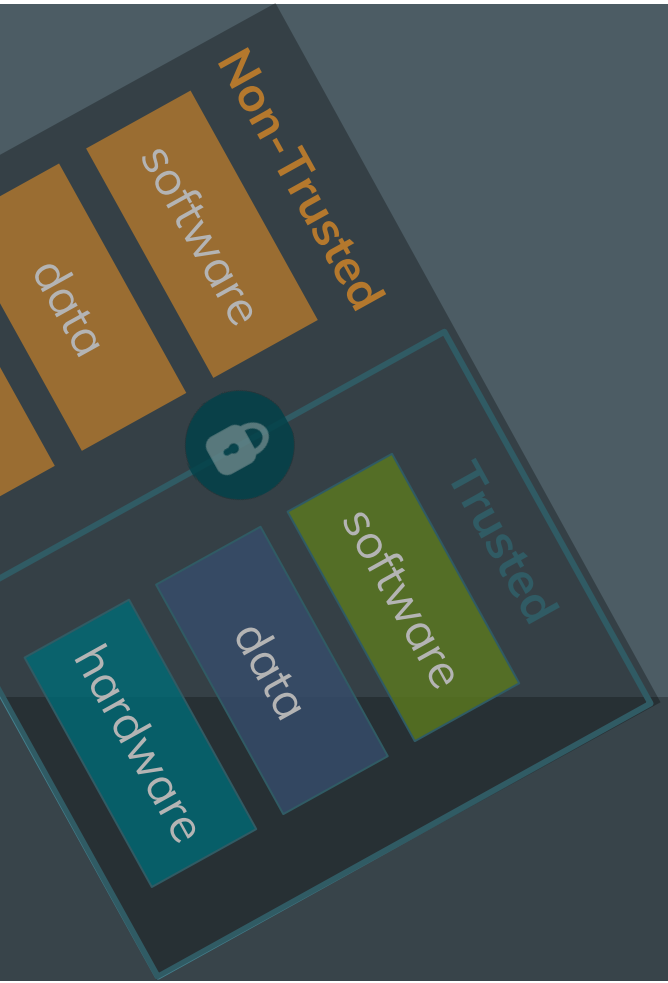


Open Source Secure World Software

Trusted Firmware

Update February 2019

SPONSORED BY: arm

HOSTED BY: Linaro

Trusted Firmware

Trusted Firmware adopted open governance in October 2018

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

Members (February ‘19)

Arm

Cypress

Data I/O

Google

Linaro

Texas Instruments

STMicroelectronics

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, Attestation and Audit Logs available

Trusted Firmware-M – Feb'19 Progress

- TF-M v1.0-Beta Tag
  - Enabled TF-M Users (Silicon Platforms, RTOSes) to be PSA Level1 and Functional API certified(https://psacertified.org/)
  - PSA APIs for Secure Storage, Crypto and Attestation Implemented.
- TF-M Integration on v8-M platforms showcased at Embedded World'19
- PSA Firmware Framework IPC Support merged to master.
- Initial Attestation Service implemented following EAT Specification with a set of claims
- Arm/Cypress Collaboration progressing to enable TF-M for dual v7-M/pSoC6
- Secure Boot Rollback Protection Design posted for review.

Trusted Firmware-M Plan

CQ1-Q2'19

- [TF-M Core] Secure Partition Manager- Level 2 Isolation
- [Secure Storage] Compatible with PSA Firmware Framework IPC
- [Crypto] Compatible with PSA Firmware Framework IPC
- [Attestation] Compatible with PSA Firmware Framework IPC
- [Secure Boot] Rollback Protection

CQ2-Q3’19

- [TF-M Core] Multiple Secure Context, Interrupt Handling
- [Storage] Crypto Binding
- Boot and Runtime Crypto Hardware Integration

Trusted Firmware-A – February ‘19 Progresses

- v2.1 preparation
  - Code freeze by 15th March - Release end of March / early April
  - Armv8.3 Pointer Authentication support completed
  - Armv8.5 PSTATE.SSBS support completed (for both Cortex-A76 / Neoverse-N1)
  - Various errata for Cortex-A53, A55, A57, A73, A75, A76
- Armv8.5 BTI enablement ongoing (need official GCC9 support)
- Secure Partitions:
  - Reviewing SPCI Alpha2 spec and planning Foundation work (Resource description)
  - Planning investigation on multiple signing domains for multiple Secure Partitions
- Investigating and planning Platform Security Requirements
  - Measured Boot, [Discrete/Firmware] TPM interactions & Boot Flow
  - Dynamic configuration and Secure world → Normal world information passing

