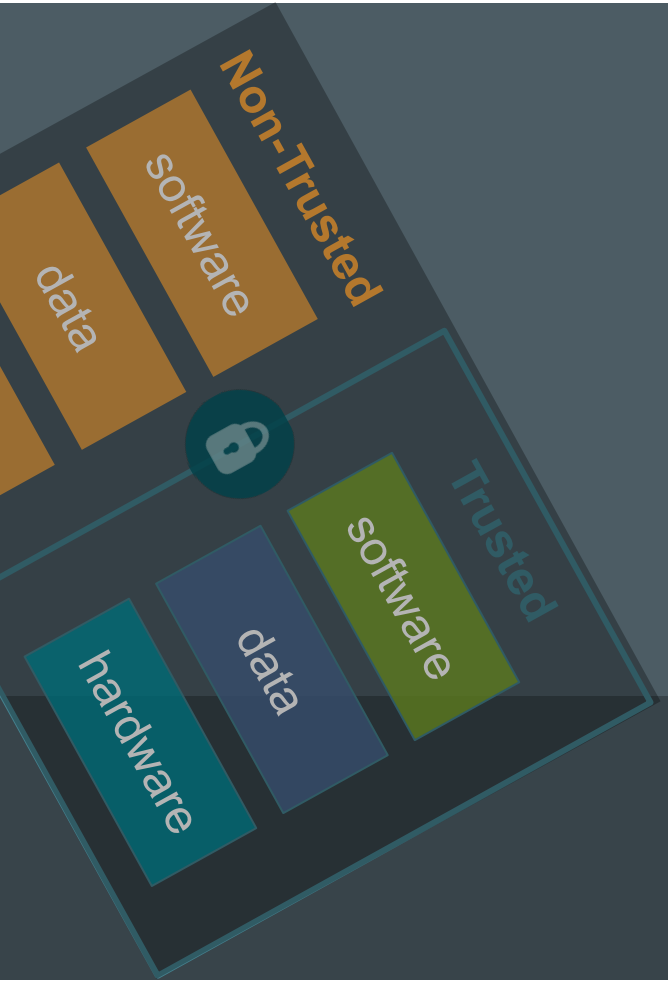


Open Source Secure World Software

Trusted Firmware Governing Board Meeting

For TSC

18 October, 2023

HOSTED BY:

Linaro

Agenda

- Open CI Updates
- General Topics
  - PSA Certified and TF-M LTS
  - MBed TLS/PSA Crypto Update
  - Marketing Update
  - AOB

board@lists.trustedfirmware.org

Vote Results: Membership Restructure

Vote Results: Passed with 100% of membership voting “Yes”

Next steps:

- Use the adjusted rates from the vote to assure balanced FY24 Budget - Done
- Adjust pricing with Linaro finance to begin sending out near-term quotes to members
- Update Website with newly approved Charter and Membership Agreement
- Update the overview slide deck and post on the website
- Send out the FY2024 budget for Board Vote

Open CI Updates

Open CI Updates

Progress - August/September

- TFC-274: Mirror TF-A, TF-M and Trusted Services repo in TF github
  - Delivered to production
- TFC-493 TF-A CI: Support for staging area or similar environment for testing during toolchain-upgrade
  - Support for TF-As' plans to upgrade the toolchain for every release (6-month cycle).
- TF-A/M Release Support
  - Analysis of issues during stress testing
  - Note: Community Mgr approved adding 2 backend servers for 2 months (~$1,200) to support TF-A release
    - Increase number of FVP workers
    - Decrease LAVA timeouts/number of LAVA resubmission retries
- Boards/Lab
  - Chromebook - Corsola - deployed and running tests
- MISRA TF-A / TF-M efforts
  - Collaborating w/ Bugseng for a MISRA White Paper; awaiting final review before publishing

Active Issues:

- Active Hardware Issues
- Active Infrastructure Issues
  - Monitoring infrastructure TF-M/A releases in November.

Open CI Priorities

Identified Priorities for FY'24 (Can tweak/add based on Trusted Firmware Board feedback)

- Deploy new member boards
- TF-A LTS
- Integrating new compiler licensing technology (UBL)
- Add IAR compiler support for TF-M and Mbed TLS
- Bugseng (MISRA) TF-M and any TF-A tuning after receive all feedback
- TF-RMM Infrastructure
- Verify Disaster Recovery process, procedures, docs
- Trusted Services CI
- TF-A Windows Build

Priorities - over the next month

- Support TF-M/A releases
- Enable UBL Licensing Support
- Enable FVP jobs in the cloud
- Provide estimate for adding IAR compiler

Reminders: Current deployed devices, Job test results, EPIC: Trusted Firmware Community Board Enablement

Open CI Platform Prioritized Backlog

Current Open CI Platform Enablement Activities:

1. Add Renesas EK-RA6M4 - On hold
2. Add Corsola Chromebook - Done
3. Google next Chromebook - Holder for FY 23
4. ST next platform - Holder for FY 23

Board enablement pipeline now caught up.
Next boards?

