Linaro Connect
MADRID 2024 | MAY 14-17 2024

TrustedFirmware.org Project Update

Matteo Carlini & Shebu V. Kuriakose

Gearing up for Cyber Security Regulations?

THE WHITE HOUSE

FEBRUARY 26, 2024

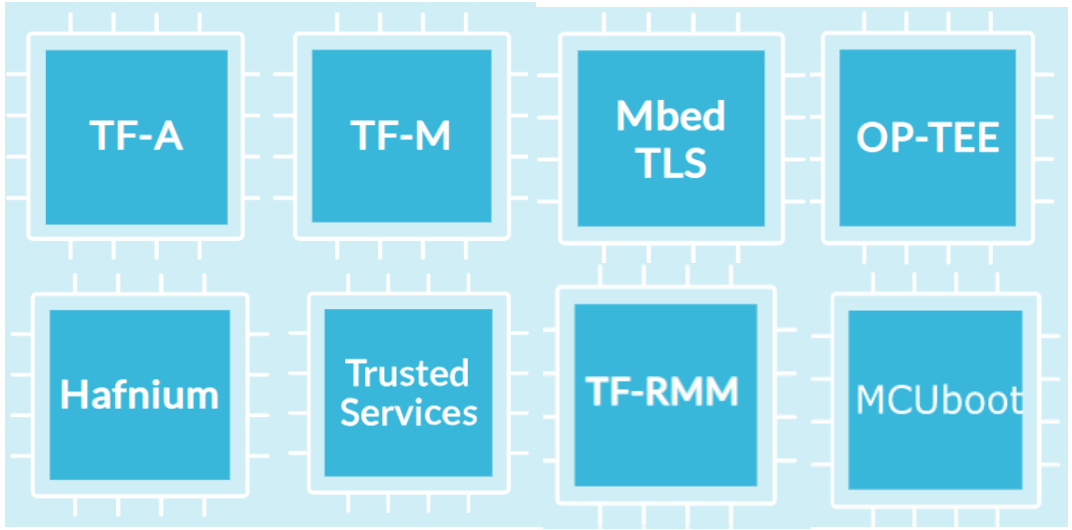
Press Release: Future Software Should Be Memory Safe

Collaborative Security: Meet Regulations Economically

Regulatory Requirements

- Updates
- Vulnerability Reporting
- Secure Communication
- Secure Storage
- Crypto
- Authentication
- Logging

Collaborative Security: Meet Regulations Economically



Regulatory Requirements

- Updates
- Vulnerability Reporting
- Secure Communication
- Secure Storage
- Crypto
- Authentication
- Logging

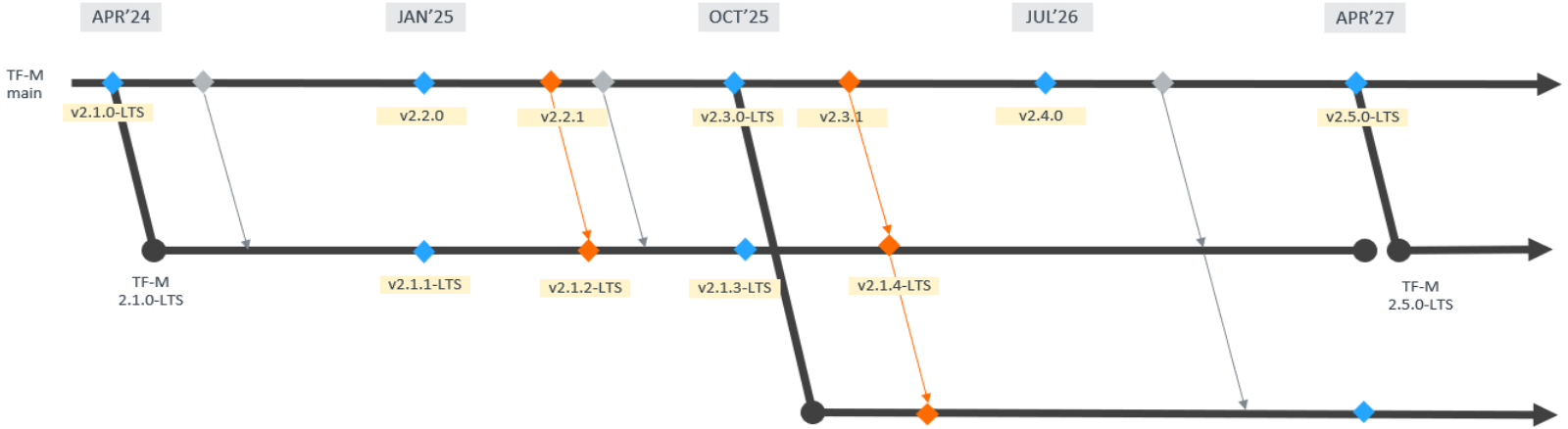
Long Term Support: Keeping Devices Secure

