Trusted Firmware Community Project
TrustedFirmware.org

Collaborative Security

Reference
Secure
Software

Governing bodies:
Board & TSC

Open Governance Community Project

Complexity solved once for all

Shared Ownership

Security at Scale
Current members

Diamond Members

arm  Google

Platinum Members

Linaro  NXP  Renesas  ST

General Members

Futurewei  NXM  Nordic

Partners

bugSeng

TrustedFirmware
Member Benefits: Highlights

- Governing Board seat driving strategic direction and investments
  (Budget, Marketing Initiatives, explore new investment areas)

- Part of Technical Steering Committee driving technical direction of project
  (Define Release process, Security Incident Handling process, Roadmaps reviews & influence)

- Add and maintain platforms in Open CI *(Refer to the “Open CI & Board Farm” slide)*

- Opportunity for close engineering collaboration with other members

- Refer “Membership Structure” slide for details on membership tiers and benefits
The Virtuous Circle Of Collaboration!

Tech Forums

Mailing Lists

Open Collaboration

Open CI

Open Source

Open Reviews

Workshop

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

https://ci.trustedfirmware.org/

https://git.trustedfirmware.org/

https://review.trustedfirmware.org/

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

- TF-A
- OP-TEE
- Hafnium
- TF-RMM

- TF-M
- Mbed TLS
- Trusted Services
- mcuboot
Build Security Collaboratively

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

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

Gerrit
review.trustedfirmware.org

Jenkins
ci.trustedfirmware.org

Artifacts

TF.org
Patch

Result +1

Build Slaves

Trigger 2

Trigger 3

LAVA
validation.linaro.org

TPM2

Member boards

https://tf.validation.linaro.org/scheduler/device_types
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/
TF-A very first LTS release!

- A TF.org community effort to create and maintain the first TF-A LTS release!
  - LTS v2.8.0 launched in February (based on TF-Av2.8 release)
  - Already 6 maintenance releases produced with urgent bugfix (latest LTS v2.8.6)
  - Dedicated mailing list tfa-lts@lists.trustedfirmware.org

- Commitment to keep it supported for 5 years
  - First year effort sustained by community members from interested companies
  - Seeking for wider engagement and contributions to achieve the LTS requirements

- Ideally a new LTS release will be created again next year, aligned with autumn TF-A release (subject to community interest and engagement)

- Full LTS requirements and proposal can be found here
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)
TF-RMM (Arm CCA)

- Reference implementation of the Arm Realm Management Monitor (RMM) specification for the Arm Confidential Compute Architecture (Arm CCA)
**TF-A-Tests**


A suite of bare-metal functional tests to exercise TF-A features from the Normal World, without dependencies on a Rich OS. It provides a strong basis for TF-A developers to validate their own platform ports and add their own test cases, interacting with TF-A through its SMC interface.

Features currently tested include:

- SMC Calling Convention
- Power State Coordination Interface (PSCI)
- Software Delegated Exception Interface (SDEI)
- Performance Measurement Framework (PMF)
- Trusted Board Boot Requirements (TBBR)
- Secure Partition Manager (SPM) … and lots more!
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, Firmware update, 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/) v1.1.x and the [TEE Client API](https://www.globalplatform.org/) 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 and other Secure Services
MCUBoot

- Secure bootloader
- Widely deployed secure boot solution
- Define a common infrastructure for the bootloader, system flash layout on microcontroller systems
- Enables simple software upgrades
- Used as BL2 bootloader in TF-M
- MCUBoot is operating system and hardware independent and provides a hardware abstraction layer.
## Membership Structure

<table>
<thead>
<tr>
<th>Diamond</th>
<th>Platinum</th>
<th>General (Uni/Non-profit)</th>
<th>Individual (invite only)</th>
<th>Non-Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Access, Review Participation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Technical Forums</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Logo and marketing recognition (scaled per tier)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Technical Steering Committee (TSC) seat + vote</td>
<td>Yes (2 votes each)</td>
<td>Yes (1 vote each)</td>
<td>Yes (1 vote every 5)</td>
<td>Yes (1 vote every 5)</td>
</tr>
<tr>
<td>Governing Board seat + vote</td>
<td>Yes (2 votes each)</td>
<td>Yes (1 vote each)</td>
<td>Yes* (1 vote every 5)*</td>
<td>Yes (1 vote every 5)</td>
</tr>
<tr>
<td>Boards in Open CI</td>
<td>2 new / year</td>
<td>1 new / year</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Fees</td>
<td>$100k</td>
<td>$50k</td>
<td>G1: $2.5K G2: $10K G3: $25K</td>
<td>$2.5K</td>
</tr>
</tbody>
</table>

*: Only for G2 & G3 General members
G1: $2.5K (0 to 50 empl. only)
G2: $10k (0-499)
G3: $25k (500+)

Additional benefits will be evaluated and revisited for future investment topics (MISRA, LTSs, …) when it happens
Adopt Trusted Firmware to build your next secure platform

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