Member	Platform	FY '21	FY '22	FY '23	FY '24
Renesas	EK-RA6M4	1/1			
ST	STM32MP15		1/2		
ST	STM32U5		2/2		
Google	Chromebook Tomato		1/2		
Google	Chromebook Corsola		2/2		
Arm	N1SDP			1/2	
Google next	Chromebook next			1/2	
ST next	STM32xx			1/1	

Platform Quota usage per members

General Topics

PSA Certified & TF-M Long Term Stable (LTS)

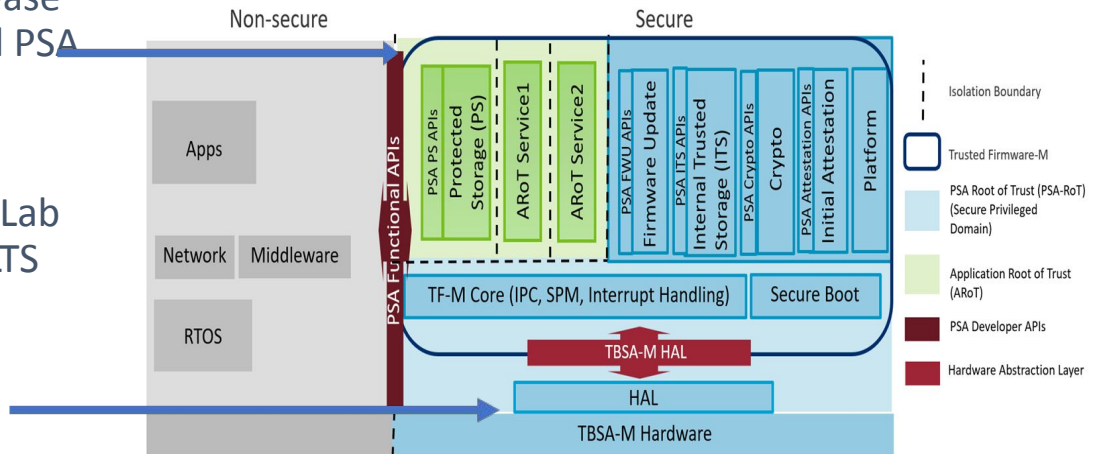
- Today chips are PSA Certified using a particular version of TF-M (PSA Updatable RoT)
  - No efficient way to update PSA certificate with future TF-M versions – Expensive & time consuming.
  - Certificate can be invalid once vulnerabilities found in TF-M
- TF-M LTS enables an efficient way to update PSA Certification of chips with latest security and bug fixes.
  - Chips are certified using a TF-M LTS release. Chips then update to future LTS updates after updates go through PSA Security evaluation
  - Certificate can be kept valid and latest TF-M shipped in chip vendor SDKs and in end devices
- New LTS release created every 18 months and maintained for 3 years. During the 3years,
  - 9-monthly bug fix LTS update releases alongside the 9-monthly mainline releases
  - Ad hoc security fix releases
- Platform independent TF-M fixes are evaluated once & applicable to PSA Certified chips on the LTS release.
  - Platform specific changes would require chip specific evaluation.

