



Open Source Secure World Software

# Trusted Firmware Governing Board Meeting

15 March 2023

HOSTED BY:



# Agenda

- Membership updates
- Action Item Review
- MCUboot transition to TF.org
- Financial updates
- Open CI Updates
- General Topics
  - Charter Update/Review
  - LTS Messaging status
  - Marketing Update
  - AOB

[board@lists.trustedfirmware.org](mailto:board@lists.trustedfirmware.org)

## Our Members

### Diamond Members

arm

Google

### Platinum Members

Linaro

NXP

RENESAS

ST  
life.augmented

### General Members

FUTUREWEI  
Technologies

NXM

## TF-M Technical Overview



Joseph Yiu | Monday, February 27, 2023 | 1 min read

White Paper: Trusted Firmware-M (TF-M) Technical Overview

## Trusted Firmware-A LTS v2.8.0 released!



Matteo Carlini | Monday, February 13, 2023 | 1 min read

# Membership Updates

- **Inquiries:**
  - No updates
- Infineon decided to not renew membership
- Nordic will join as General member

# Action Item Review

## Feb 15, 2023 Board Meeting Actions

- David Brown confirm w/ Dominic (Nordic) that he is OK with this transition.  
**Mar 6:** Dominic is OK as long as the rest of Nordic is. **Closed**
- Shebu talk to Nordic on the agree discount transition proposal  
Nordic has chosen to join as General member. **Closed**
- Don raise vote to accept MCUboot project as a [trustedfirmware.org](https://trustedfirmware.org) project.  
Vote raised and passed. **Closed**
- Don raise vote on known required infrastructure cost increases  
Vote raised and passed. **Closed**
- Eric Finco send email w/ comments re: latest Charter update draft.  
Received inputs and Don incorporated changes into the latest Charter and circulated for review March 7th. To be reviewed during today's board meeting. **Closed**

# MCUboot transition to TrustedFirmware.org

- Board has voted to transition project under trustedfirmware.org
- TrustedFirmware will receive \$30k of MCUboot project fund
- Don will create a project mini website for MCUboot in coming weeks similar to other Trusted Firmware project websites
- The [MCUboot documentation](#) will also be hosted under trustedfirmware.org
- Source code repository [in github](#) will remain unchanged
- Arranging mcuboot project update in TSC meeting

# Financial Updates



# Open CI Updates



# Open CI Updates

## Progress - February

- Upgraded LAVA Master to the cloud
- Continued progress of performance issues in Mbed TLS CI (TFC-260)
  - IO limitations and job delays are still an issue despite increasing EC2 size and throughput configurations. Continuing to Investigate.
- Progress with TF-A team for LTS build and testing
- MISRA TF-A deployed acquiring feedback from team for improvements. TF-M currently in proto-type.
- Boards
  - Chromebooks Lazor & Asurada deployed to Lab and Running tests
  - STM32mp15 deployed, working with ST to deploy testing
  - STM32U5 enabled in LAVA, awaiting deployment to Lab
  - Chromebook - Tomato enabled in LAVA; awaiting deployment to Lab

## Active Issues:

- Active Hardware Issues
  - None
- Active Infrastructure Issues
  - See TFC-260 above(MBed TLS)

# Open CI Priorities

## Identified Priorities for FY'23 (Can tweak/add based on Trusted Firmware Board feedback)

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

## Priorities - over the next month

- Upgrade Jenkins Master; UBS Licensing Support
- TF-A LTS Support
- Resolve Mbed TLS Performance issues
- Continue MISRA integration into TF-M
- Enable testing for STM32MP15
- Deploy STM32U5 and Chromebook Tomato to the Lab

**Reminders:** [Current deployed devices](#), [Job test results](#), [EPIC: Trusted Firmware Community Board Enablement](#)

# Open CI Platform Prioritized Backlog

## Current Open CI Platform Enablement Queue:

1. Add Renesas EK-RA6M4 - On hold
2. Add STM32MP15 - Deployed, passing boot tests
3. Chromebook LAVA tests - Tests running on Asurada, Lazor - Completed
4. Add STM32U5 - In Progress; awaiting Lab deployment
5. Add Tomato Chromebook - In Progress; awaiting Lab deployment
6. Add Corsola Chromebook - Backlog
7. Add N1SDP Arm platform - Backlog
8. Google next Chromebook - Holder for FY 23
9. ST next platform - Holder for FY 23

**Charter draft second update circulating to clarify platform additions per year**

Member	Platform	FY '21	FY '22	FY '23
Renesas	<a href="#">EK-RA6M4</a>	1/1		
ST	<a href="#">STM32MP15</a>		1/2	
ST	<a href="#">STM32U5</a>		2/2	
Google	<a href="#">Chromebook Tomato</a>		1/2	
Google	<a href="#">Chromebook Corsola</a>		2/2	
Arm	<a href="#">N1SDP</a>			1/2
Google next	<a href="#">Chromebook next</a>			1/2
ST next	<a href="#">STM32xx</a>			1/1

