Trusted Firmware Community Project

TrustedFirmware.org

Trusted Firmware

Open Governance Community Project

Evolution of former Open Source **Arm Trusted Firmware** project

Reference implementation of Secure world software for Armv7 & Armv8 architectures (both A/M-Profiles)

Membership open to all

Governance overseen by a board of member representatives

Technical direction overseen by TSC

~~Arm Trusted Firmware~~

Trusted Firmware
Open Governance
Community Project

TrustedFirmware.org

Not new! Arm Trusted Firmware since 2013!

Feb 13	Conception	Arm has idea of providing reference EL3 firmware for Armv8-A to help defragment the Arm software ecosystem
Sep 13	Implementation	v0.1 binaries in Linaro AArch64 release
Oct 13	Introduction	v0.2 source code at GitHub and LCU13 announcement
Jun 14	Adoption	Early adopters port v0.4 to silicon
Aug 14	Celebration	v1.0 released, including Juno port OP-TEE support at LCU14
Feb 15	Evolution	v1.1 completes mandatory PSCI v1.0 Trusted Board Boot prototype
Dec 15	Acceleration	v1.2 provides minimally complete TBB Upstreaming of Non-Arm platforms
Oct 16	Extension	v1.3 adds AArch32 PSCI Dropped CLA, security hardening
Jun 17	Optimisation	v1.4 adds DynamIQ, GIC-600, SCMI, PSCI with OP-TEE, HiKey/HiKey960
Mar 18	Expansion	v1.5 introduces RAS & Secure Partitions, Dynamic Configuration, Armv7 support
Oct 18	Open Governance	v1.6/v2.0 – TF.org migration with TF-M