Trusted Firmware-M LTS – Generic & Platform Specific Changes

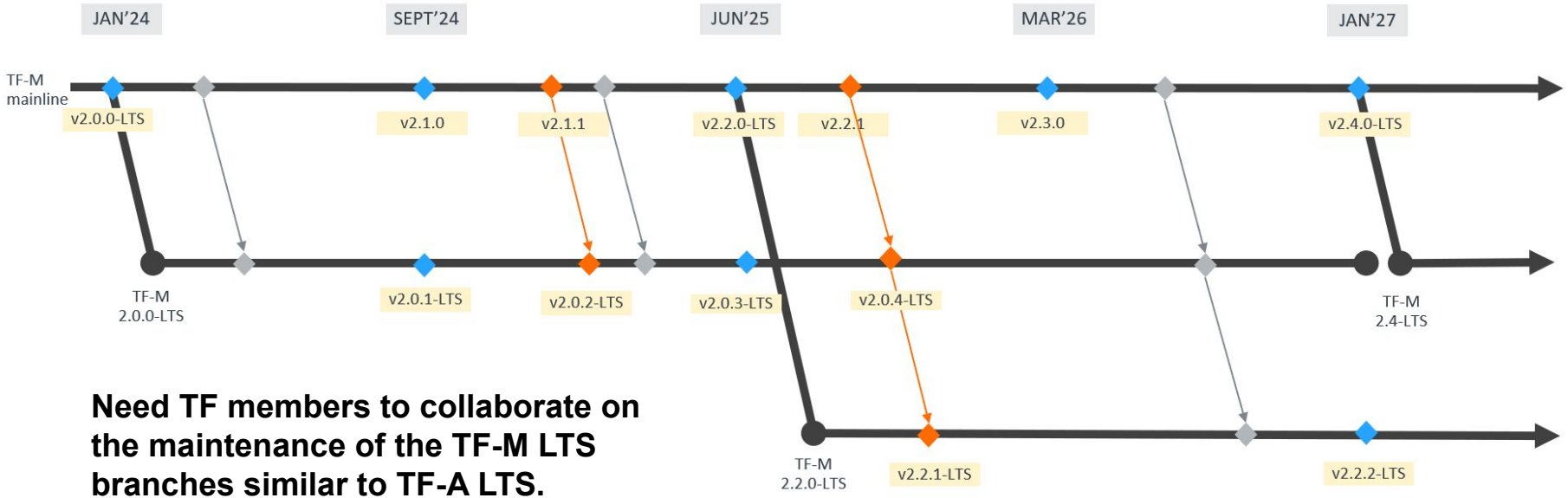
Platform independent TF-M fixes in LTS release evaluated once by Lab. and applicable to all PSA Certified chips based on the LTS release.

Trustedfirmware.org & Arm will work with Lab and TrustCB to evaluate changes between LTS releases

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



3 Year LTS; Created every 18months; Released every 9 months



Need TF members to collaborate on the maintenance of the TF-M LTS branches similar to TF-A LTS.

Will be challenging for Arm to undertake the maintenance on its own

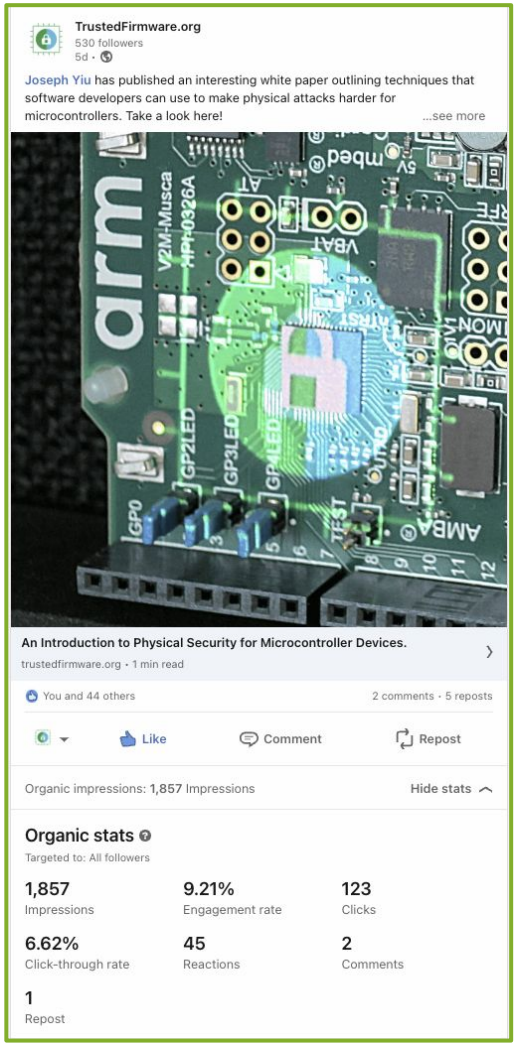
Mbed TLS, PSA Crypto Update

- New repository, **TF-PSA-Crypto** published in Mbed TLS github
  - Provides PSA Crypto API reference implementation
  - Prototype read only repository for now
  - Aim to make the repository the live development repository by early next year
  - Makes PSA Crypto implementation separate from Mbed TLS

- Mbed TLS and TF-PSA-Crypto going back to dual license Apache2.0/GPLv2.0:
  - Today inbound license is Apache-2.0 AND GPL-2.0-or-later and outbound license is Apache2.0
  - Reverting outbound license to Apache-2.0 OR GPL-2.0-or-later as it was back in 2018
  - Discussed in TF TSC in May 2023 and in TF board in 2022.
  - Allows GPL-2.0 licensed projects such as uboot to integrate Mbed TLS.
  - Apache2.0 licensed projects can continue to take Mbed TLS under Apache2.0 license

