Trusted Firmware Community Project
TrustedFirmware .org

Collaborative Security

- Reference Secure Software
- Governing bodies: Board & TSC
- Security at Scale
- Complexity solved once for all
- Shared Ownership

Open Governance Community Project
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!

- Mailing Lists
- Open Collaboration
- Tech Forums
- Open CI
- Workshop
- Open Source
- Open Reviews

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
- Faster TTM & Reduced Cost
- Shared Ownership
- Complexity solved once for all
- 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

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/
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

https://trustedfirmware-a-tests.readthedocs.io/en/latest/

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](#) v1.1.x and the [TEE Client API](#) v1.0, as defined in the [GlobalPlatform API](#) 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.
10yrs of growing collaboration in building security

- Open CI
- LTS
- MISRA

- 150+ platforms
- 5000+ yearly code contributions
- Hundreds of collaborators
## Membership Structure

<table>
<thead>
<tr>
<th></th>
<th>Diamond</th>
<th>Platinum</th>
<th>General</th>
<th>Community (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>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Technical Forums</td>
<td>Yes</td>
<td>Yes</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>
<td>N/A</td>
<td>No</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>
<td>Yes</td>
<td>No</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>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Boards in Open CI</td>
<td>1 (D1) or 2 (D2) new / year</td>
<td>1 new / year</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Fees</td>
<td>D1: $100k</td>
<td>$60k</td>
<td>G1: $3K</td>
<td>$3K</td>
<td>$600</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>D2: $120k</td>
<td></td>
<td>G2: $12K</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>G3: $30K</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*: Only for G2 & G3 General members
G1: $3K (0 to 50 empl. only)
G2: $12k (0-499)
G3: $30k (500+)
Adopt Trusted Firmware to build your next secure platform

Visit [www.TrustedFirmware.org](http://www.TrustedFirmware.org) or email enquiries@trustedfirmware.org for more information

Thank you