Current members

arm

Linaro

Google

Data I/O

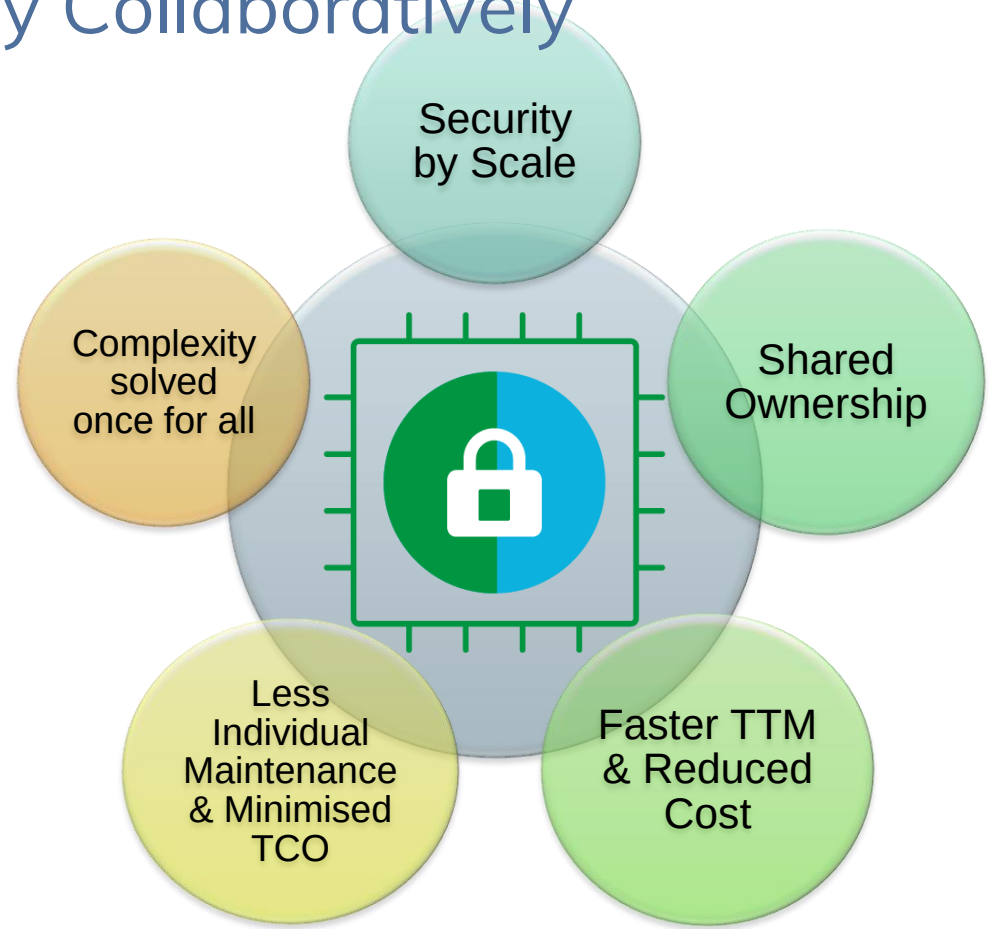
Texas Instruments

CYPRESS
EMBEDDED IN TOMORROW™

life.augmented

TrustedFirmware.org

Build Security Collaboratively



TrustedFirmware.org

All market segments

Devices

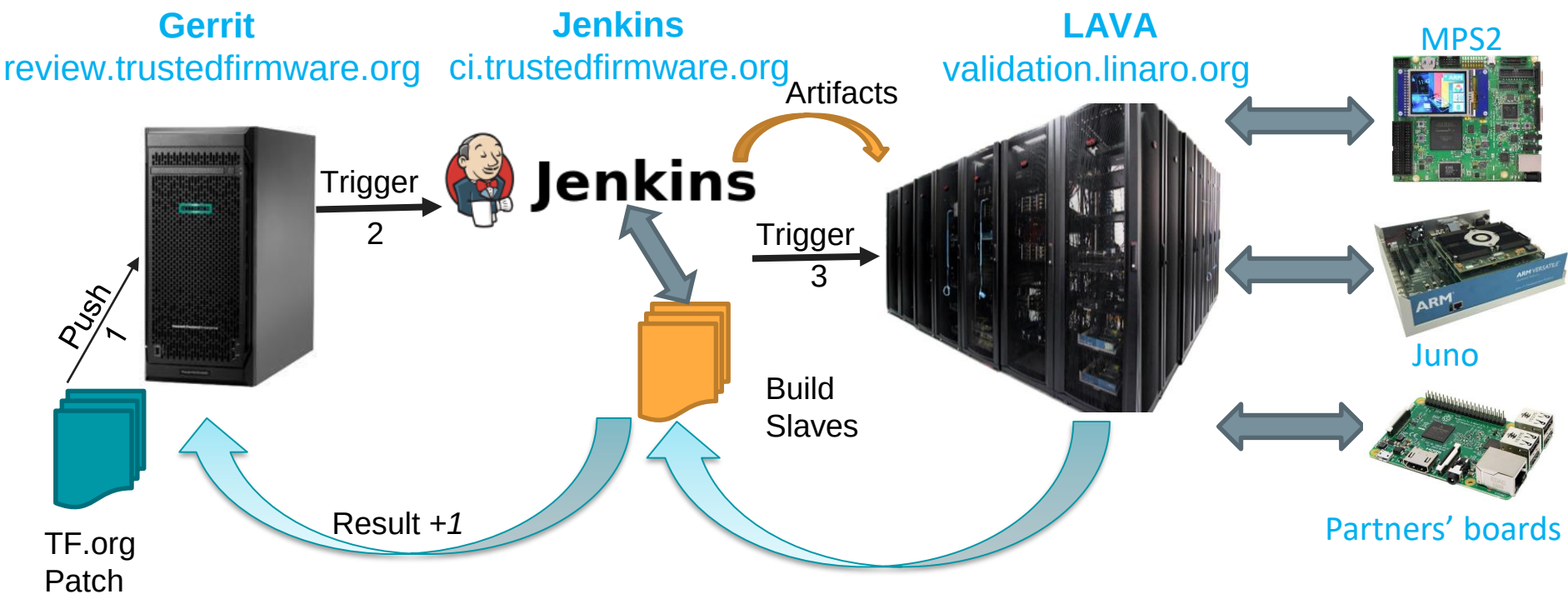
IoT/Mobile/Auto/Laptop

Embedded Edge

Cloud Server

TrustedFirmware.org

Open CI & Board Farm



TrustedFirmware.org

Details & Resources

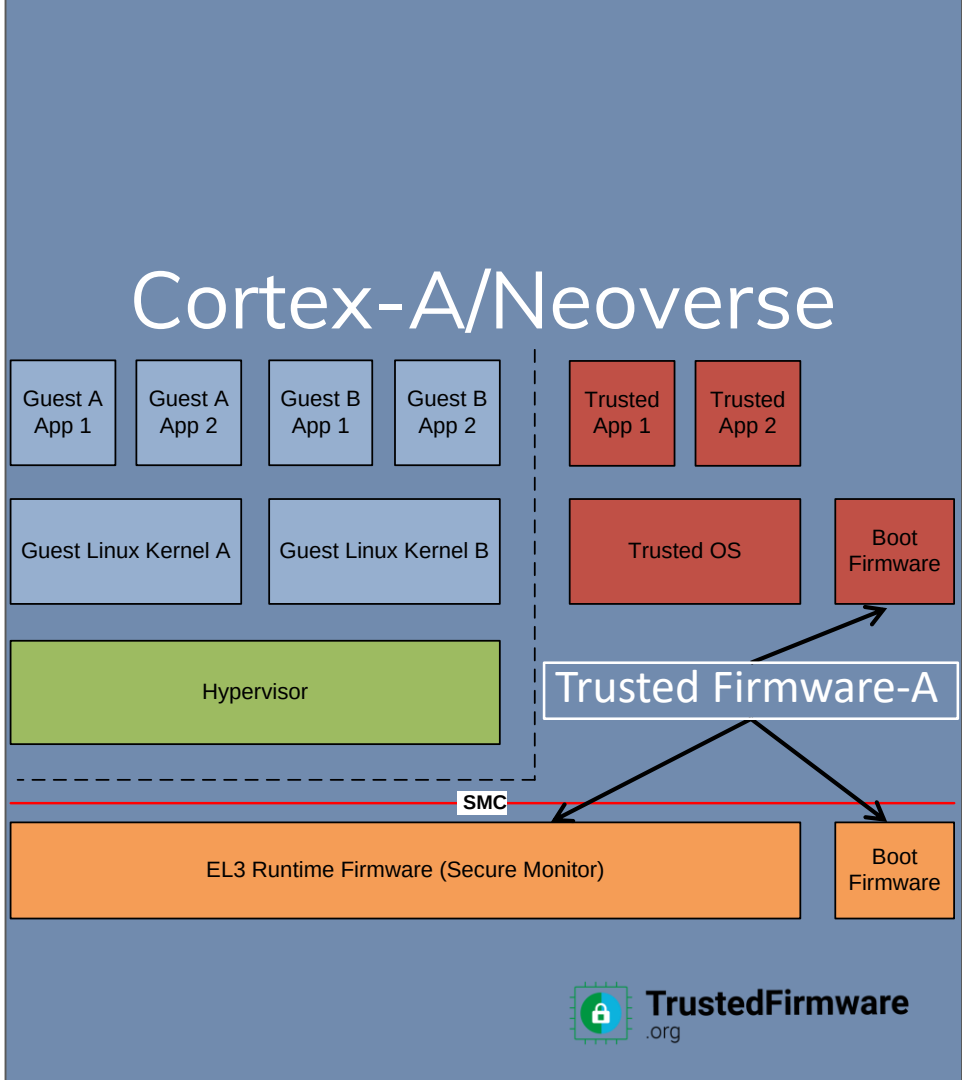
- Open Source permissive **BSD 3-clause license**