- Community effort to provide TF-A Long Term Support
  - Maintained for 5 years and a new LTS created every year
- Backporting bug and security fixes
- 2 live LTS branches today with 22 releases done so far.
- Maintenance effort coming from multiple organizations
- Hugely reduces burden of individually maintaining support branches by Silicon Providers and OEMs.

Launching TF-M Long Term Support

- Project extending Long Term Support to TF-M Project
  - v2.1.0 released
  - Maintained for 3 years and a new LTS created every 18 months
  - Includes Mbed TLS/PSA Crypto LTS

- Backporting security and bug fixes



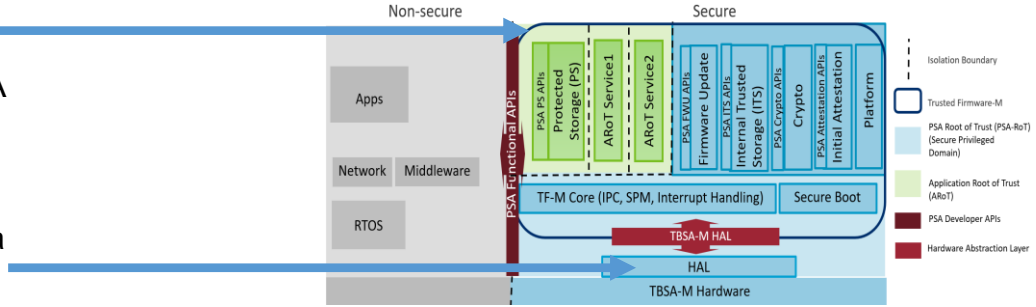
TF-M LTS & PSA Certifications

- Today chips PSA Certified using a particular version of TF-M
  - No efficient way to update PSA certificate with future TF-M versions
  - Certificate can be invalid once vulnerabilities found in TF-M

- Efficient way to update PSA Certification of chips with latest security and bug fixes.
  - Chips certified using TF-M LTS can move to updated LTS versions keeping the PSA certificate valid
  - Chip vendors able to ship latest PSA Certified TF-M that end devices can use.

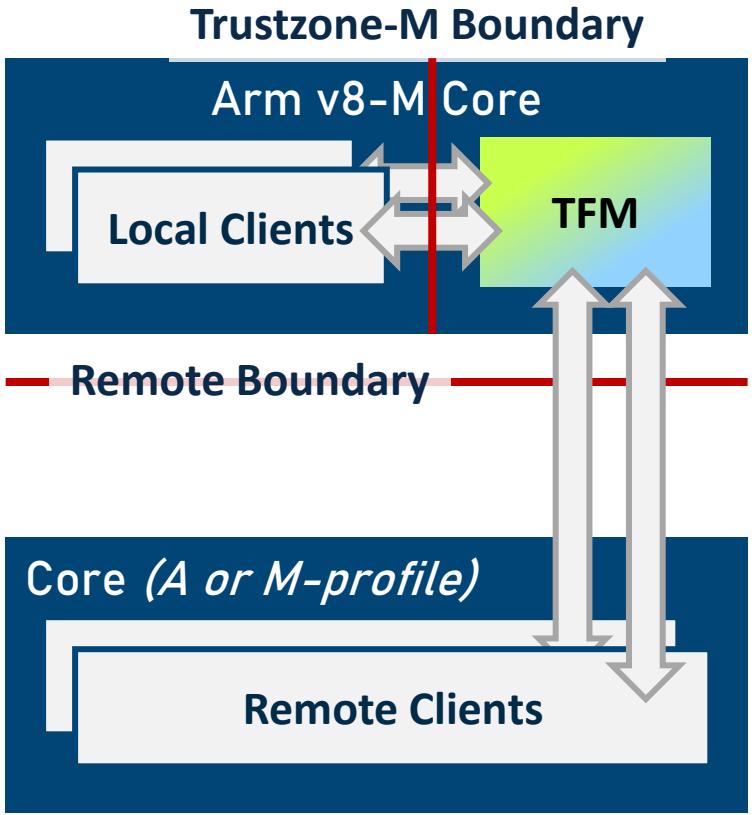
Platform independent TF-M fixes in LTS release evaluated once by Lab. and applicable to all PSA Certified chips based on the LTS release.

