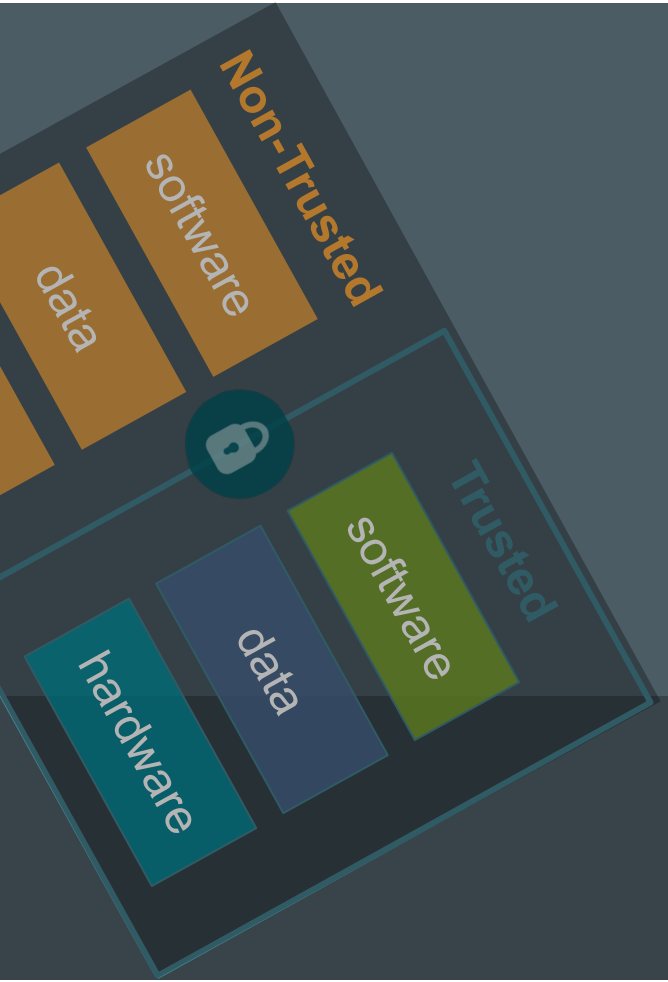


Open Source Secure World Software

Trusted Firmware Governing Board Meeting

12 July, 2023

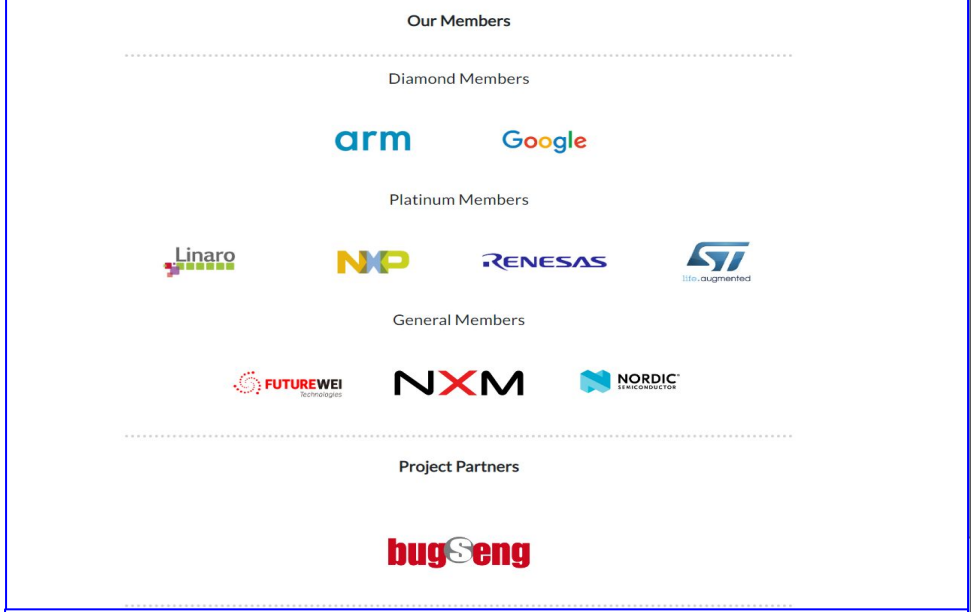
HOSTED BY:

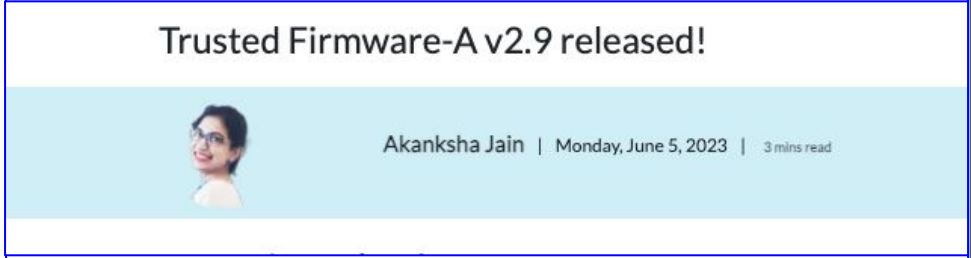
Linaro

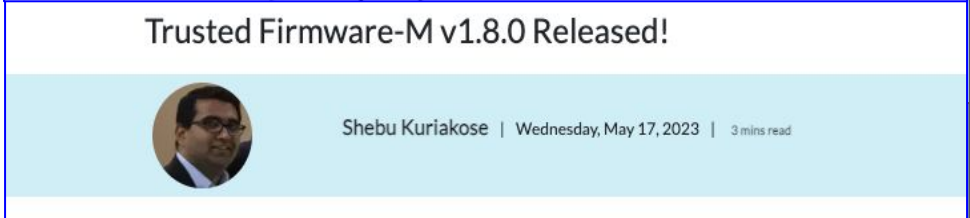
Agenda

- Membership updates
- Action Item Review
- ~~Financial updates~~
- Open CI Updates
- General Topics
  - Marketing Update
  - AOB

board@lists.trustedfirmware.org







Membership Updates

- Inquiries:
  - Meta:
    - **Stage**: Initial discussions
    - Don provided overview of TF-A and OP-TEE. Met and shared content. Particular interest in TAs.
    - Next step: Awaiting their feedback after internal review of info I shared
  - Xilinx/AMD:
    - **Stage**: Initial discussions
    - Matteo has started a thread.
    - Next step: Provide updates as hear back
  - Analog Devices:
    - **Stage**: Initial discussions
    - Next step: Follow up in September
  - Marvell:
    - **Stage**: Initial discussions.
    - Secure Firmware development on A & M Class Arm processors

Stage:
- Initial discussions
- Educating decision makers
- Initial Agreement drafted
- Agreement signed

Action Item Review

- No Opens

Open CI Updates

Open CI Updates

Progress - June

- Migrated MbedTLS to Prod - now monitoring performance
- Upgraded disk space for Jenkins master
- MISRA TF-A / TF-M code refactoring
- Prepping for MISRA TSC presentation
- Boards
  - N1SDP deployed in lab; working to deploy testing
  - Chromebook - Corsola - in progress
- Added Device descriptions based on Board feedback. Example here

Active Issues:

- Active Hardware Issues
  - None
- Active Infrastructure Issues
  - TFC-456 TF Support for FVP jobs in the cloud
    - FVPs currently run on Jenkins master. This creates heavy loads during releases. This ticket is to solve the issue by moving the FVPs to a cloud instance.
  - TFC-454 Migrate mbedtls jobs from the staging to the production
    - Seeing some timeouts on Windows Build tests. Investigating

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
- Add IAR compiler support for TF-M and Mbed TLS
- Verify Disaster Recovery process, procedures, docs
- Trusted Services CI
- TF-A Windows Build

Priorities - over the next month

- Complete the enablement for N1SDP, Work on Chromebook Corsola
- Work with TF-M team for MISRA integration/feedback
- Enable UBS Licensing Support
- Enable FVP jobs in the cloud

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 STM32MP15 - Done
3. Add Tomato Chromebook - Done
4. Add N1SDP Arm platform - In progress
5. Add Corsola Chromebook - In progress
6. Google next Chromebook - Holder for FY 23
7. ST next platform - Holder for FY 23

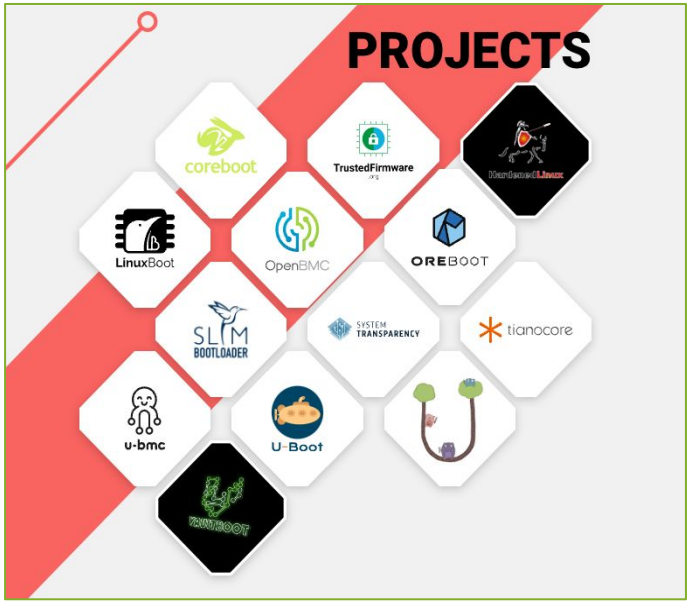
Member	Platform	FY ‘21	FY ‘22	FY ‘23
Renesas	EK-RA6M4	1/1		
ST	STM32MP15		1/2	
ST	STM32U5		2/2	
Google	Chromebook Tomato		1/2	
Google	Chromebook Corsola		2/2	
Arm	N1SDP			1/2
Google next	Chromebook next			1/2
ST next	STM32xx			1/1

