TrustedFirmware
.org

Trusted Firmware-M Workshop, Lyon

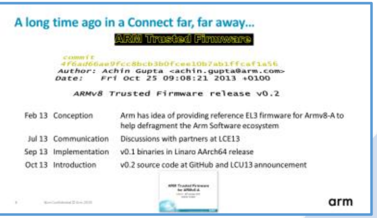
Setting the Scene

- Trustedfirmware.org
- Who All Are Here?
- What Do We Want to Achieve?, What Next?
- TF-M Today, What’s Coming?

Trustedfirmware.org

TrustedFirmware
.org

Trusted Firmware History



A long time ago in a Connect far, far away…

ARM Trusted Firmware

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

    ARMv8 Trusted Firmware release v0.2
```

Feb 13	Conception	Arm has idea of providing reference EL3 firmware for Armv8-A to help defragment the Arm Software ecosystem
Jul 13	Communication	Discussions with partners at LCE13
Sep 13	Implementation	v0.1 binaries in Linaro AArch64 release
Oct 13	Introduction	v0.2 source code at GitHub and LCU13 announcement

arm

Oct 2013

Arm Trusted Firmware

Trusted Firmware M-Class (TF-M) is new!

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

START
Platform Security Architecture
arm

Mar 2018

Trusted Firmware-M

Trusted Firmware-A

Oct 2018

TrustedFirmware.org

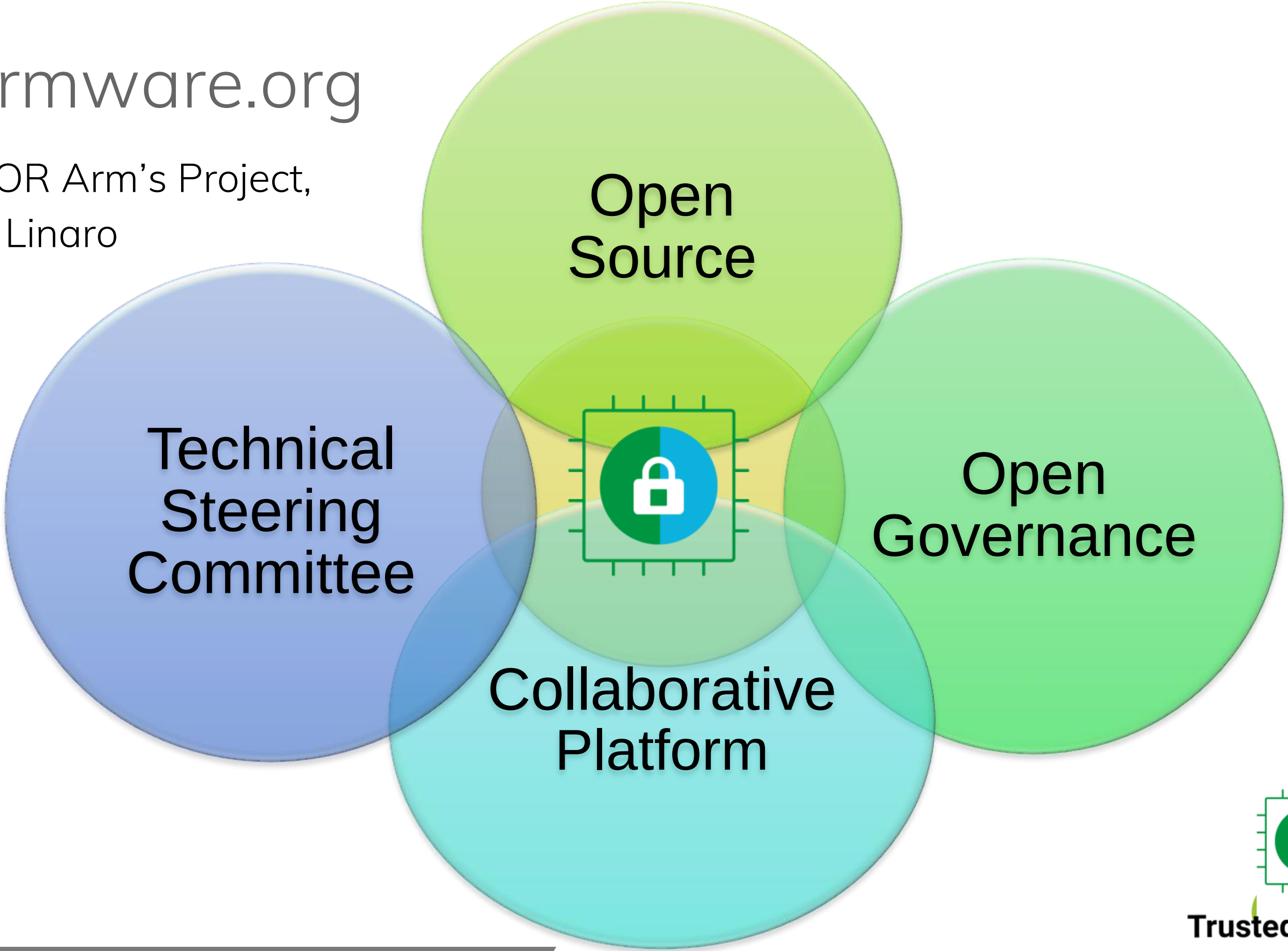
Today

OP-TEE .org

TrustedFirmware .org

Trustedfirmware.org

- NOT Linaro OR Arm’s Project, HOSTED BY Linaro



Open Source

Technical Steering Committee

Open Governance

Collaborative Platform

TrustedFirmware .org

Current members

arm

Data I/O

CYPRESS
EMBEDDED IN TOMORROW™

Linaro

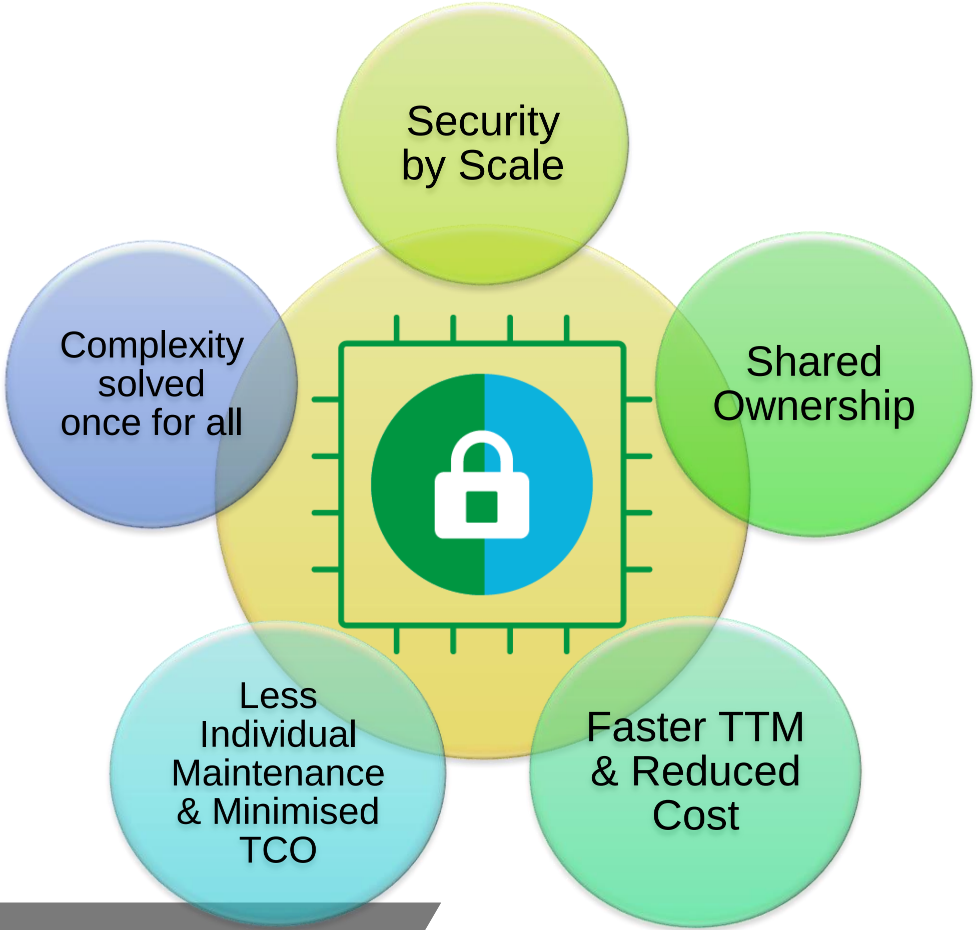
Google

Texas Instruments

ST
life.augmented

TrustedFirmware
.org

Build Security Collaboratively


Security by Scale
Shared Ownership
Faster TTM & Reduced Cost
Less Individual Maintenance & Minimised TCO
Complexity solved once for all

TrustedFirmware
.org

How to Get Involved

- Contribute to the open source codebase!
