Trusted Firmware Community Project
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://ci.trustedfirmware.org/

https://git.trustedfirmware.org/

https://review.trustedfirmware.org/

https://www.trustedfirmware.org/blog/
A success story: from 0% to infinity...and beyond!

Ecosystem contributions trend over years

Arm Trusted Firmware (now TF-A)

TF-M Launch

+120% in 2yrs

Hafnium

MbedTLS / PSA Crypto

TF-A & TF-M combined - 2020 projections
Current members

arm
FUTUREWEI Technologies
CYPRESS EMBEDDED IN TOMORROW
RENESAS
OPEN MOBILE PLATFORM
Linaro
Google
ST life.augmentec
NXP
NXM
Current Projects

TF-A
OP-TEE
Hafnium

TF-M
Mbed TLS
Trusted Services
Build Security Collaboratively

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

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

TF.org
Patch

Push 1

Jenkins

Trigger 2

Artifacts

Trigger 3

Build Slaves

Result +1
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.
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](https://www.globalplatform.org/api/teeci/) v1.1.x and the [TEE Client API](https://www.globalplatform.org/api/teelci/) v1.0, as defined in the [GlobalPlatform API](https://www.globalplatform.org) 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.
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
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