Trusted Firmware Community Project

TrustedFirmware.org

Trusted Firmware: Build Security Collaboratively

Open Governance Community Project

Reference open source implementation of Secure world software for Arm processors across all market segments

Membership open to all

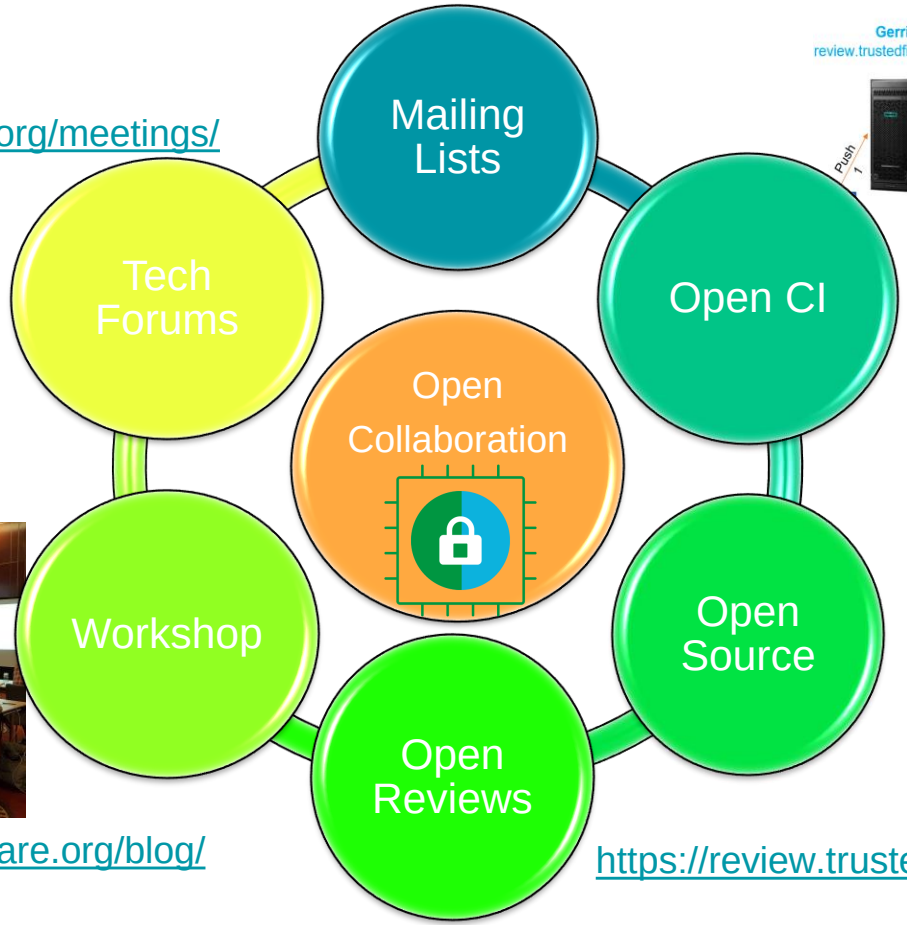
Board

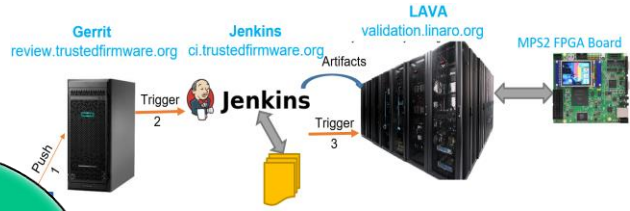
Technical Steering Committee

The Virtuous Circle Of Collaboration!

