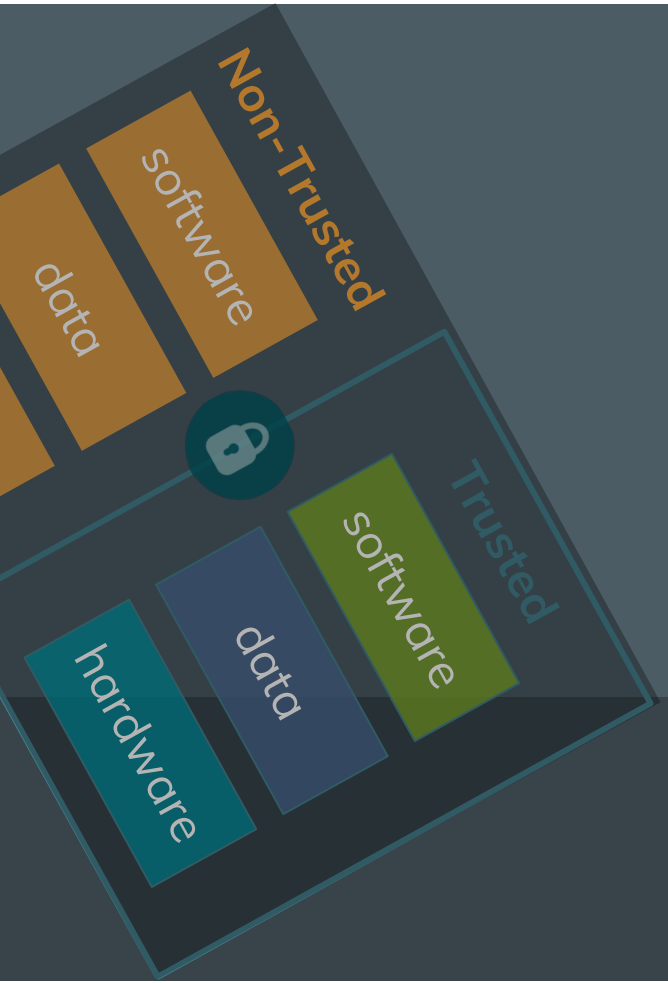


Open Source Secure World Software

Trusted Firmware

Update November 2018

SPONSORED BY: arm

HOSTED BY: Linaro

Trusted Firmware

Arm's Trusted Firmware is adopting open governance

Reference implementation of secure world software for Armv8-A and Armv8-M

Membership of the Trusted Firmware project is open to all

Everyone interested in Trusted Firmware is encouraged to join

Initial Members

Arm
Cypress
Data I/O
Google
Linaro
Texas Instruments

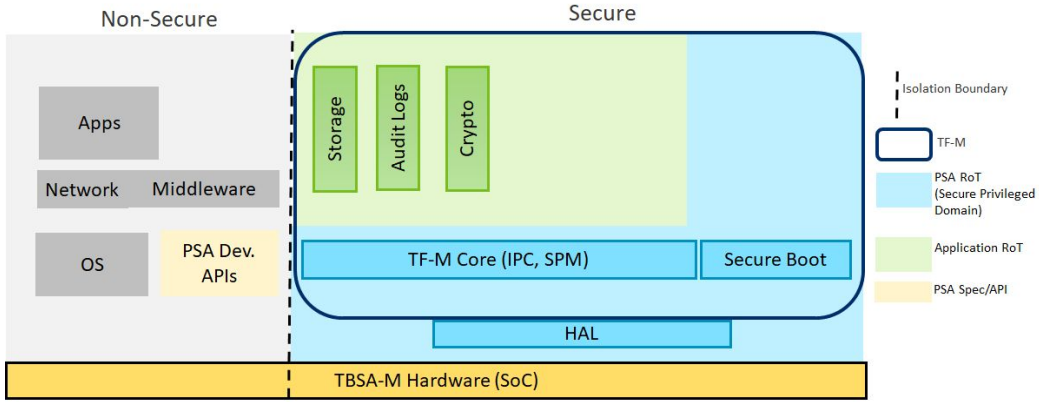
TrustedFirmware.org

Trusted Firmware-M

- Provides Software Components for building a Secure Platform providing
  - Isolated Secure execution environment for Arm v7-M and v8-M
  - Secure services invoked from Non-Secure apps
  - Trusted device initialisation and Trusted boot
- Reference Implementation of Arm Platform Security Architecture (PSA)
  - Aimed at Constrained Devices
  - Flexible and Configurable design allowing Partners to adapt to meet their needs
  - Different levels of Isolation, Leverages Trustzone in v8-M.
- Initial implementation of Secure Boot, Secure Storage, Crypto and Audit Logs available

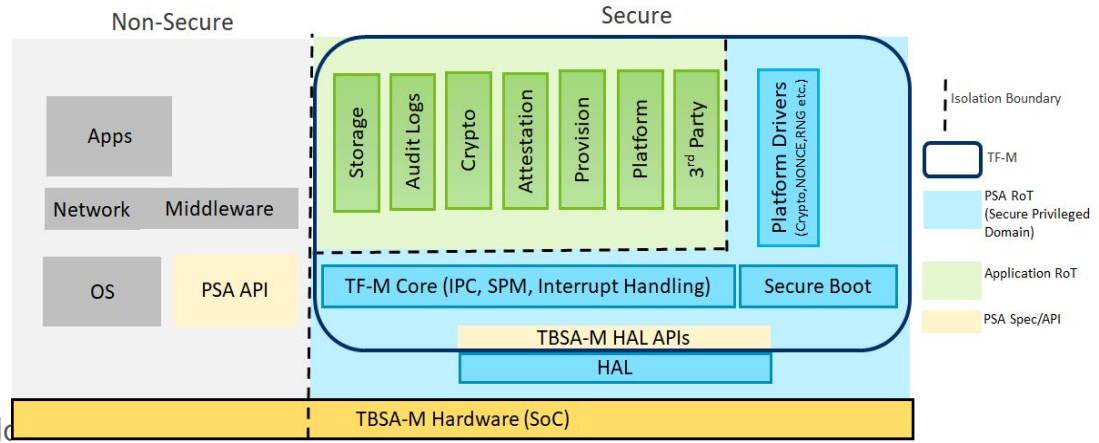
Trusted Firmware-M – Progress since YVR'18

