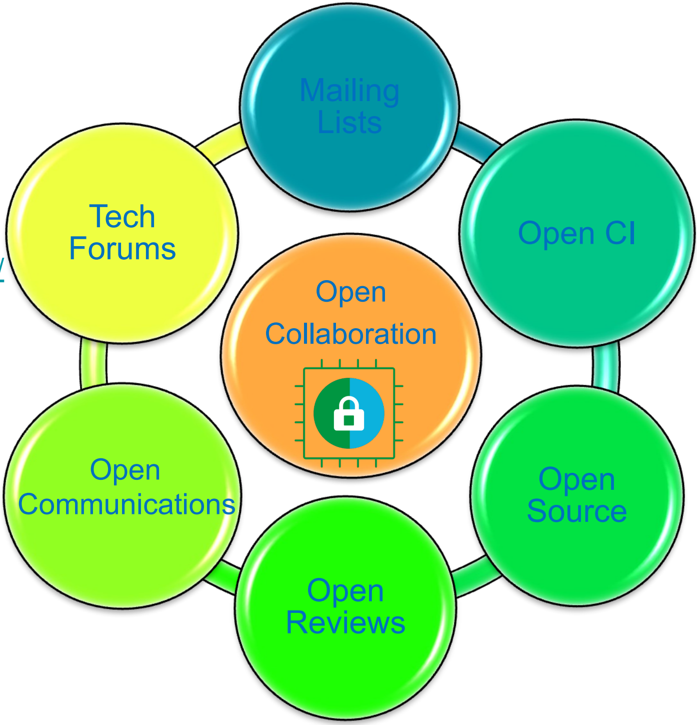
RENESAS

- 150+ platforms
- 5000+ yearly code contributions
- Hundreds of collaborators

The Virtuous Circle Of Collaboration!