Chip vendors will have to undertake delta evaluation if changes in platform code



Securing Hybrid Platforms with TF-M

- TF-M: Secure Processing Environment (RoT) for Cortex-M cores
  - Non-Secure Application and RTOS as clients avail TF-M secure services
- Community collaborating on enabling TF-M as RoT for platforms beyond Cortex-M only MCUs
- Hybrid platforms contain A and M-profile or multiple M-profile cores.
  - TF-M as RoT runs on the secure side of Trustzone enabled M-profile core
  - Remote and local clients avail services from TF-M
  - Different solution configurations to meet different client requirements



Welcome ProvenRun!

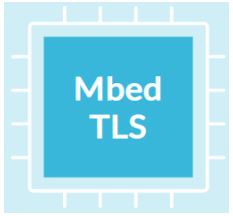
Diamond Members

Platinum Members

General Members

Partners

Projects milestones & news



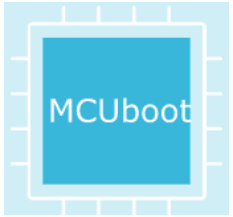
v3.6.0 LTS release

Upcoming:
- v4.0 release
- TF-PSA Crypto

FF-Av1.2 support
SME enablement
Upcoming:
- Secure Timer Virt
- FW Update Live activation

CCA RMMv1.0
EAC5 spec support

RMMv1.1 support upcoming

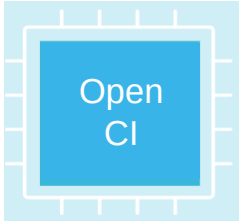


v2.0.0 release

v2.1.0 upcoming

- v1.0.0 release
- PSA services for Cortex-A devices

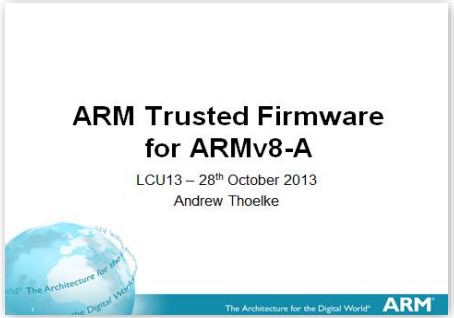
Upcoming:
- fTPM support
- mbedTLS updates



- MISRA for TF-A/M
- 5M+ tests per year
- 12 members platforms

Upcoming:
- TF-RMM
- Trusted Services

Celebrating 10+ Years of Trusted Firmware-A
LCU13 to MAD24



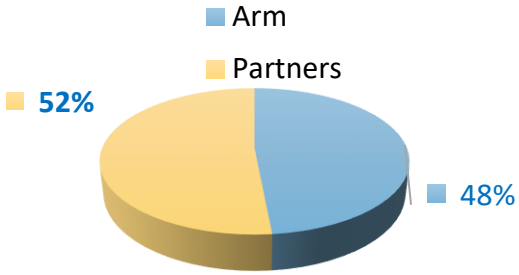
```
commit
4f6ad66ae9fcc8bcb3b0fcee10b7ab1ffcaf1a56
Author: Achin Gupta
<achin.gupta@arm.com>
Date:   Fri Oct 25 09:08:21 2013 +0100

    ARMv8 Trusted Firmware release v0.2
```

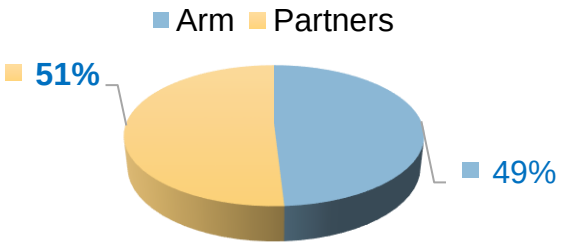
2013 – LCU13 | 2018 – YVR18 | 2023 – LON23 | MAD24

