Trusted Firmware Community Project
September 2021
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
Current members
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
- Workshop
- Open Reviews
- Open Source
- Open CI

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-M
Mbed TLS
Trusted Services
Build Security Collaboratively

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

TrustedFirmware.org
All market segments

Devices

IoT/Mobile/Auto/Laptop

Embedded

Edge

Cloud

Server
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-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
Arm CCA: Open Source Software enablement

https://connect.linaro.org/resources/arm-cca/

Brand new open source component

Dynamic Secure memory support

New TF-A Monitor
Arm CCA: More resources

- Introducing the TF-A Monitor code for the Arm CCA architecture
- CCA Awakens on Arm’s Modelling Platform
- LVC21F-311 Overview of Firmware Architecture for Arm CCA
A-class Secure Software Roadmap

TF-A v2.5
EL3+S-EL2 Hafnium SPM + OP-TEE integration
Hafnium PAC/BTI/MTE
Cortex-A78AE & GIC-600AE
SMMU support Stage2
Secure FW update

FF-A:
• Notifications
• Pwr mgmt. Boot

Trusted Services:
• PSA Crypto SP
• PSA ITS, PS SP
• OP-TEE: SPMC

H1 2021

TF-A v2.6 (incl. RME support)
Armv8.7 feat (HCX, LPA2)
Armv9 Debug (ETE)
MISRA scan in OpenCI

FF-A:
• Pwr mgmt. Runtime
• Secure Interrupts (GIC emulation)
• Indirect messaging
• Trusty integration

Trusted Services:
• PSA Attestation SP
• OP-TEE: SPMC Upstream, StMM
• FF-A Linux userspace interface
• Yocto support

H2 2021

Armv8.8
Armv8-R64 PSCI
DRTM
Bloblists for info passing through BL stages

Trusted Services:
• Firmware Update
• 32-bit

H1 2022

Armv8.9

Trusted Services:
• Firmware Update

H2 2022+

FF-A next
Dynamic Secure Memory
TF-RMM
Attestation
FW Transparency
Trusted Services:
• Shim layer for legacy TAs
• fTPM

FF-A spec (SPCI) v1.0 specification EAC - https://developer.arm.com/docs/den0077/a
### 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>2 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>$100k</td>
<td>$50k</td>
<td>G1: $2.5K, G2: $10K, G3: $25K</td>
<td>$2.5K</td>
<td>$500</td>
<td>No</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