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

https://lists.trustedfirmware.org/mailman3/lists/



Mailing Lists

Open CI

Open Source

Open Reviews

Open Communications

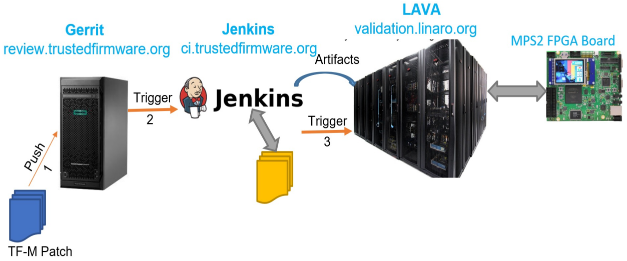
Tech Forums

Open Collaboration

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

TrustedFirmware Discord Server

https://review.trustedfirmware.org/



Gerrit
review.trustedfirmware.org

Jenkins
ci.trustedfirmware.org

LAVA
validation.linaro.org

MPS2 FPGA Board

Push 1

Trigger 2

Trigger 3

Artifacts

Jenkins

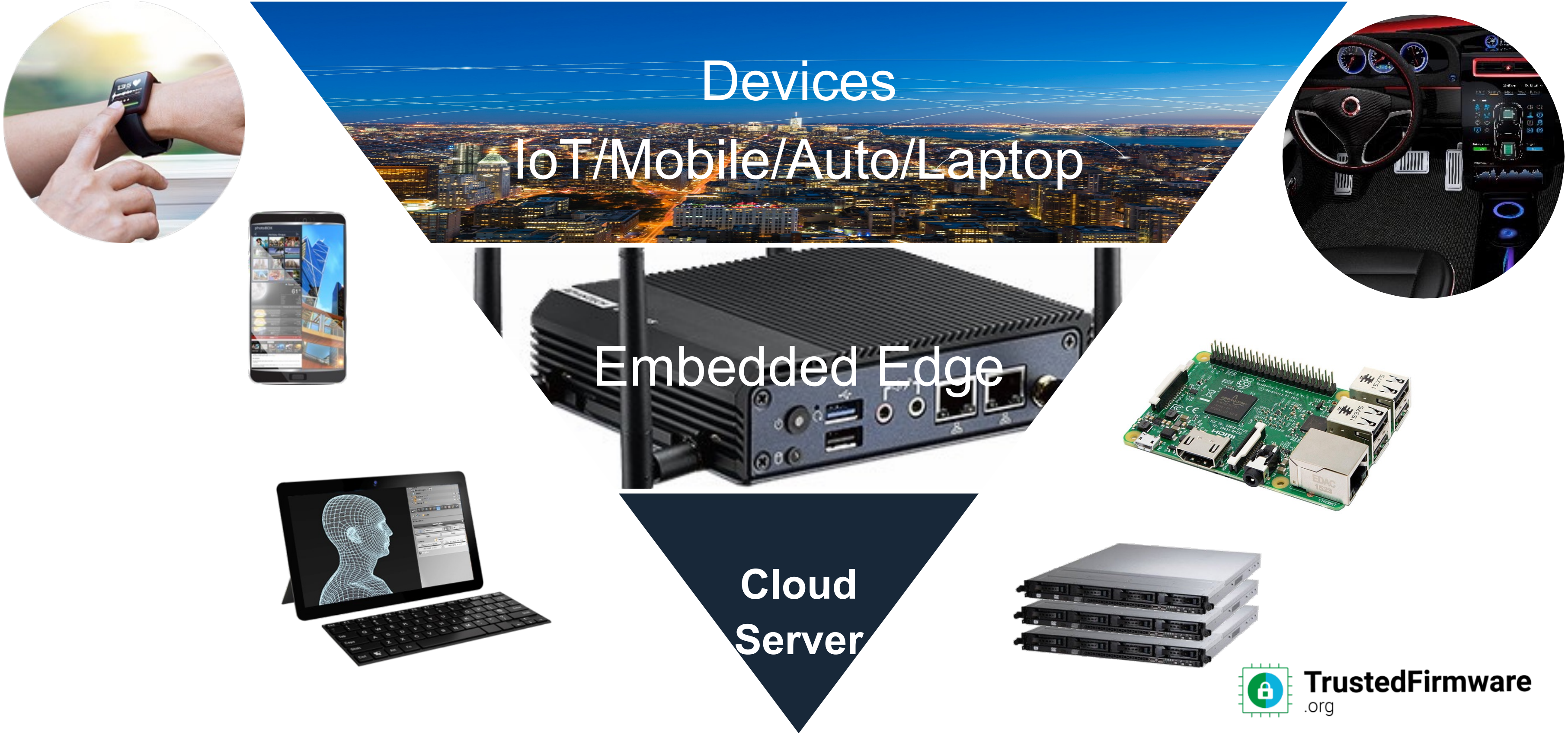
TF-M Patch

https://ci.trustedfirmware.org/
https://mbedtls.trustedfirmware.org/
https://tf.validation.linaro.org/

https://git.trustedfirmware.org/

TrustedFirmware .org

For all market segments



Trusted Firmware Security Center

TrustedFirmware.org security incident handling and vulnerability disclosure process.

- https://trusted-firmware-docs.readthedocs.io/en/latest/security_center/index.html

- Found a security vulnerability in Trusted Firmware?

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

- Coordinated disclosure with Trusted Stakeholders and ESS
  - https://trusted-firmware-docs.readthedocs.io/en/latest/security_center/incident_handling_process.html#trusted-stakeholder-registration
- Per-project security email aliases
  - https://trusted-firmware-docs.readthedocs.io/en/latest/security_center/mailing_aliases.html

TrustedFirmware .org

Membership Structure & Benefits

***: 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
Platforms 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