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

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



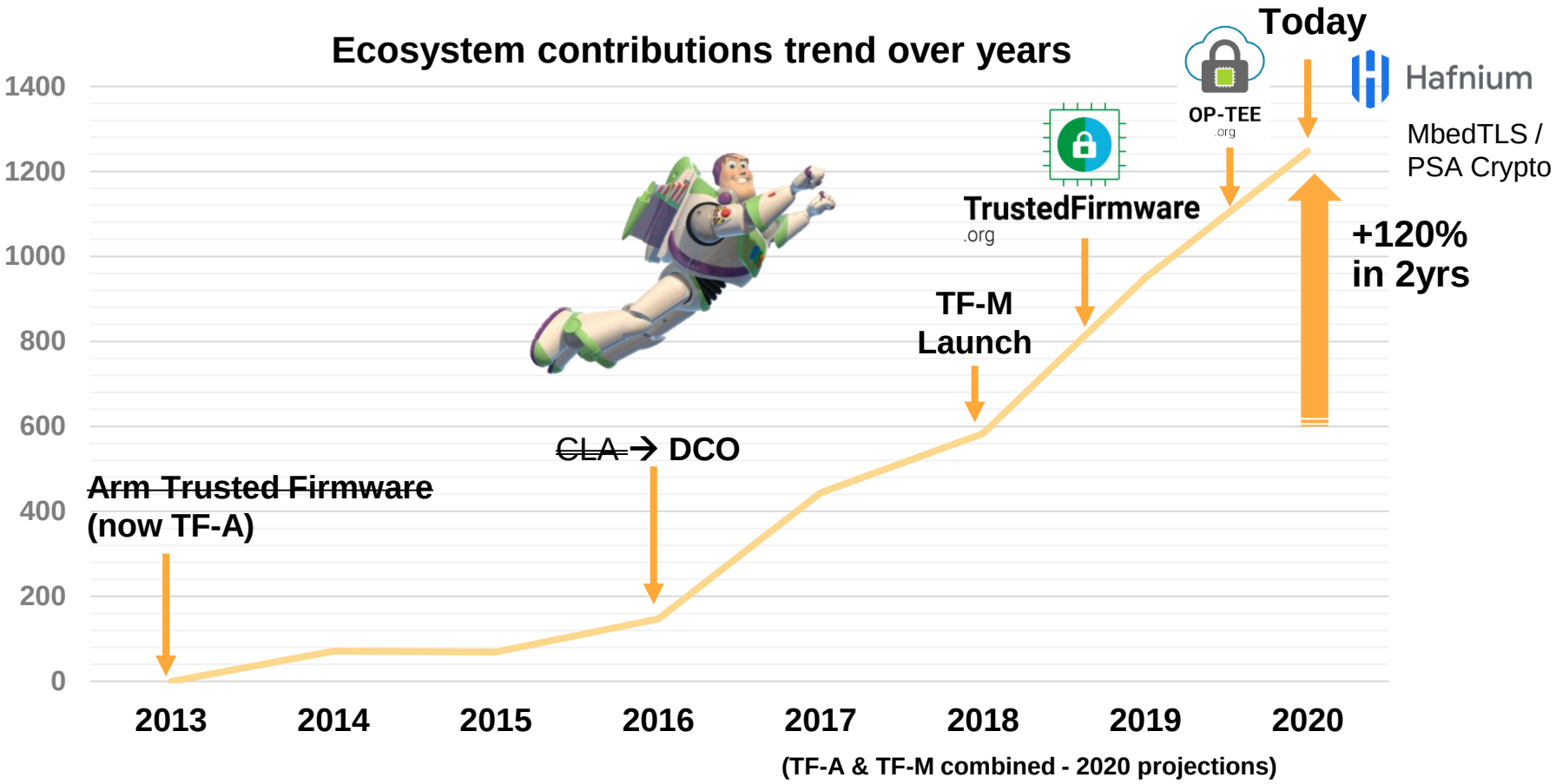


https://ci.trustedfirmware.org/

https://git.trustedfirmware.org/

https://review.trustedfirmware.org/

A success story: from 0% to infinity...and beyond!