- Join the project mailing lists!
- ...and last but not the least: **become a project member!** (enquiries@trustedfirmware.org)
    - Own the strategic and technical direction of the project
    - Have your board supported and maintained by the open CI
    - Become a Trusted Firmware ambassador!

Who All Are Here?

arm

TF-M, PSA, CMSIS, mbed

CYPRESS
EMBEDDED IN TOMORROW™

Linaro

NXP

TEXAS INSTRUMENTS

life.augmented

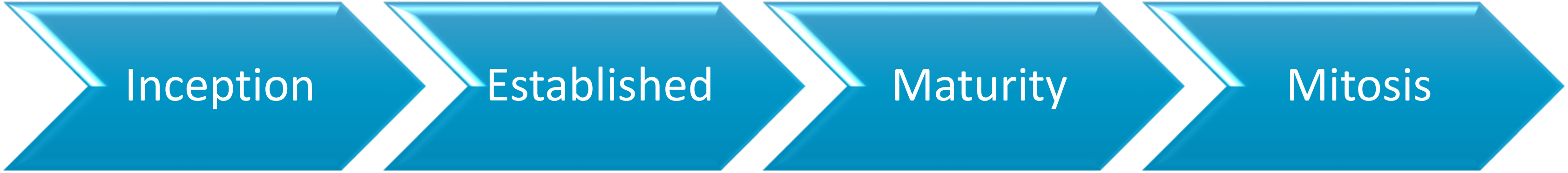
RENESAS

TrustedFirmware
.org

What Do We Want to Achieve?, What Next?

TrustedFirmware
.org

Build TF-M Community…



Inception

- Invite members to join
- Create Discussions
- Relationship building
- Transparency & Openness

Established

- Content
- Hackathons
- Conferences
- Meetups