Current members

TrustedFirmware
.org

Diamond Members

arm

Google

Platinum Members

Linaro

NXP

RENESAS

ST
life.augmented

General Members

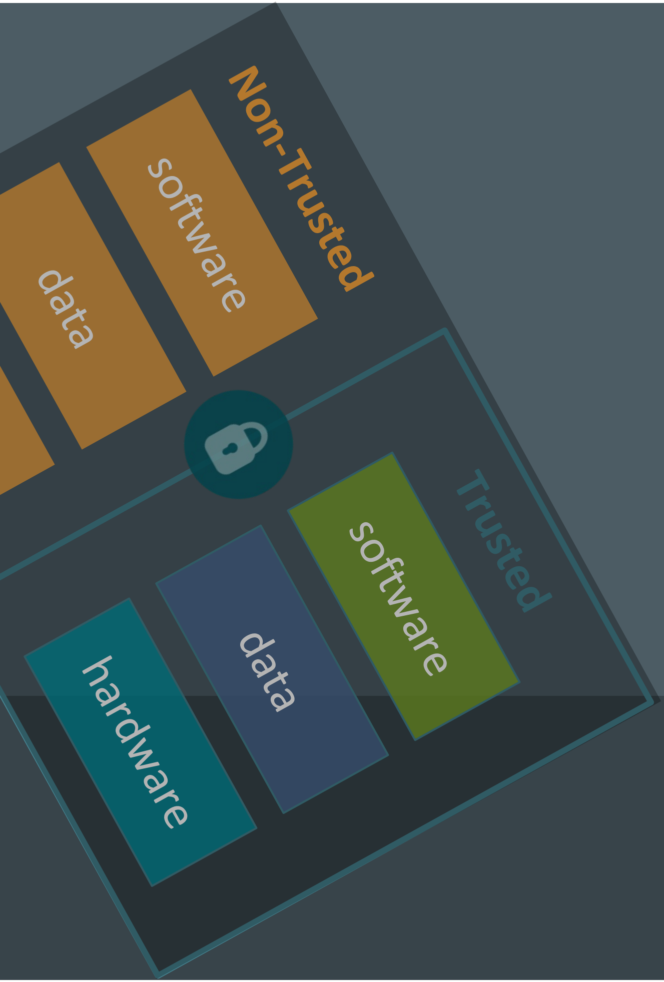
FUTUREWEI
Technologies

NORDIC
SEMICONDUCTOR

PROVENRUN

Partners

bugseng



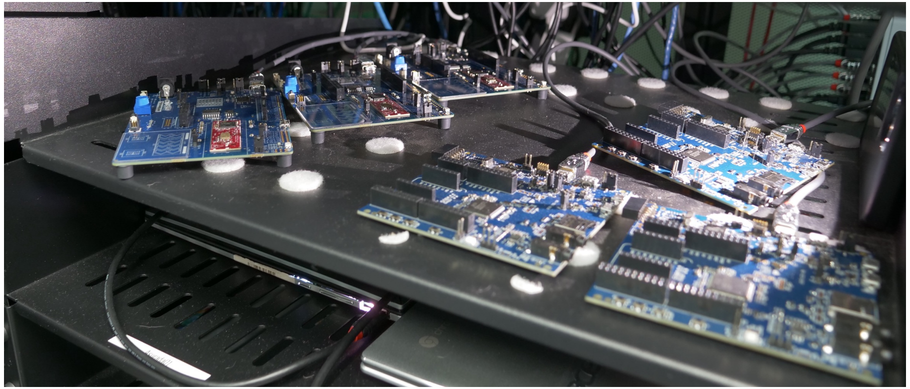
Open CI Summary

Open CI Summary

TrustedFirmware .org

The Trusted Firmware **Open CI** (Continuous Integration) is a cloud-based CI infrastructure that leverages multiple components including Git, Gerrit, Jenkins, TuxSuite, and LAVA to create a comprehensive end-to-end development, integration, test, and release infrastructure.

- Validates TrustedFirmware.org builds on Member hardware located in a centralized hardware lab
- Integrated ECLAIR MISRA test suites / Static Analysis tooling assuring high-quality codebases and providing formal compliance jumpstarts
- Currently leveraged by TF-M, TF-A, Mbed TLS and Hafnium, with additional TrustedFirmware supported projects planned



Open CI Additional Features

TrustedFirmware .org

Additional features of Open CI:

- Integrates different System Specifications, interfaces, architectures
- Supports a Trusted Boot Chain composed of a multi-stage boot process
- Supports TrustZone and the isolation of critical security functions such as secure boot code and cryptographic operations
- Provides facilities for Secure Debugging
- Facilitates the foundation for Security Certifications as required in the marketplace
- Support for multiple Arm Architectures and multiple toolchains

All the above, while providing an efficient software development and validation environment that supports a community centric software development environment