Current members

arm

FUTUREWEI Technologies

CYPRESS EMBEDDED IN TOMORROW™

RENESAS

OPEN MOBILE PLATFORM

Linaro

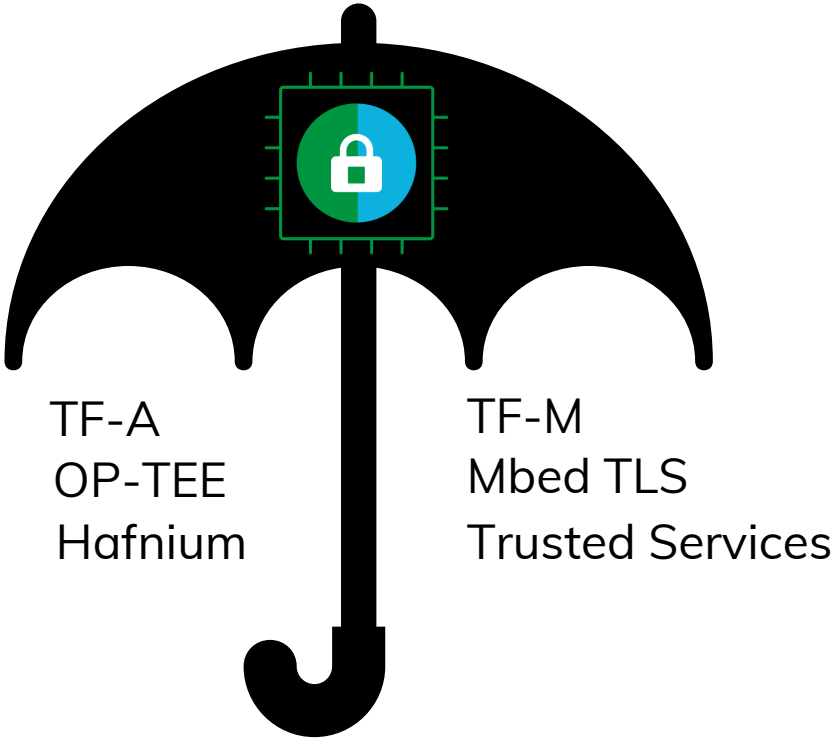
Google

life.augmented

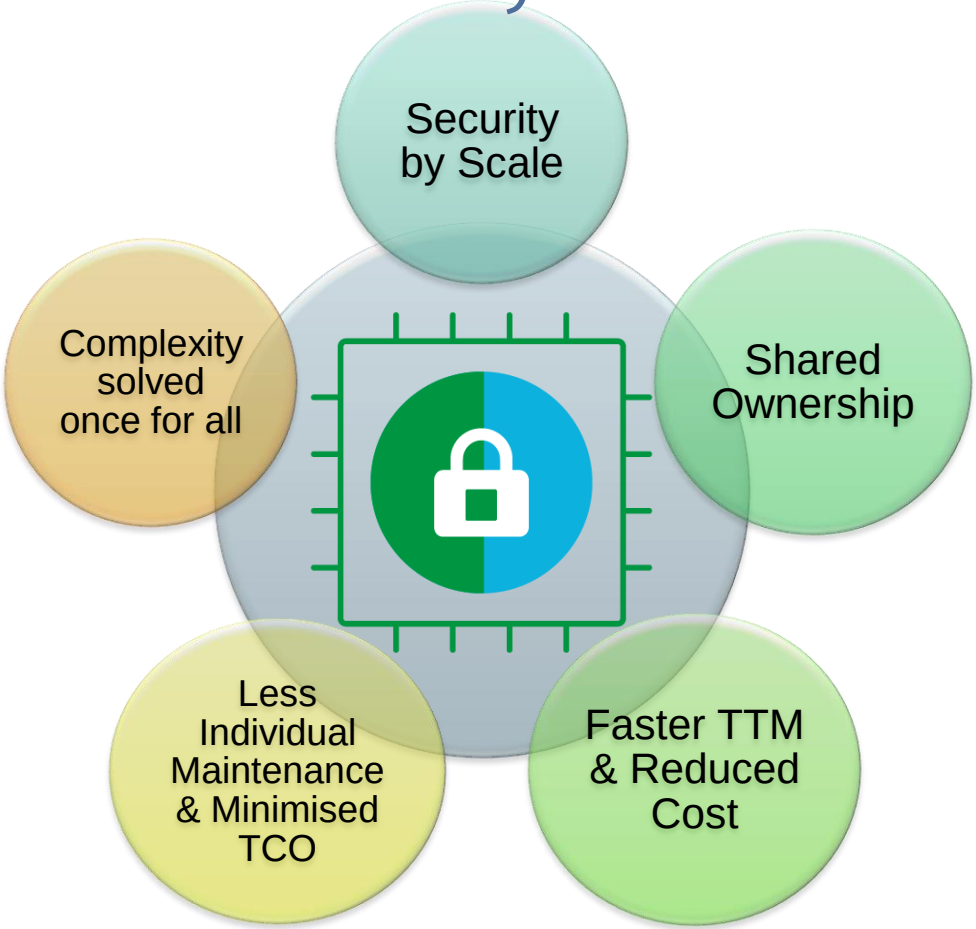
NXP

NXM

Current Projects



Build Security Collaboratively



TrustedFirmware.org

All market segments

Devices