Marketing/Website updates

- Discord server for TF available: See https://www.trustedfirmware.org/faq/ for instructions.
- Website
  - Trusted Services 1.1.1 release blog posted
  - Started efforts to migrate off current wiki, CoC moved
  - Updated Charter and Membership Agreement
  - Nearing completion of MISRA white paper w/ Bugseng
- Feedback from OSFC



AOB (Any Other Business)

Next Board Meeting

Nov 15 @ 17:00 BST/UTC+1

09:00 Pacific (San Jose)

Thank You

www.TrustedFirmware.org
enquiries@TrustedFirmware.org

Linaro

Resolved Tickets - Last 30 Days

T	Key ↑	Summary	Status	Assignee	Reporter	Resolution	Resolved
	TFC-210	TF-M CI: Fail to clone repos to Share Folder in new created job	RESOLVED	Paul Sokolovskyy	Xinyu Zhang	Fixed	13/Oct/23
	TFC-247	Mirror TF-M, TF-A, TS projects into GitHub	RESOLVED	Arthur She	Anton Komlev	Done	03/Oct/23
	TFC-358	TF-A: Add Corsola Chromebook platform to Open CI	RESOLVED	Arthur She	Don Harbin	Done	16/Oct/23
	TFC-420	LAVA/SQUAD Access Request	RESOLVED	Benjamin Copeland	Joanna Farley	Delivered	12/Apr/23
	TFC-428	Github Auth request for access to LAVA	RESOLVED	Antonio Terceiro	Joanna Farley	Done	16/Oct/23
	TFC-449	TF-A: Make number of LAVA retries configurable as a Jenkins job parameter	RESOLVED	Paul Sokolovskyy	Paul Sokolovskyy	Done	04/Oct/23
	TFC-488	TF-A CI / tf-l3-code-coverage tests random failures	RESOLVED	Paul Sokolovskyy	Olivier Deprez	Fixed	05/Oct/23
	TFC-492	Create Windows AMI with missing TF-A dependencies	RESOLVED	Arthur She	Harrison Mutai	Fixed	27/Sep/23
	TFC-493	TF-A CI: Support for staging area or similar environment for testing during toolchain-upgrade	RESOLVED	Paul Sokolovskyy	Jayanth Dodderi Chidanand	Done	05/Oct/23
	TFC-498	Pre-release (2023-10) load testing cover epic to track any issues needing addressing	RESOLVED	Paul Sokolovskyy	Joanna Farley	Done	09/Oct/23
	TFC-499	2023-09-15 Joanna's testing	RESOLVED	*Unassigned*	Paul Sokolovskyy	Done	09/Oct/23
	TFC-500	2023-10-02 Joanna's testing	RESOLVED	*Unassigned*	Paul Sokolovskyy	Done	09/Oct/23
	TFC-502	2023-10-04 LAVA FVP bottleneck	RESOLVED	Paul Sokolovskyy	Paul Sokolovskyy	Done	07/Oct/23
	TFC-505	Decrease LAVA timeouts/number of LAVA resubmission retries	RESOLVED	Paul Sokolovskyy	Paul Sokolovskyy	Done	09/Oct/23
	TFC-506	Increase number of FVP workers	RESOLVED	*Unassigned*	Paul Sokolovskyy	Done	09/Oct/23
	TFC-507	2023-10-06 Joanna's testing	RESOLVED	*Unassigned*	Paul Sokolovskyy	Done	09/Oct/23
	TFC-508	Prepare for load testing a TF-A patch leading to high rate of tests with timeouts	RESOLVED	Paul Sokolovskyy	Paul Sokolovskyy	Done	09/Oct/23
	TFC-509	2023-10-07 Paul's testing	RESOLVED	Paul Sokolovskyy	Paul Sokolovskyy	Done	09/Oct/23
	TFC-512	TF-M CC Job: Find a more proper time to run the job	RESOLVED	Paul Sokolovskyy	Xinyu Zhang	Done	13/Oct/23
	TFC-514	TFC-198 / Install ArmClang 6.18 in TF-A docker image(s)	RESOLVED	Paul Sokolovskyy	Paul Sokolovskyy	Done	12/Oct/23

1–20 of **20**

Mbed TLS License (TF Board Slide Mar'22)

- **Background**: Dev releases and latest LTS available only under Apache-2.0 and not dual license (Apache-2.0 or GPL-2.0-or-later).
  - GPL-2.0 licensed projects (e.g., Open VPN) unable to integrate Mbed TLS releases anymore
  - Under Arm governance, GPLv2 was dropped in dev. branch releases following concerns from partners
  - New LTS release made recently also licensed under Apache-2.0 only
- **Question**: Does the project need to go back to dual license or stick with Apache-2.0 only?