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
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
Trusted Firmware-A

Oct 2018
TrustedFirmware.org

Sept 2019
OP-TEE joins TrustedFirmware.org
Welcome OP-TEE into TrustedFirmware.org!

Comprehensive reference implementation of Secure world software and Secure services for all Arm-based systems

Easily portable to many other trusted software implementations

Current members

arm

Linaro

Google

Data I/O

FUTUREWEI Technologies

CYPRESS Embedded in Tomorrow

TrustedFirmware.org
Build Security Collaboratively

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

Build Security Collaboratively
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

Push
1

TF.org Patch

Trigger
2

Jenkins

Build Slaves

Result +1

Trigger
3

MPS2

Juno

Partners’ boards
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.
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](http://www.TrustedFirmware.org) or email [enquiries@trustedfirmware.org](mailto:enquiries@trustedfirmware.org) for more information

Thank you