IoT/Mobile/Auto/Laptop

Embedded

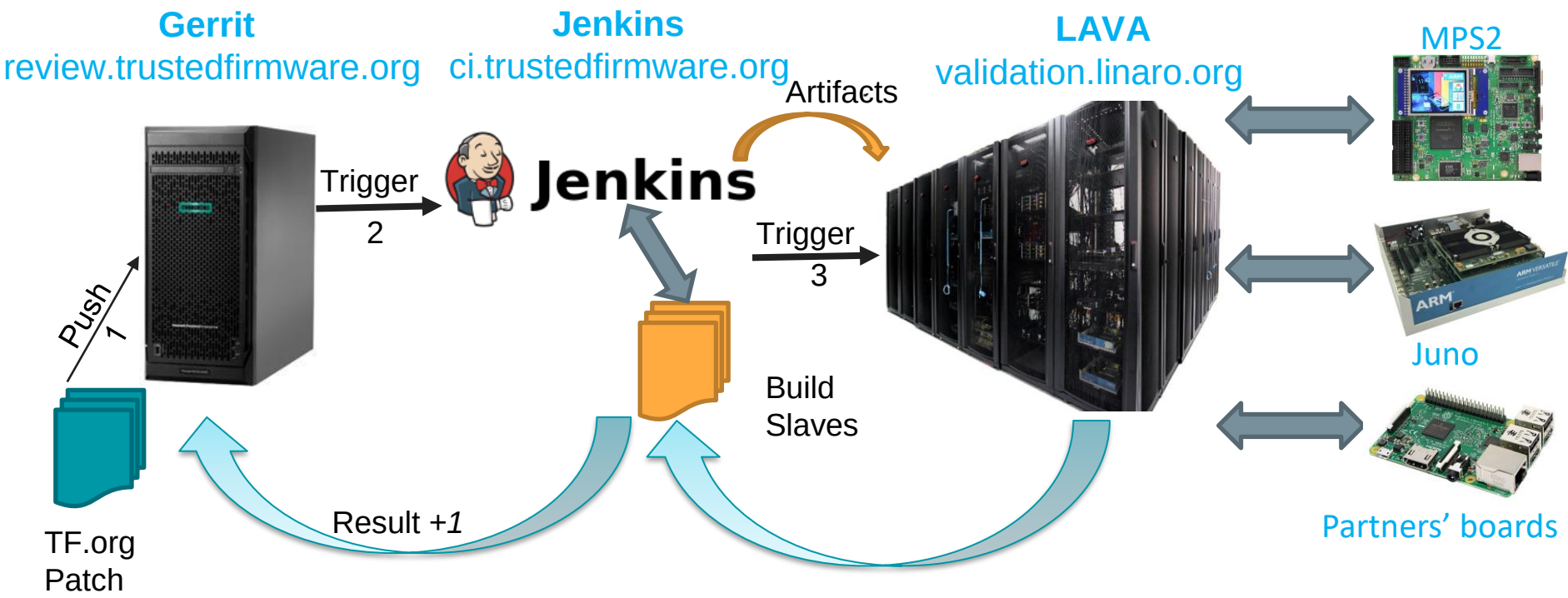
Edge

Cloud

Server

TrustedFirmware.org

Open CI & Board Farm



TrustedFirmware.org

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/

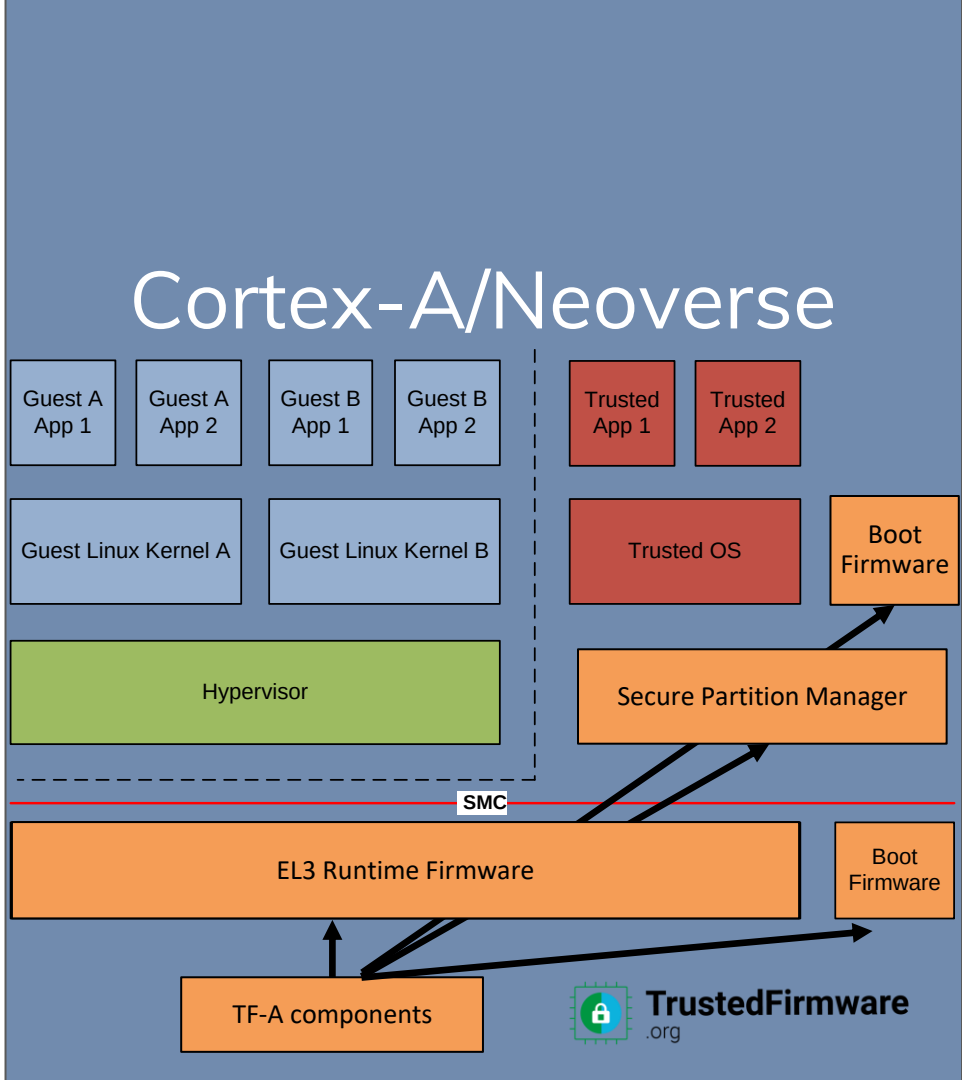
- Per-project security email aliases