- PSA Firmware Framework
  - IPC Implementation being done
- Initial Attestation Service
  - PSA API under review
- Secure IRQ Handling
  - Initial Implementation
- Support for latest Arm IoT Reference platform - Musca-B1
- PoC with mbedOS/Pelion Cloud
  and Zephyr/Google Cloud shown at ELC-E
- Presentations at ELC-E



Trusted Firmware-M Plan

- Q4 2018
  - Attestation - Initial Attestation Service
  - Scheduler Design
  - Crypto Service Enhancements
  - IPC Enhancements
  - Open Continuous Integration (CI)
- Q1 2019
  - Full Isolation (Level 2 & 3)
  - Scheduler Initial Implementation
  - Secure Boot - Multiple Image Upd
  - Platform APIs - NVCount, Timer
  - Provisioning - Initial Investigation/API Prototype
- Q2 2019
  - Scheduler Enhancements
  - [Secure Boot] Key Revocation
  - [Secure Storage] Lifecycle Management
  - [Audit Logs] Secure Storage, Crypto Binding
  - [Platform] GPIO, Debug, NONCE



Trusted Firmware-A – Progresses since YVR'18

- Trusted Firmware-A Tests first open source release (v2.0)!
  - See detailed blogpost & project landing page on TF-A-Tests Git repository
  - BSD 3-clause license and contributions accepted under DCO as parent TF-A project
- TF-A codebase recent progresses:
  - Dynamic Configuration
    - Position Independent Executable (PIE) support for BL31 (enabled for FVPs)
  - Added option to jump straight to Linux Kernel in AArch32 mode without the need for an intermediate BL33 boot-loader (option already present in AArch64 mode)
  - Platforms support
    - Arm NeoVerse N1 System Development (N1SDP)
    - Arm SGI-Clark.Ares
    - Renesas R-Car Gen3
    - Amlogic Meson S905
    - Armada 3700

Trusted Firmware-A – Plans for Q4 2018 / H1 2019

- Plans for Q4 2018 / H1 2019:
  - Secure Partitions
    - Enhanced Secure Partition Manager for Multiple S-EL0 partitions
    - SPCI/SPRT Alpha/Beta specifications support
  - Trusted Firmware-A migration to new TrustedFirmware.org infrastructure
    - **Phase 1: TF-A-Tests go live announcement under Git/Gerrit @trustedfirmware.org**
    - Phase 2: TF-A codebase migration from GitHub to Git/Gerrit @trustedfirmware.org
    - Phase 3: CI migration from internal Arm infrastructure to trustedfirmware.org
  - SCMIv2 specification support
  - Armv8.x architectural features support
  - v2.1 Release (March 2019)

TrustedFirmware Project Activity

TrustedFirmware TF-A Project Activity

Domains by Commits for October

Domains	Commits
arm.com	163
baylibre.com	17
marvell.com	9
st.com	7
ti.com	4
linaro.org	4
socionext.com	2
semihalf.com	2
siemens.com	1
nvidia.com	1

Generated 2018-11-07

- Total Files: 1833
- Total Lines of Code: 309340 (491099 added, 181759 removed)
- Total Commits: 4308 (average 3.8 commits per active day, 2.3 per all days)
- Total Authors: 171 (average 25.2 commits per author)

TrustedFirmware TF-A Project Activity

Top 10 authors for October

Author	Email	Commits
Soby Mathew	soby.mathew@arm.com	47
Antonio Nino Diaz	antonio.ninodiaz@arm.com	36
Andre Przywara	andre.przywara@arm.com	21
Antonio Niño Díaz	antonio.ninodiaz@arm.com	18
Jorge Ramirez-Ortiz	jramirez@baylibre.com	17
Konstantin Porotchkin	kostap@marvell.com	9
Daniel Boulby	daniel.boulby@arm.com	9
Chandni Cherukuri	chandni.cherukuri@arm.com	9
Yann Gautier	yann.gautier@st.com	7
Dimitris Papastamos	dimitris.papastamos@arm.com	7

TrustedFirmware TF-M Project Activity

Generated 2018-11-07

Domains by Commits for October

Domains	Commits
arm.com	11
linaro.org	1

- Total Files:
  511
- Total Lines of Code:
  115461 (157417 added, 41956 removed)
- Total Commits:
  227 (average 2.0 commits per active day, 0.7 per all days)
- Total Authors:
  18 (average 12.6 commits per author)

TrustedFirmware TF-M Project Activity

Top 10 authors for October

Author	Email	Commits
Antonio de Angelis	antonio.deangelis@arm.com	4
David Vincze	david.vincze@arm.com	3
Jamie Fox	jamie.fox@arm.com	2
Marc Moreno Berengue	marc.morenoberengue@arm.com	1
Karl Zhang	karl.zhang@linaro.org	1
Alexander Zilberkant	alexander.zilberkant@arm.com	1

How to Get Involved

Become a project member

Platinum Board (voting) members define the mission and strategy: $50K/year

General members receive project updates, make requests to the board and may attend monthly calls: $2.5-25K*/year

Maintainers to be appointed from members

* Fee according to company size and type

Contact:

board@TrustedFirmware.org

for more information

TrustedFirmware.org