Platform Quota usage per members

General Topics

Marketing/Website updates

- Discord server for TF available: See https://www.trustedfirmware.org/faq/ for instructions
- Blogs/News Updates
  - OP-TEE 3.22 Released July 7. Blog to follow
- Reminder: OSFC Fall ‘23
  - Oct 10-12
  - **Moved** to Sunnyvale, CA - Google campus
  - Joakim to let us know if he will attend
  - Bronze Sponsorship Package: 2,000 €
  - 1 Complimentary Registration, Social Media recognition, Newsletter recognition, Logo on website



AOB (Any Other Business)

- Dedicated Discord Server
  - Created with a few invites sent out. Invite link: https://discord.gg/KENVUvRf
  - A channel for each project and a private channel for TSC
  - Next steps?
- TF-M LTS: Waiting for feedback from PSA JSA/Trust CB
- Getting feedback from Mbed TLS users/contributors on going to back dual license Apache2.0/GPLv2.0
- FYI: MISRA / ECLAIR update in TF-A Tech Forum on July 27th
  - Find dial-in details in calendar here: https://www.trustedfirmware.org/meetings/
  - Will be recorded as well.

Next Board Meeting

(?) August 16th @ 17:00 BST/UTC+1

09:00 Pacific (San Jose)

Lkbjj

Thank You

www.TrustedFirmware.org
enquiries@TrustedFirmware.org

Linaro

Resolved Tickets - Last 30 Days

T	Key ↑	Summary	Status	Assignee	Reporter	Resolution	Resolved
	TFC-207	Analyze TODOs for unconverted/disabled expect scripts	RESOLVED	Chris Kay	Paul Sokolovskyy	Done	10/Jul/23
	TFC-224	Add ST STM32MP15 Platform to OpenCI	RESOLVED	Arthur She	Glen Valante	Done	13/Jun/23
	TFC-311	UI: Make the device ID's on Open CI more human readable	RESOLVED	Arthur She	Don Harbin	Done	06/Jul/23
	TFC-357	TF-A: Add Tomato Chromebook platform to Open CI	RESOLVED	Arthur She	Don Harbin	Delivered	13/Jun/23
	TFC-361	Add N1SPD Board to TF Rack for testing	RESOLVED	Arthur She	Joanna Farley	Done	10/Jul/23
	TFC-378	Prototype job to build multiple TF-M configurations	RESOLVED	Paul Sokolovskyy	Paul Sokolovskyy	Done	03/Jul/23
	TFC-379	Prepare ECLAIR docker image for TF-M	RESOLVED	Paul Sokolovskyy	Paul Sokolovskyy	Done	03/Jul/23
	TFC-384	tf-a-main failure: Legitimate test failure in fvp-linux-fvp-tc0-tbb:fvp-linux.tc-fip.tc-tc0-debug config	RESOLVED	Manish Badarkhe	Paul Sokolovskyy	Won't Fix	05/Jul/23
	TFC-391	Update qa-tools to clone the upstream.	RESOLVED	Saul Romero	Joanna Farley	Fixed	06/Jul/23
	TFC-399	TF-M CI: LAVA test getting slower	RESOLVED	Glen Valante	Xinyu Zhang	Delivered	13/Jun/23
	TFC-436	Fix permissions for user RcColes on review.trustedfirmware.org	RESOLVED	Kelley Spoon	Antonio De Angelis	Done	27/Jun/23
	TFC-461	Add new JIRA users to create and view for TFC board	RESOLVED	Glen Valante	Joanna Farley	Done	05/Jul/23
	TFC-462	Update ReadtheDocs config file due to deprication	RESOLVED	Arthur She	Glen Valante	Done	05/Jul/23
	TFC-464	Hafnium ACS jenkins job doesn't show in dashboards	RESOLVED	Paul Sokolovskyy	Olivier Deprez	Fixed	29/Jun/23

1–14 of 14