  - https://developer.trustedfirmware.org/w/collaboration/security_center/mailing_aliases/

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)
- FF-A (Firmware Framework for A-Profile)

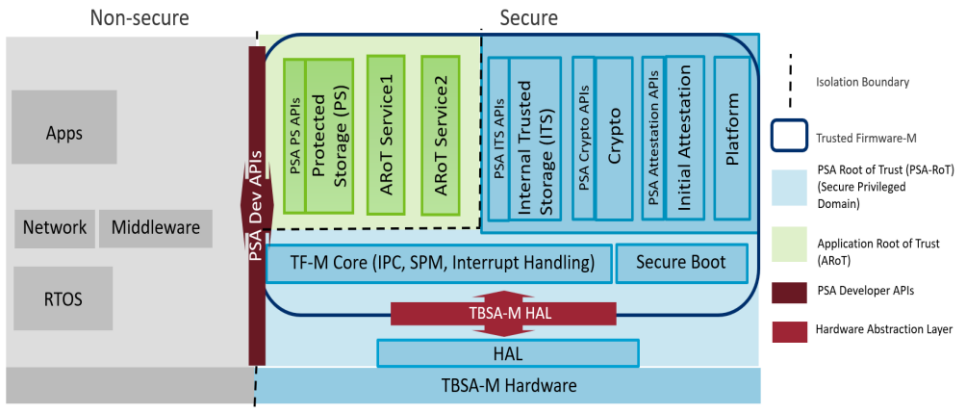


Trusted Firmware-M

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 etc. for Applications accessible via PSA Functional APIs.