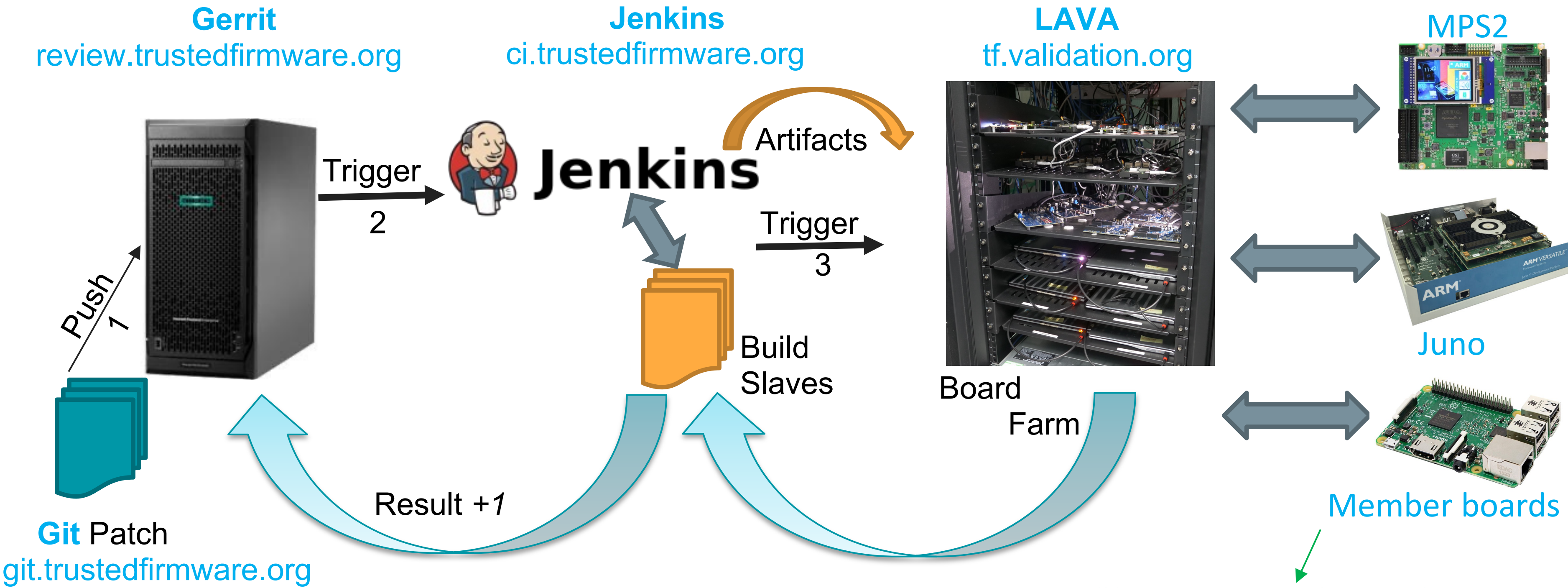
Open CI Additional Features cont'd

Additional features of Open CI:

- Hardware validation lab additional details:
  - Leverages LAVA for validation of software updates on member hardware
    - Code update regression testing /validation prior to final review and merge
  - Validates code updates on multiple toolchains and hundreds of unique configurations
  - Arm Fixed Virtual Platform (FVP) software emulators leveraged for enhanced validation and test configurations
  - Includes Mbed TLS unit tests validated on multiple OS's

All the above, while providing an efficient software development and validation environment utilizing a community centric software development environment

Open CI & Board Farm



Gerrit
review.trustedfirmware.org

Jenkins
ci.trustedfirmware.org

LAVA
tf.validation.org

MPS2

Juno

Member boards

Git Patch
git.trustedfirmware.org

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

Adopt Trusted Firmware to build your next secure platform

FY23 results

250+ Unique Contributors

Trusted Firmware Projects 8

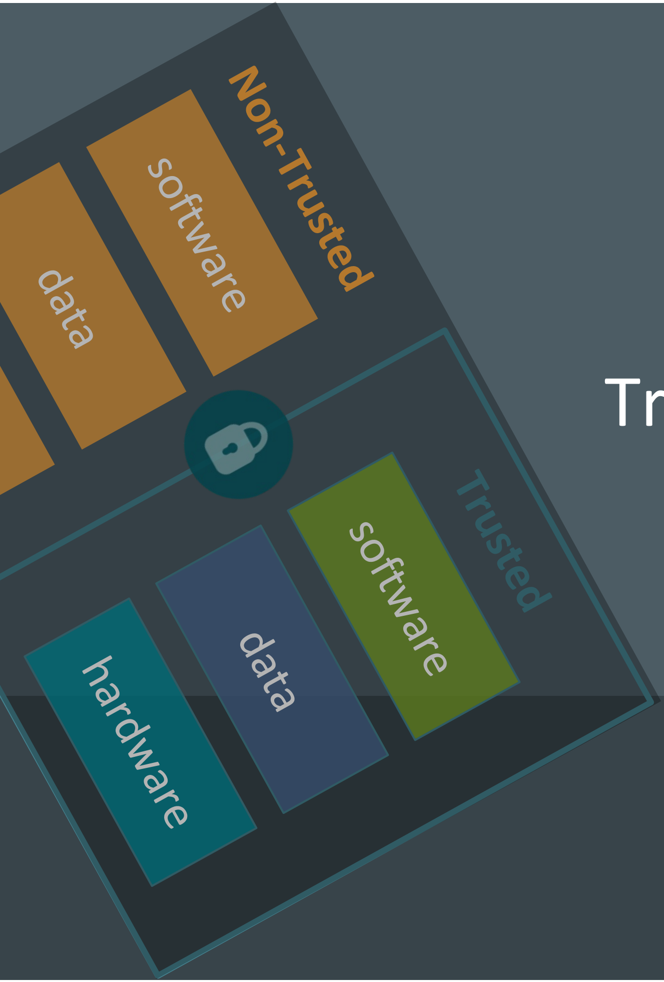
12 Number of Member Platforms in Open CI