- All contributions accepted under the terms of **DCO**
- Project mailing lists for technical discussions
- Git & Gerrit for open reviews
- Monthly project status updates
- Board meeting minutes
- Project Charter

Trusted Firmware-A

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:

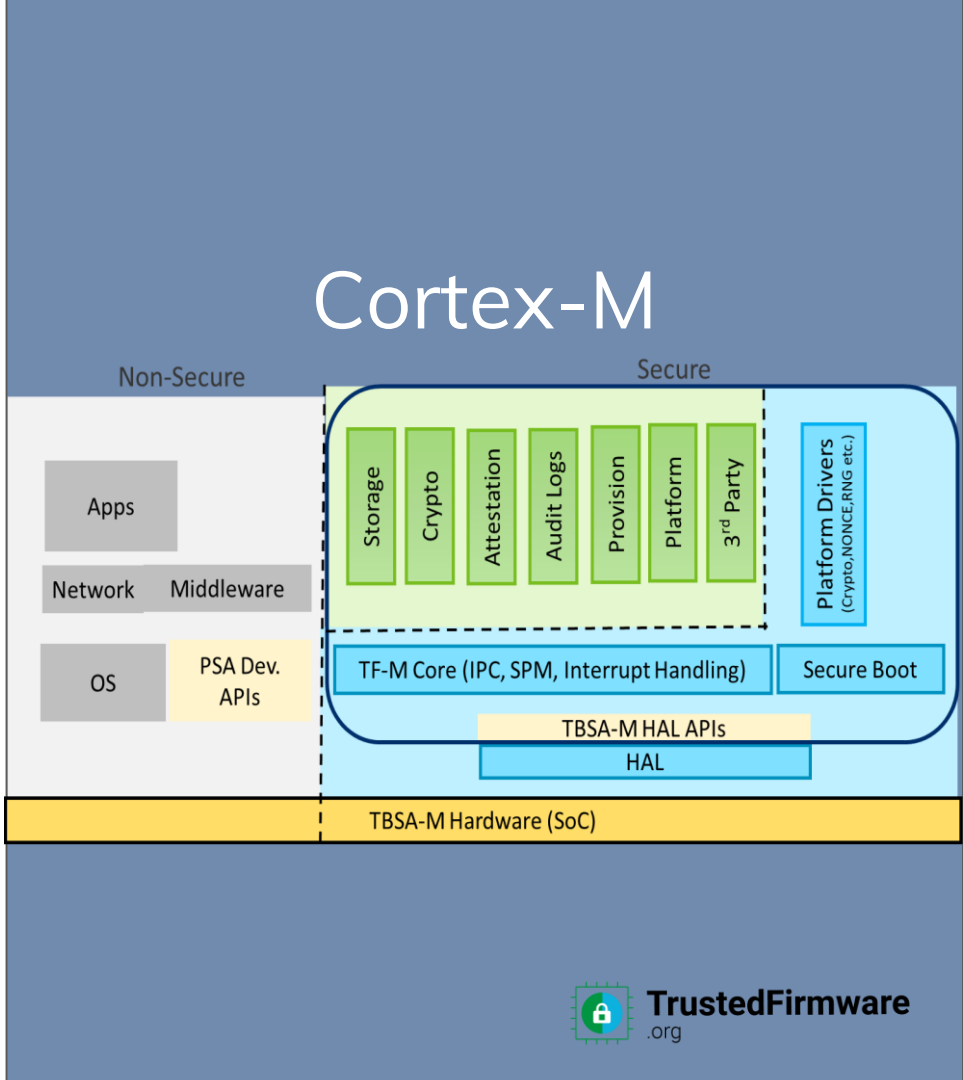
- SMCCC (SMC Calling Convention)
- TBBR (Trusted Board Boot Requirements)
- PSCI (Power State Coordination Interface)
- SCMI (System Control & Management Interface)
- SPCI (Secure Partitions Client Interface)