Cortex-M

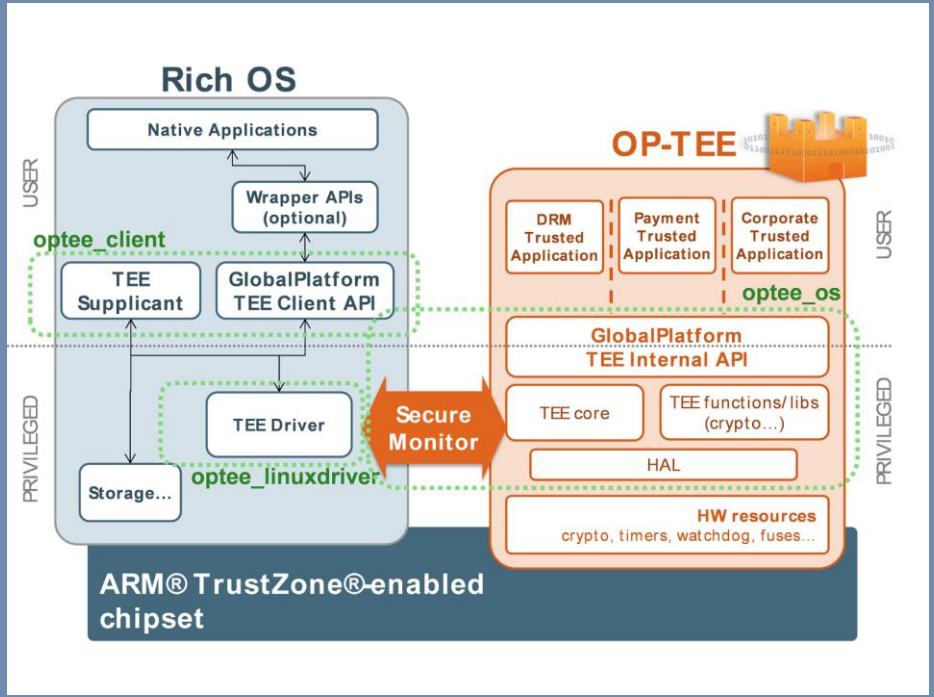


TrustedFirmware.org

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.

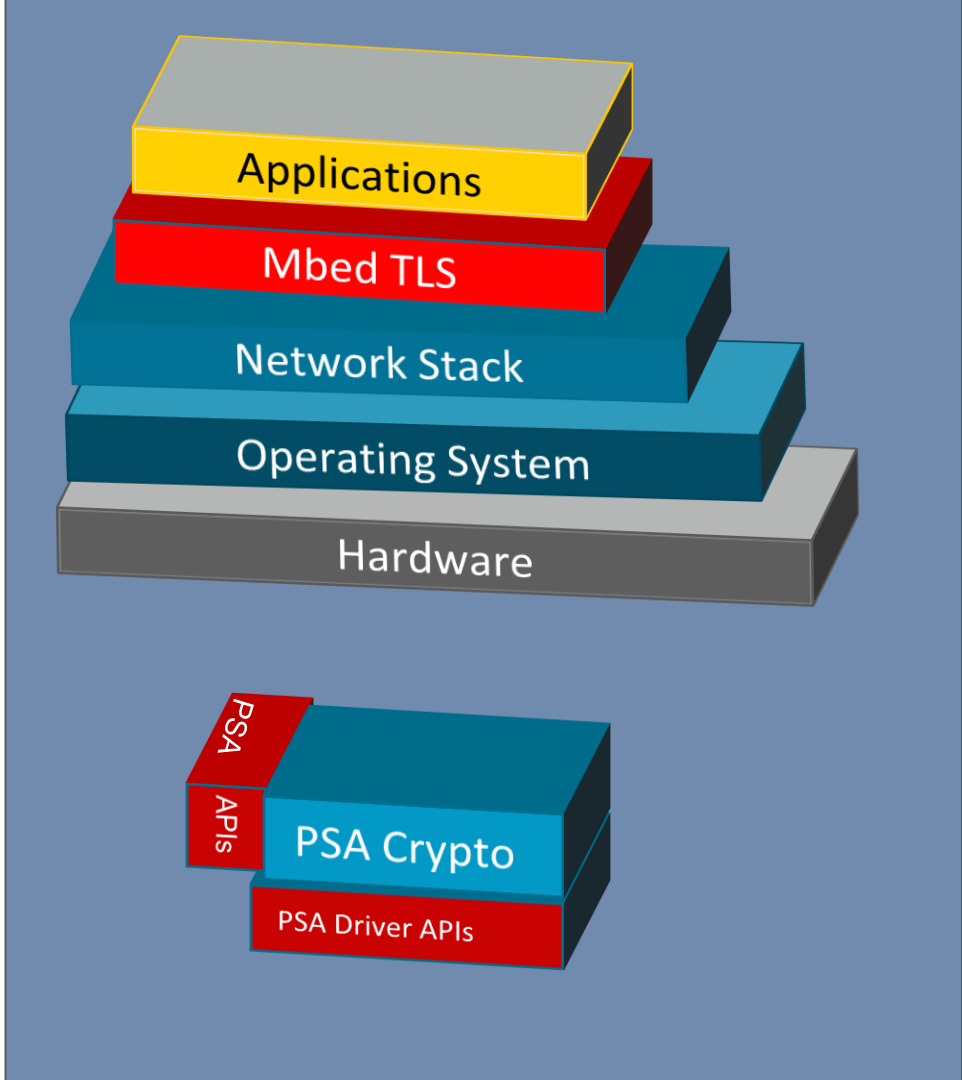
Implements TEE Internal Core API v1.1.x and the TEE Client APIv1.0, as defined in the GlobalPlatform API specifications.