LOC Deltas +300K+ -100K+

40+ Companies contributing

15+ Number of Major Releases

Open CI Tests per Year 5M+



TrustedFirmware.org Projects Summaries

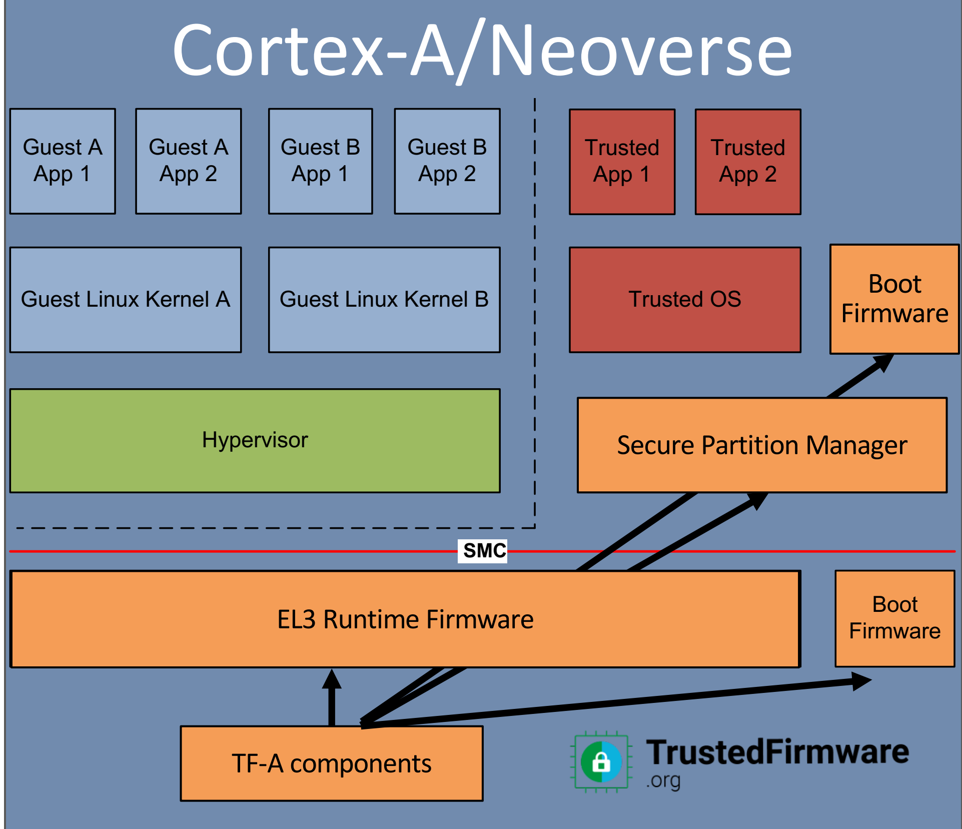
Trusted Firmware-A

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:

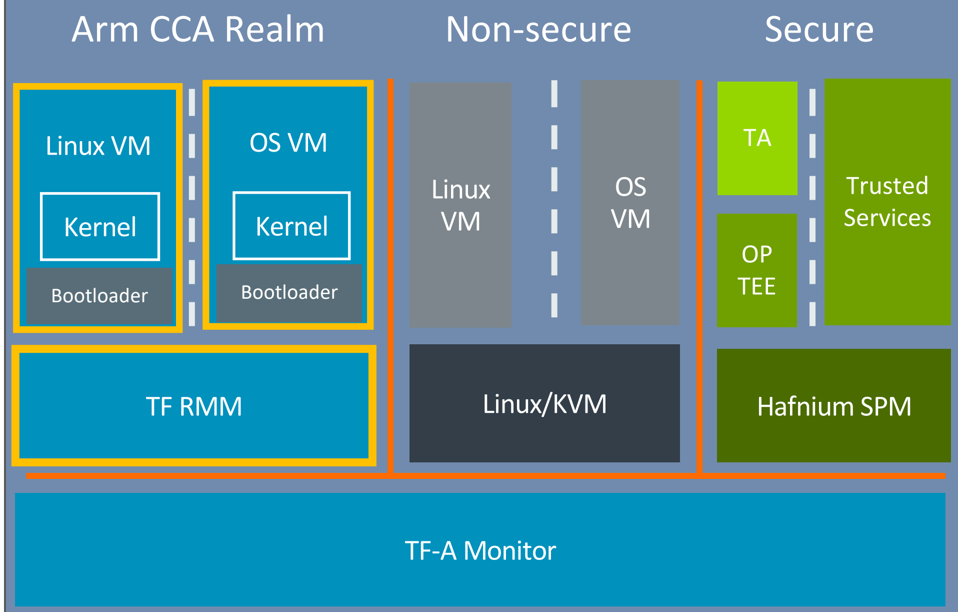
- SMC CC (Secure Monitor Call Calling Convention)
- TBBR (Trusted Board Boot Requirements)
- PSCI (Power State Coordination Interface)
- SCMI (System Control & Management Interface)
- FF-A (Firmware Framework for A-Profile)



