Contents

• What is Trusted Firmware? What is new?
• What is PSA?
• Open Source Project
• Learn More
• Q & A
What is Trusted Firmware?

It is a set of foundational software components which implement the services required for a secure platform:

• Reference software for partners to build on which creates a trusted execution environment
• Secure Function invocation (Software Interface to TrustZone)
• Secure Device Initialisation and Setup
• Trusted Boot (image verification derived from RoT)
• PSA Compliance (more on this later)
What is Trusted Firmware? (cont’d)

This Reference Software is designed to be:

• Ported to applicable SoCs to ensure they provide the system security offered by the hardware – **Minimise Production Effort**

• A standardisation of how secure services get invoked to allow for more portable secure software integrations – **Ease Software Integration**

• A standardisation of how hardware functions to support security get invoked (to optimally address vulnerabilities) – **Security by Scale**
This is not new!

Trusted Firmware for A-profile systems (TF-A)

• Mature Open Source Project
  • v0.2 went public in October 2013 (http://connect.linaro.org/resource/lca14/lca14-102-adopting-arm-trusted-firmware/)
  • Well established collaboration model
  • Security Incident Handling
  • Security and MISRA hardened (and ongoing hardening)

• Used in most production Armv8-A systems
  • Trusted Boot Support
  • Integrated with main TEEs and secure software solutions
Trusted Firmware A

Reference boot flows
- For all Armv8-A systems
- AArch64 & AArch32 support
- Armv7-A systems support

Open Source at GitHub
- BSD License
- Contributors welcome (DCO)

Latest release = v1.5
- RAS (SPM, SDEI, EHF) support
- Secure Partitions initial support
- PSCI v1.1 & SMCCC v1.1 support
- Dynamic Configuration Phase 1
- BL2 optional execution at EL3

https://github.com/ARM-software/arm-trusted-firmware
Trusted Firmware M (TF-M) is new!

TF-M builds on TF-A terminology & principles to create a unified approach for secure device software:

- Isolated secure and non-secure execution environments
- Methods to invoke secure services from non-secure apps
- Trusted device initialisation and trusted boot mechanisms

Albeit more honed to the M-profile device eco-system

- Aimed at more constrained devices, thus more configurability
- Different mechanism for TrustZone isolation
- Much more fragmented OS and software eco-system
TF-M is the start of a journey

TF-M provides a good starting point for secure software implementations now, but there is lots more to do…
What is PSA?

Relevant to all segments – but starting with IoT
Platform Security Architecture for simpler IoT security

A recipe for building secure systems from analysis to implementation

Analyse
- Threat models and security analyses

Architect
- Firmware architecture & hardware specifications

Implement
- Source code & hardware IP

PSA documents

Enabling products & contributions
Threat Models and Security Analyses

- Asset Tracker TMSA
- Smart Water Meter TMSA
- Network Camera TMSA

https://pages.arm.com/psa-resources.html
PSA Firmware Framework Concepts

- Secure Partition Manager (SPM)
  - provides the boot, isolation and IPC services to the SPE
- Partition
  - the unit of execution
- Secure function
  - a set of related APIs invoked through secure IPC
- Trusted function
  - a secure function that provides a Root of Trust
PSA - Standardized interfaces

PSA specifies interfaces to decouple components

- Enables reuse of components in other device platforms
- Reduces integration effort

PSA provides an architectural specification

- Hardware, firmware and process requirements and interfaces
- Partners can provide alternative implementations

Trusted Firmware is example PSA software
(Back to) Trusted Firmware M - Plans

1. Align with the PSA specifications by the time they make public release
   1. Standardised APIs for crypto, attestation, secure storage, IPC, hardware RoT, audit logging, debug control, etc
   2. Full SPM and IPC to isolate many secure functions and their interactions
   3. Device initialisation, Trusted boot and firmware update
   4. Many build configurations to support from most constrained to most secure

2. Support Arm development platforms and IP
   1. Musca test-chip, SDK-20x FPGA on MPS2/3, AEMv8-M/IoT-kit FVP
   2. V8-M system IP, Arm Cryptocell, Arm CryptoIsland

3. Support and enable contributions
   1. Partner SoCs and systems
   2. Software integrations – secure services, RTOSes, secure-OSes

All in a public open source project
Open Governance Trusted Firmware

• Trusted Firmware for A-profile Arm SoCs has been publicly available as free open source software for many years at https://github.com/ARM-software/arm-trusted-firmware

• This software has received contributions from many partners and is very widely used across the eco-system

• Now that partners depend on this firmware (or have expectations of depending on TF-M) it has been requested that this open source software been moved to an open governance model

• While developed as reference code by Arm, it is designed to provide common functionality across all the partnership SoCs and products.

• Enable the whole ecosystem to participate and steer the direction of the project.
Linaro Community Projects Division

Linaro is forming a new division to host open-governance open source software projects
• Projects are operated independently from the main Linaro organisation
• Each project has own board, committees, funding, URLs, etc
• This division is contracted to provide services such as IT infrastructure, finance, legal, marketing and engineering – as requested by the project
• Project membership equally open to Linaro members and non-members
• For each project:
  • Board members – kept between viable minimum and project maximum
  • General members
    Get to steer strategy and investment plans for the project
Infrastructure is live now

https://git.trustedfirmware.org/
  • Public Git containing TF-A and TF-M master codebases

https://review.trustedfirmware.org
  • Public Gerrit review server for patch submissions and review

https://issues.trustedfirmware.org/
  • Public phabricator ticket server for bugs and change requests to be raised

Codebase includes maintainer files and contribution guidelines

TF-M ready to take contributions there now

TF-A will transition from GitHub contributions over next few months
Get Involved

Platinum, General and Community memberships available

- Linaro and Arm presenting details to potential members
- Take partial ownership of a project you depend on
- Ensure your dependencies are maintained and continually validated
  - Your Board in the CI farm
  - Your Software Tests in the CI suite
- Reduce internal maintainership costs by pushing generic features you need
- Help ensure that the open source community supports Trusted Firmware interfaces and features

Contact board@trustedfirmware.org for more information
Deep dive presentations around TF-M this afternoon

1. Trusted Firmware M : Core and Partition Manager (Miklos Balint)
2. Trusted Firmware M : Secure Storage (Ashutosh Singh)
3. Trusted Firmware M : Trusted Boot (Tamas Ban)

Hacking in the LITE room to integrate TF-M and Zephyr for Arm v8-M platforms
• Ask now (or after the presentation)
• Come to the LITE hacking room and find a TF engineer
• Email board@trustedfirmware.org or james.king@arm.com
Thank You!
Danke!
Merci!
谢谢！
ありがとう！
Gracias!
Kiitos!