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
<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 13</td>
<td>Conception</td>
<td>Arm has idea of providing reference EL3 firmware for Armv8-A to help defragment the Arm software ecosystem</td>
</tr>
<tr>
<td>Sep 13</td>
<td>Implementation</td>
<td>v0.1 binaries in Linaro AArch64 release</td>
</tr>
<tr>
<td>Oct 13</td>
<td>Introduction</td>
<td>v0.2 source code at GitHub and LCU13 announcement</td>
</tr>
<tr>
<td>Jun 14</td>
<td>Adoption</td>
<td>Early adopters port v0.4 to silicon</td>
</tr>
<tr>
<td>Aug 14</td>
<td>Celebration</td>
<td>v1.0 released, including Juno port OP-TEE support at LCU14</td>
</tr>
<tr>
<td>Feb 15</td>
<td>Evolution</td>
<td>v1.1 completes mandatory PSCI v1.0 Trusted Board Boot prototype</td>
</tr>
<tr>
<td>Dec 15</td>
<td>Acceleration</td>
<td>v1.2 provides minimally complete TBB Upstreaming of Non-Arm platforms</td>
</tr>
<tr>
<td>Oct 16</td>
<td>Extension</td>
<td>v1.3 adds AArch32 PSCI Dropped CLA, security hardening</td>
</tr>
<tr>
<td>Jun 17</td>
<td>Optimisation</td>
<td>v1.4 adds DynamIQ, GIC-600, SCMI, PSCI with OP-TEE, HiKey/HiKey960</td>
</tr>
<tr>
<td>Mar 18</td>
<td>Expansion</td>
<td>v1.5 introduces RAS &amp; Secure Partitions, Dynamic Configuration, Armv7 support</td>
</tr>
<tr>
<td>Oct 18</td>
<td>Open Governance</td>
<td>v1.6/v2.0 – TF.org migration with TF-M</td>
</tr>
</tbody>
</table>
Build Security Collaboratively

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

Diagram:
- **TF.org Patch** → **Push 1** → **Jenkins** (Trigger 2) → **Artifacts** → **Jenkins** (Trigger 3) → **Build Slaves** → **Result +1** → Partner’s boards
- **Jenkins Build Slaves** → **Jenkins** (Trigger 3) → **Artifacts** → **LAVA** (validation.linaro.org)

**MPS2**

**Junot**
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 (Ongoing migration into TF.org)

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.
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

Contact:

enquiries@TrustedFirmware.org for more information

* Fee according to company size and type
Thank you

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