TF-RMM (Arm CCA)

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

- Enhanced security isolation
- Flexible workload isolation
- Reduced attack surface



TF-A-Tests

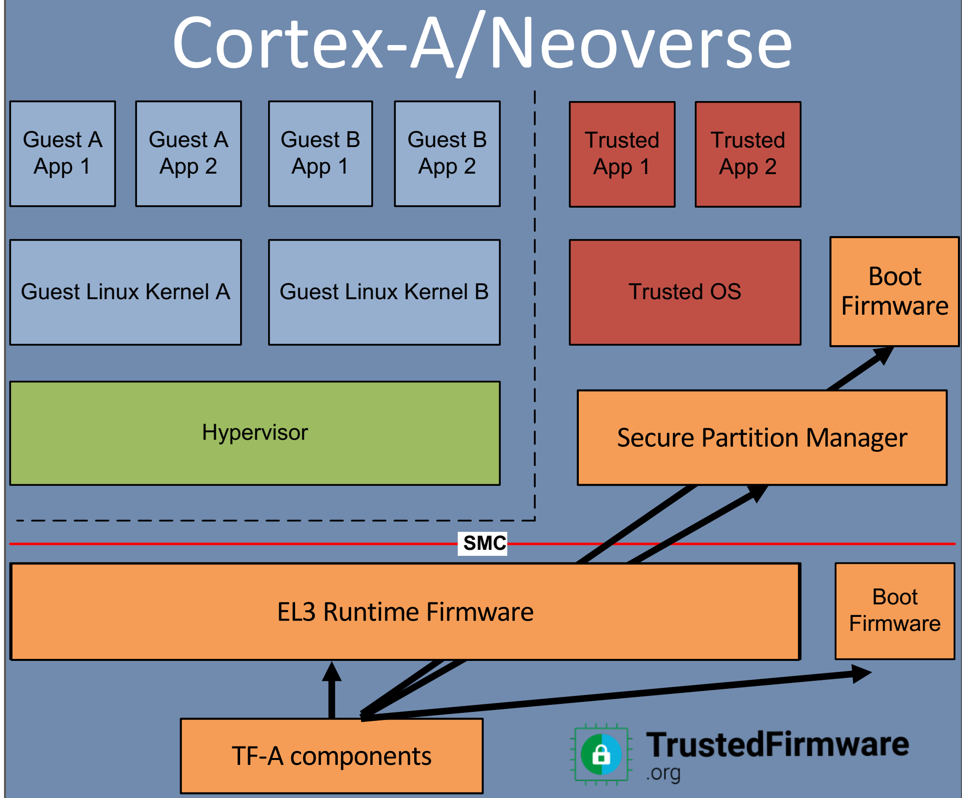
https://trustedfirmware-a-tests.readthedocs.io/en/latest/

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

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 more!



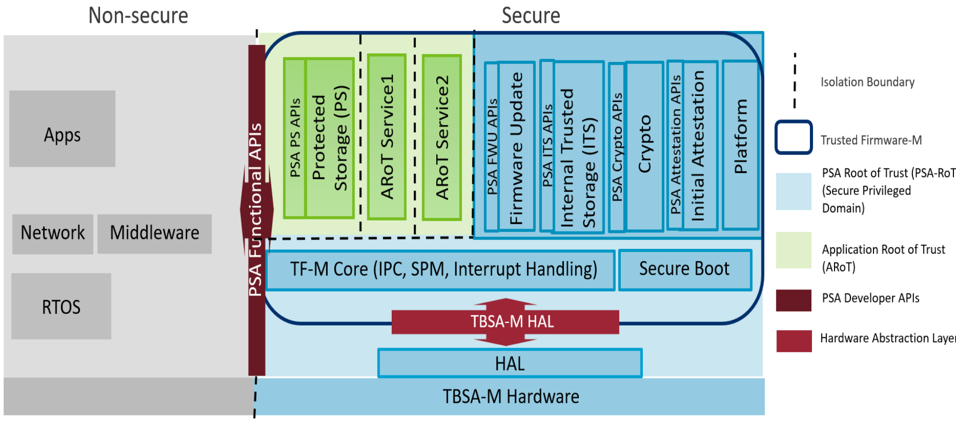
TrustedFirmware .org

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.