Maturity

- Growing Influence
- Community Ownership
- Streamlining

Mitosis

- Focussed Subgroups

TrustedFirmware
.org

Workshop & Beyond…

- Each Slot is NOT a ‘death by power point’ by presenters
- 2-3 slides to kick off each topic, followed by Open Discussion
- Active participation by attendees
- Not an opportunity to ask Arm to do more ☺, but to solve problems jointly
- Starting point for more involved mailing list discussions on design/implementation
- Opportunity for
    - Follow up on important topics in a bi-weekly TF-M Technical Forum
    - Making this workshop an annual event

TrustedFirmware
.org

TF-M – Today & Future

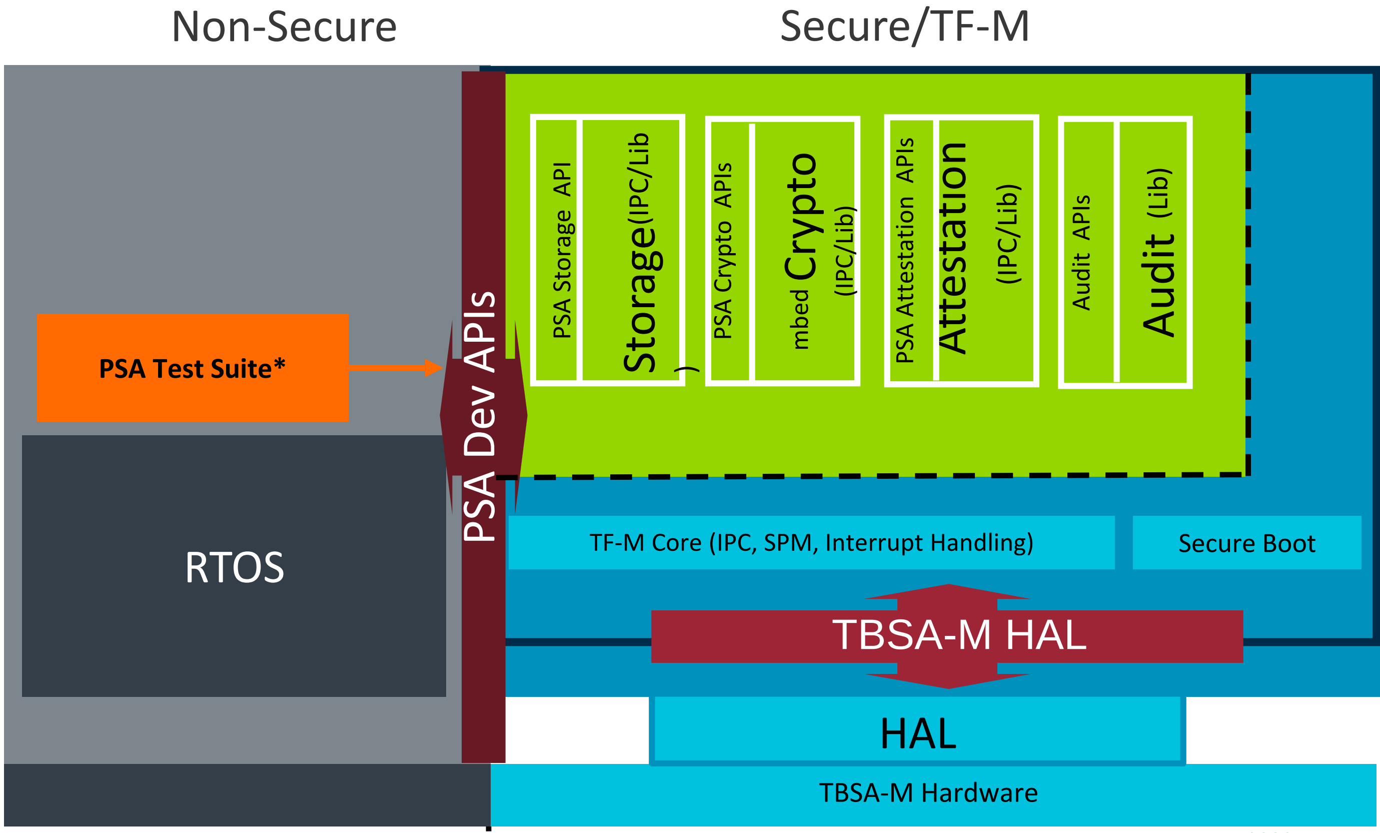
TrustedFirmware
.org

Growing up as a Toddler….

With a Lot of Friends and Toys!!!