Platform Quota usage per members

# Resolved Tickets - Last 30 Days

T	Key ↑	Summary	Status	Assignee	Reporter	Resolution
	TFC-338	TF-M CI: stm32i562e-dk-03 wrongly skips BL2 test	RESOLVED	Maria Högberg	Xinyu Zhang	Delivered
	TFC-396	TF-A CI Appears broken again with load issues	RESOLVED	Paul Sokolovskyy	Joanna Farley	Done
	TFC-400	TF-A: Codecov jobs fail with "genhtml: ERROR: no valid records found in tracefile coverage.info"	RESOLVED	Paul Sokolovskyy	Paul Sokolovskyy	Done
	TFC-401	Adding the tf-a-eclair-delta job to AllowCI+2	RESOLVED	Paul Sokolovskyy	Joanna Farley	Done
	TFC-408	TF-M CI: Clean outdated document artifacts	RESOLVED	Paul Sokolovskyy	Xinyu Zhang	Done
	TFC-410	tf.validation: fvp devices: Different behavior on tf-master.tflab vs tf-fvp-remote01 workers	RESOLVED	Paul Sokolovskyy	Paul Sokolovskyy	Done
	TFC-418	Chromebook Board Boot Tests in TF-A OpenCI seem broken	RESOLVED	Arthur She	Joanna Farley	Done
	TFC-419	JIRA access request	RESOLVED	Glen Valante	Joanna Farley	Delivered

1-8 of 8 

# General Topics



# Charter update/review

- Primary goal: To tighten up the wording around when and how many platforms a member can add to the Open CI lab per Fiscal Year.
  - Red-lined copy circulated for Jan Board Meeting
  - Feb: Incorporated Jan Board meeting comments (Active Membership Clause) and circulated markup
  - March: Incorporated latest comments from Eric
- Comments?

# LTS Messaging Status

- November (end) '22
  - ~~TF-Av2.8 release blogpost~~
- December '22 (shortly after TF-Av2.8)
  - ~~Blogpost announcing LTS branch, name & mailing list. [Here](#)~~
  - ~~Social media publishing (LinkedIn/Twitter)~~
  - ~~Tech Forum Topic~~ → **planned for 26th Jan**
- ~~LTS v2.8.0 launched on Feb 14th~~ (see mailing list [announcement](#))
- February '23
  - ~~Follow up blogpost based~~
  - ~~Social media publishing (LinkedIn/Twitter)~~
- Springtime '23:
  - Follow up Tech Forum

# Marketing update

- OSFC Fall '23
  - October 10-12, Kirkland, Washington (Seattle)
  - Bronze Sponsorship Package: 2,000 €
  - 1 Complimentary Registration, Social Media recognition, Newsletter recognition, Logo on website
- Website updated to support TF-A LTS

# AOB (Any Other Business)

- TF-M Technical Overview for S/W Developers found [here](#)
- Shared TF slack channel eval ends tomorrow, no funding planned to extend
  - Transition to Discord?
- [Linaro Connect](#) is April 26-28 in London.
  - Suggestion for combined Board and TSC meeting with available reps.
  - Trusted Firmware project update session submitted by Matteo and Shebu

## Next Board Meeting

April 12th(?) @ 17:00 BST/UTC+1  
09:00 Pacific (San Jose)



# Thank You

Lkbjj

Visit [www.TrustedFirmware.org](http://www.TrustedFirmware.org) or email [enquiries@TrustedFirmware.org](mailto:enquiries@TrustedFirmware.org) for more information





# Backup

# LTS Initial Proposal Reminder

Get commit from primaries to build out an initial TF-A LTS branch (as per Tech proposal)

- Initial support from Google, NVidia, Arm (...others?)
- Evaluation period of 6 months to 1 year. Gather metrics on costs
- Follow below roadmap focused on maximizing visibility leading to investment/support from product developers/other SoC providers

Proposed Roadmap/Strategy:

- Google/NVidia/Arm/others commit to provide resource support (LTS maintainers, etc.)
- Leverage Open CI infrastructure for initial LTS. Expect minimal cost.
- Start+6 months, post initial release
  - Create TF-LTS mail list to allow interested parties to subscribe and keep up with updates
  - Advertise release in a TF Blog and TF-A mail list
  - Capture costs (staffing & infrastructure) for 6 month evaluation period
- After 6 month evaluation period
  - Based on TF-LTS mail list and other methods to track the user base, create a benefits proposal to encourage external users to fund releases beyond the evaluation period
  - Approach user base to garner support. Leverage the existing General TF membership tier focused on funding the effort
  - If funding support attained, continue w/ future releases, else end support. Funding options (depending upon support costs):
    - Continued (possibly limited) support from existing and any newly identified contributors
    - Budgeted into existing TF
    - Required additional General members to support