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

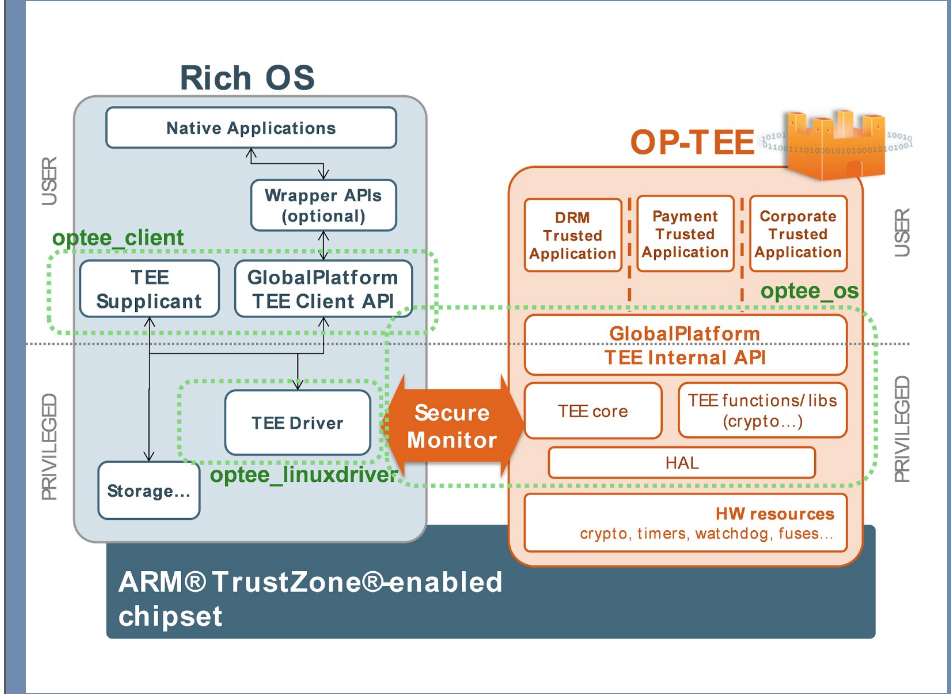


TrustedFirmware
.org

OP-TEE

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

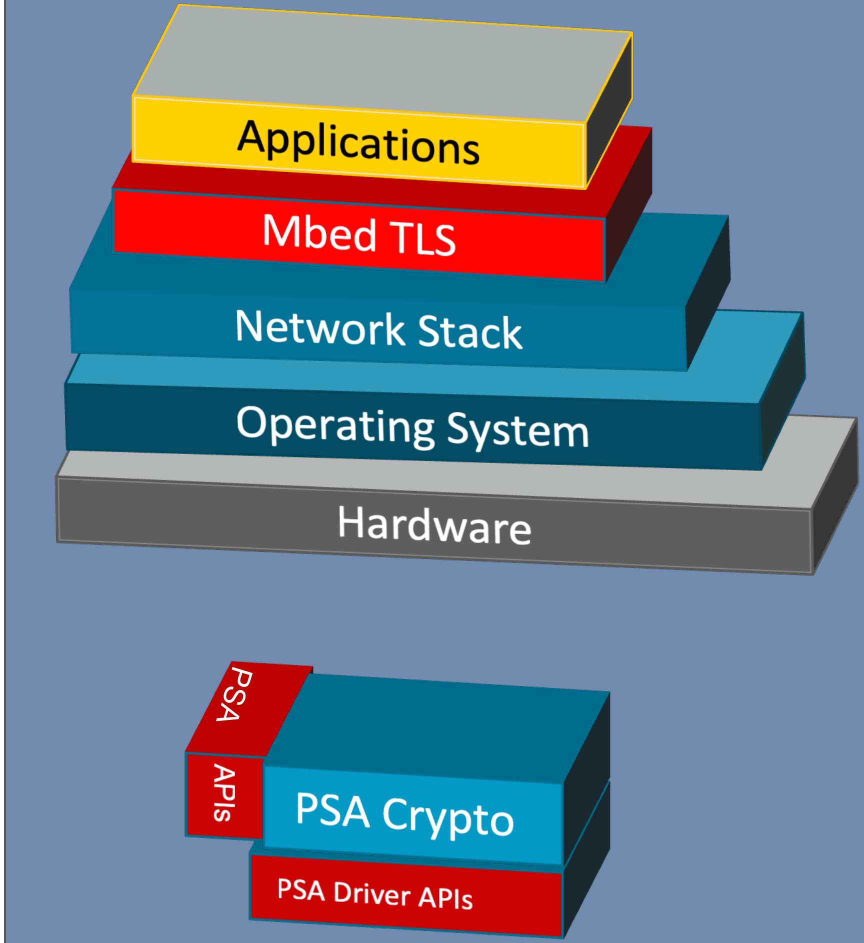
Implements TEE Internal Core API and TEE Client API as defined in the GlobalPlatform API specifications.