TrustedFirmware.org

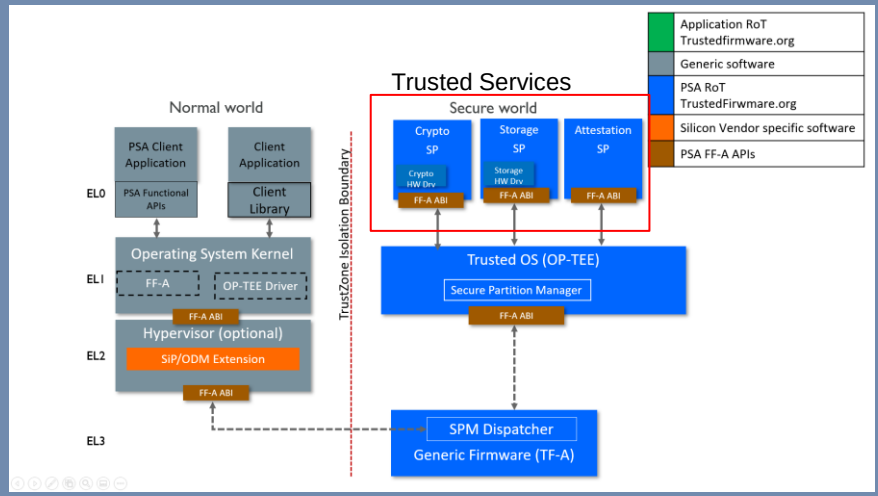
Mbed TLS

- 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.

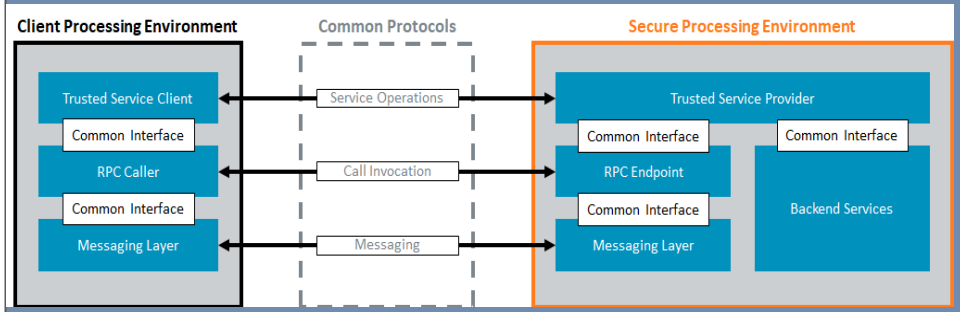


Trusted Services

- 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



Layered Model Of Trusted Services



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

Read the project Charter

* 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