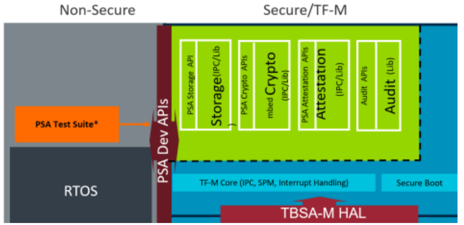
TF-Mv1.0-RC2: Enabling L1,2 and Functional API Certification

- F.INITIALIZATION
- F.FIRMWARE_UPDATE
- F.ISOLATION
- F.SECURE_STORAGE
- F.SECURE_CRYPTO
- F.SECURE_ATTESTATION
- F.SECURE_AUDIT
- F.SECURE_STATE
- PSA Dev. APIs



TrustedFirmware

Enablement in RTOSes



- mbedOS 5.12 (March'19) onwards integrated TF-M
  - PSA Level1 and Functional API certified
  - Several PSA Level1 certified platforms supported

arm MBED

- Zephyr PR integrating TF-M
  - For MuscaA, B1e and AN521 on MPS2
  - PSA L1 certified

Zephyr™

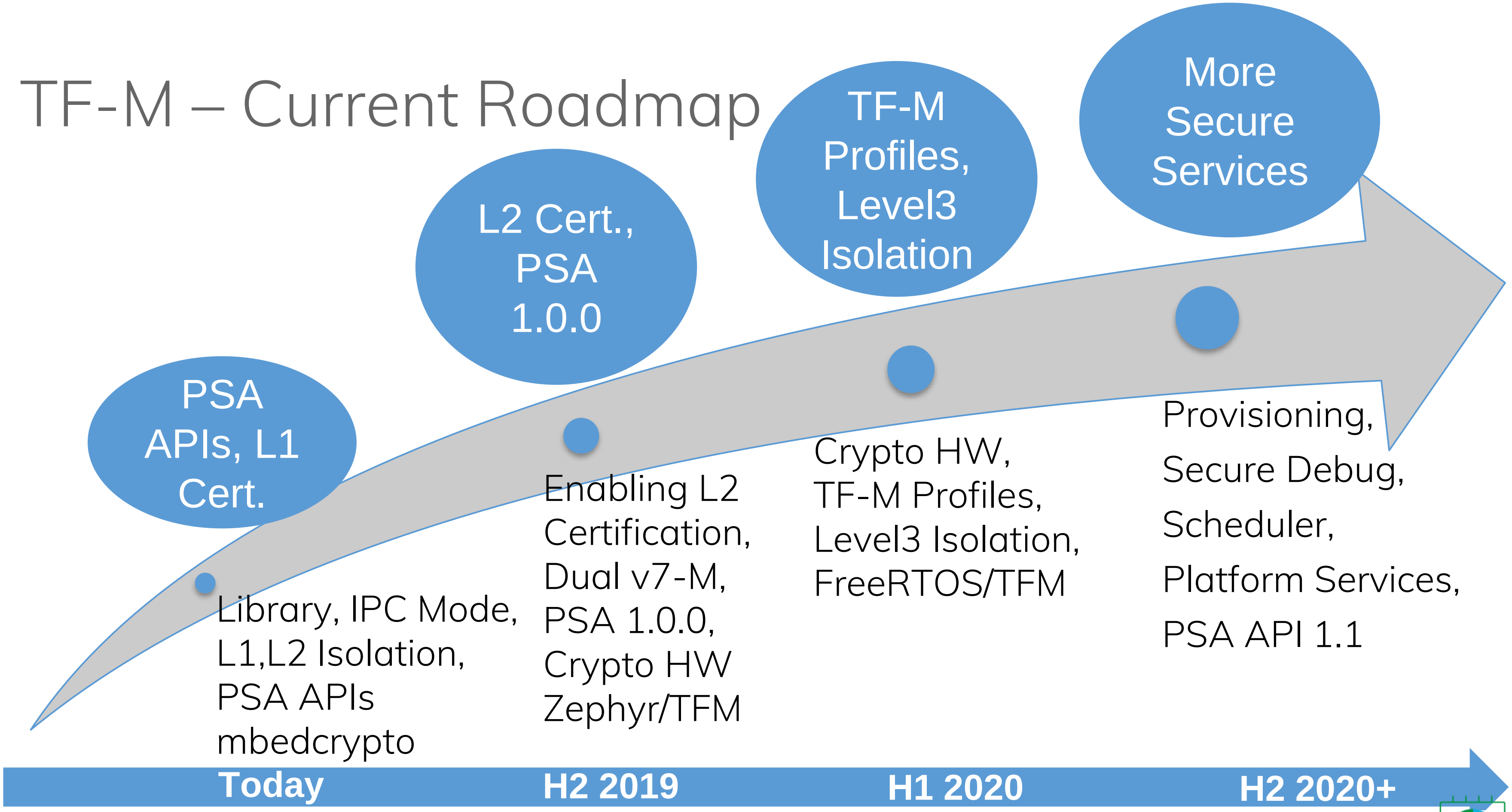
- Integration of FreeRTOS 10.2.1 and TF-M under evaluation by FreeRTOS team
  - Investigating how best TF-M can integrate with Amazon: FreeRTOS

freeRTOS

- Collaboration kicked off with RT-Thread on integration

RT-Thread
小而美的物联网操作系统

TF-M – Current Roadmap



Today

PSA APIs, L1 Cert.