Trusted Firmware-M

Reference implementation of Arm Platform Security Architecture (PSA) It provides Trusted Execution Environment for Arm Cortex-M processors.

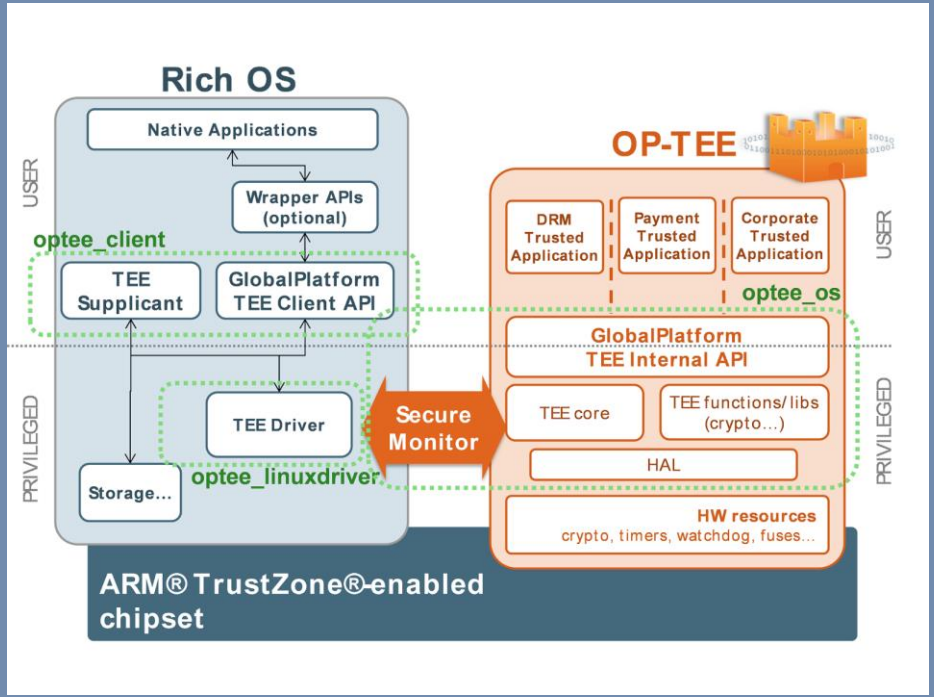
It consists of Secure Boot and a set of Secure Services such as Secure Storage, Crypto etc. for Applications accessible via PSA Developer APIs.



OP-TEE (Ongoing migration into TF.org)

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

How to Get Involved

Become a project member

Platinum Board members define the mission and strategy: $50K/year

General members receive project updates, make requests to the board and have joint representation at Board meetings: $2.5-25K*/year

* Fee according to company size and type

Contact:

enquiries@TrustedFirmware.org

for more information

TrustedFirmware.org

Thank you

Adopt Trusted Firmware to build your next secure platform

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