TF-A: Collaboration in action

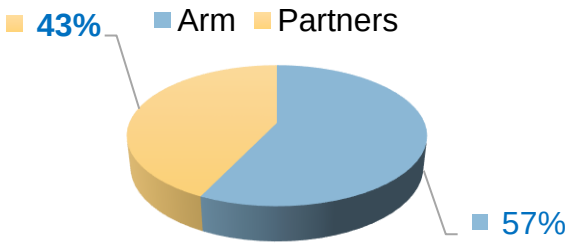
TF-Av2.8 (Nov ‘22)



TF-Av2.9 (May ‘23)



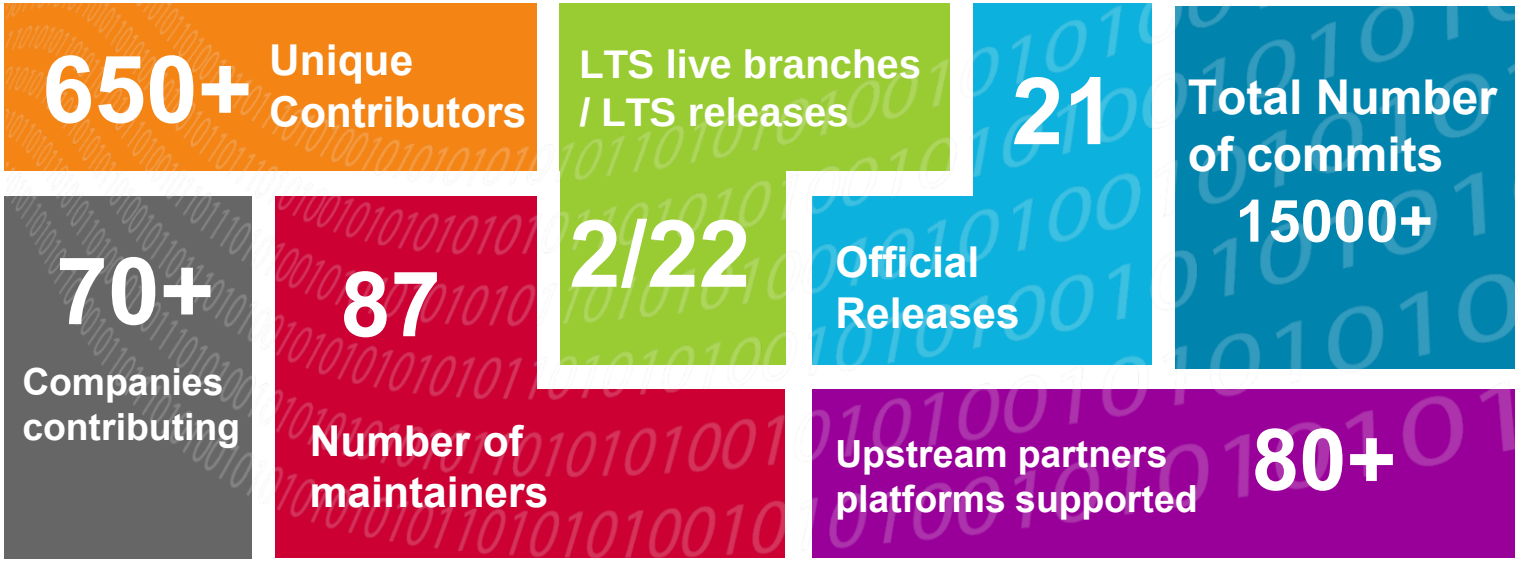
TF-Av2.10 (Nov ‘23)



Top Contributors (beyond Arm):

- NVIDIA
- STM
- AMD/Xilinx
- Linaro
- NXP
- Google
- Mediatek
- Intel
- Renesas

TF-A 10+yrs worth of statistics (as of April 2024)



Trusted Firmware Sessions @ Linaro Connect

- MAD24-106 10 years with OP-TEE
  - Tue, May 14th 15:55
- MAD24-420 OP-TEE device drivers frameworks
  - Fri, 17th May 12:40
- MAD24-325 Implementing an FF-A Secure Partition Manager in Rust
  - Thu, May 16th 15:45
- MAD24-327 Recent implementations/refactoring in TF-A
  - Thu, May 16th 16:20
- MAD24-416 Enabling mobile trust thanks to DPE/DICE in Android
  - Fri, May 17th 12:05
- MAD24-409 Arm Confidential Compute Architecture open-source enablement
  - Fri, May 17th 10:55

Now the moment you've all been waiting for…

Linaro Connect
MADRID 2024 | MAY 12-17 2024

Thank you

Now the moment you've all been waiting for…