Trusted Firmware-A – Plans for H1/H2 2019

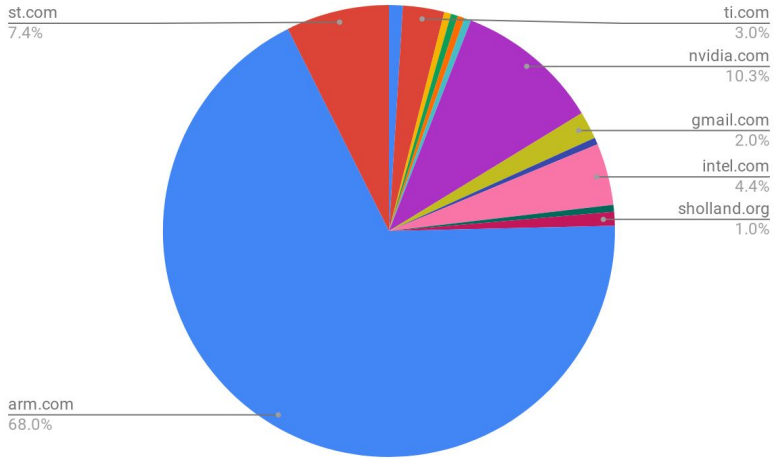
- Secure Partitions
  - H1.19 Resource Description and Chain of Trust support (including Multiple Signing domains)
  - H2.19 Multiple S-EL0, S-EL1 coexistence & TOs integration support w/out S-EL2
- Armv8.5 Memory Tagging Extensions at EL3
- Armv8.5 BTI enablement
- Platform Security Requirements investigation
  - Measured Boot reference flow
- Trusted Firmware-A migration to new TrustedFirmware.org infrastructure
  - **Phase 0 (Q4.2018): TF-A-Tests go live announcement under Git/Gerrit → Completed**
  - **Phase 1 (Q1.2019): TF-A codebase migration from GitHub to Git/Gerrit → Ongoing**
  - Phase 2 (Q2.2019): Public CI - Continuous Build open-source infrastructure
  - Phase 3 (Q3.2019): Public CI - Continuous Testing on FVPs
  - Phase 4 (Q4.2019): Public CI - Continuous Testing on LAVA Board Farm

TrustedFirmware TF-A Project Dashboard

Top Authors this month

antonio.ninodiaz	80
vwadekar	16
yann.gautier	15
dimitris.papastamos	9
ambroise.vincent	9
tien.hock.loh	8
louis.mayencourt	8
sandrine.bailleux	7
afd	6

Commits by domain this month



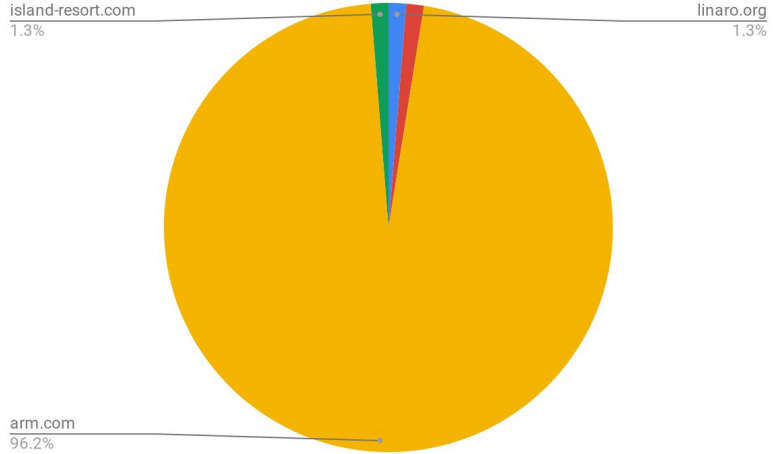
Commit history

TrustedFirmware TF-M Project Dashboard

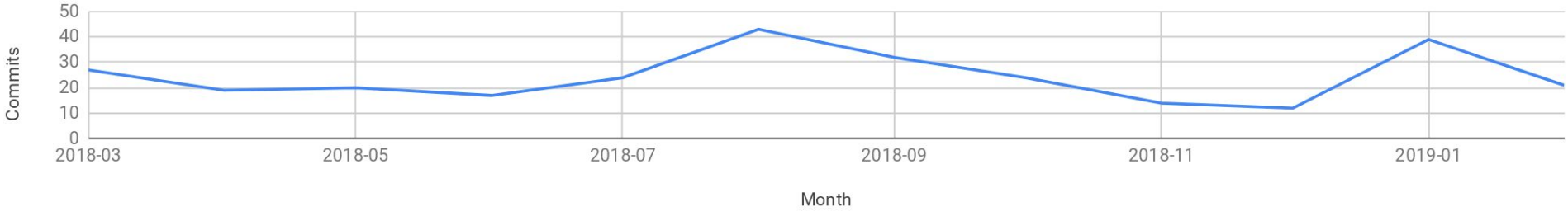
Top Authors this month

tamas.ban	37
jamie.fox	12
marc.morenoberengue	7
antonio.deangelis	6
edison.ai	4
ashutosh.singh	3
gyorgy.szing	3
lgl	2
mate.toth-pal	2

Commits by domain this month



Commit history

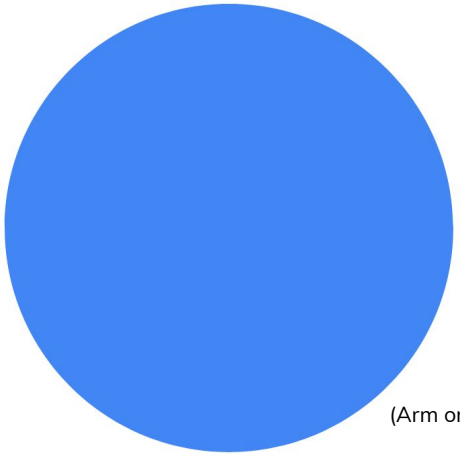


TrustedFirmware TF-A Tests Project Dashboard

Top Authors this month

ambroise.vincent	5
chandni.cherukuri	3
sandrine.bailleux	3
john.tsichritzis	1
antonio.ninodiaz	1
joel.hutton	1

Commits by domain this month



Commits vs Month

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