Library, IPC Mode,
L1,L2 Isolation,
PSA APIs
mbedcrypto

H2 2019

L2 Cert., PSA 1.0.0

Enabling L2
Certification,
Dual v7-M,
PSA 1.0.0,
Crypto HW
Zephyr/TFM

H1 2020

TF-M Profiles, Level3 Isolation

Crypto HW,
TF-M Profiles,
Level3 Isolation,
FreeRTOS/TFM

H2 2020+

More Secure Services

Provisioning,
Secure Debug,
Scheduler,
Platform Services,
PSA API 1.1

Workshop & Beyond...

- Each Slot is NOT a ‘death by power point’ by presenters
- 2-3 slides to kick off each topic, followed by Open Discussion
- Active participation by attendees
- Not an opportunity to ask Arm to do more ☺, but to solve problems jointly
- Starting point for more involved mailing list discussions on design/implementation
- Opportunity for
  - Follow up on important topics in a bi-weekly TF-M Technical Forum
  - Making this workshop an annual event

Thank You!

arm

TF-M, PSA, CMSIS, mbed

TEXAS INSTRUMENTS

CYPRESS

EMBEDDED IN TOMORROW™

life.augmented

Linaro

NXP

RENESAS

TrustedFirmware
.org

KeyNote

My Company is a trustedfirmware.org member - A Testimony

- Eric Finco, Technical Director & Fellow, STMicroelectronics & trustedfirmware.org Board member

TrustedFirmware .org

	Oct 31st (Thursday)	Host(s)/Presenter(s)
8.30-9.00am	Registration & Welcome Drinks	
9.00-9.25am	Setting the Scene	Shebu V. Kuriakose
9.25-9.45am	Keynote - Collaborating in trustedfirmware.org	Eric Finco
9.45-10.30am	Scheduler Design Ideas	Ken Liu/Mate Toth-Pal/Summer Qin
10.30-11am	Break	
11.00-12.30pm	Interrupt Handling, What Else in TF-M Core	Ken Liu/Mate Toth-Pal/Summer Qin
12.30-1.30pm	Lunch	
1.30-2.15pm	Secure Storage Service	Jamie Fox/Antonio De Angelis
2.15-3.00pm	mbedcrypto	Jaeden Amero/Janos Follath
3.00-3.45pm	Crypto Hardware Integration	Jamie Fox/Tamas Ban
3.45-4.05pm	Break	
4.05-4.50pm	mcuboot & Attestation Service	Tamas Ban
4.50-5.30pm	Dual CPU Design	David Hu
	Nov 1st (Friday)	
8.30-9.00am	Welcome Drinks	
9.00-9.45am	Build System	David Wang
9.45-10.30am	Tooling Support	Abhishek Pandit/Shebu V. Kuriakose
10.30-11am	Break	
11:00-11.45am	RTOS Enablement	David Wang
11.45-12.30pm	Open CI	Minos Galanakis
12.30-1.30pm	Lunch	
1.30-2.15pm	TF-M Profile Proposal	Shebu V. Kuriakose/Antonio De Angelis
2.15-3.00pm	HAL - Change Proposal	Antonio De Angelis
3.00-3.30pm	Break	
3.30pm-4pm	Wrap Up	Shebu V. Kuriakose

TrustedFirmware
.org