Trusted Firmware Community Project
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
Trusted Firmware Community Project

- Open Source
- Open Collaborative Platform
- Open CI
- Open Governance
Trusted Firmware History

Oct 2013
Arm Trusted Firmware

Mar 2018
Trusted Firmware-M

Oct 2018
TrustedFirmware.org

Sept 2019
OP-TEE joins TrustedFirmware

A long time ago in a Connect for: far away...

Trusted Firmware M-Class (TF-M) is new!
TF-M provides a good starting point for secure software implementations, now, but there is lots more to do...

A time ago in the world of Open Source Secure World Software...

Platform Security Assured

OP-TEE joins TrustedFirmware.org

OP-TEE joins TrustedFirmware.org

Trusted Firmware-A
Current members
Build Security Collaboratively

- Security by Scale
- Complexity solved once for all
- Shared Ownership
- Faster TTM & Reduced Cost
- Less Individual Maintenance & Minimised TCO

TrustedFirmware.org
All market segments

Devices
IoT/Mobile/Auto/Laptop
Embedded Edge
Cloud Server
Open CI & Board Farm

Gerrit
review.trustedfirmware.org

Jenkins
ci.trustedfirmware.org

LAVA
validation.linaro.org

MPS2

Juno

Partners’ boards

Push 1

TF.org Patch

Result +1

Trigger 2

Artifacts

Trigger 3

Build Slaves
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

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 & PSA Crypto

- 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 library will also support driver APIs to integrate with Secure Elements and Crypto Accelerators.
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
Adopt Trusted Firmware to build your next secure platform

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

Thank you