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)

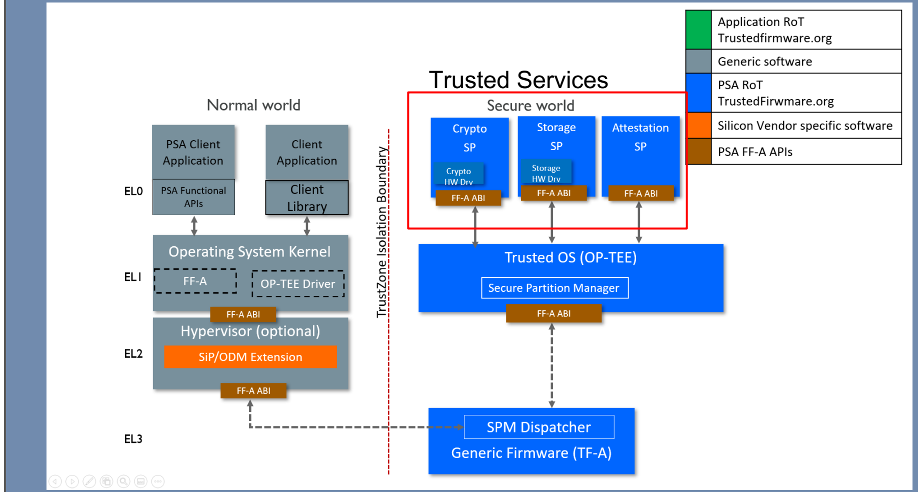
- PSA Crypto (Mbed Crypto), derived from Mbed TLS library, brings together Crypto primitives and makes them available via PSA Crypto APIs
- PSA Crypto also support driver interfaces to integrate with Secure Elements and Crypto Accelerators



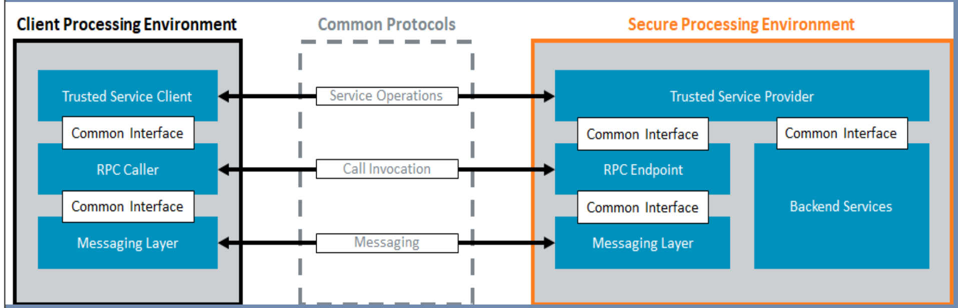
TrustedFirmware.org

Trusted Services

- Framework to develop Security related Services for enhanced device security and a standardize security approach across platforms
- Deployable over a 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 standardized service layer
- Includes Platform Security Architecture (PSA) Trusted Services for Cryptography, Storage and Attestation and other Secure Services



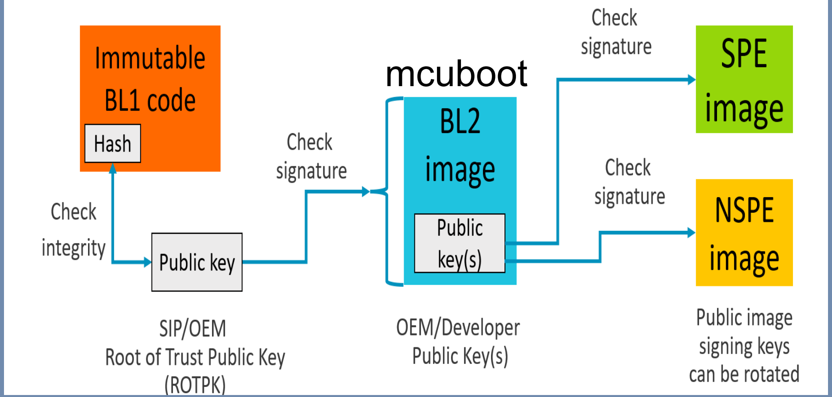
Layered Model Of Trusted Services



TrustedFirmware.org

MCUBoot

- Secure bootloader for 32 bit microcontrollers
- 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

Thank you

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