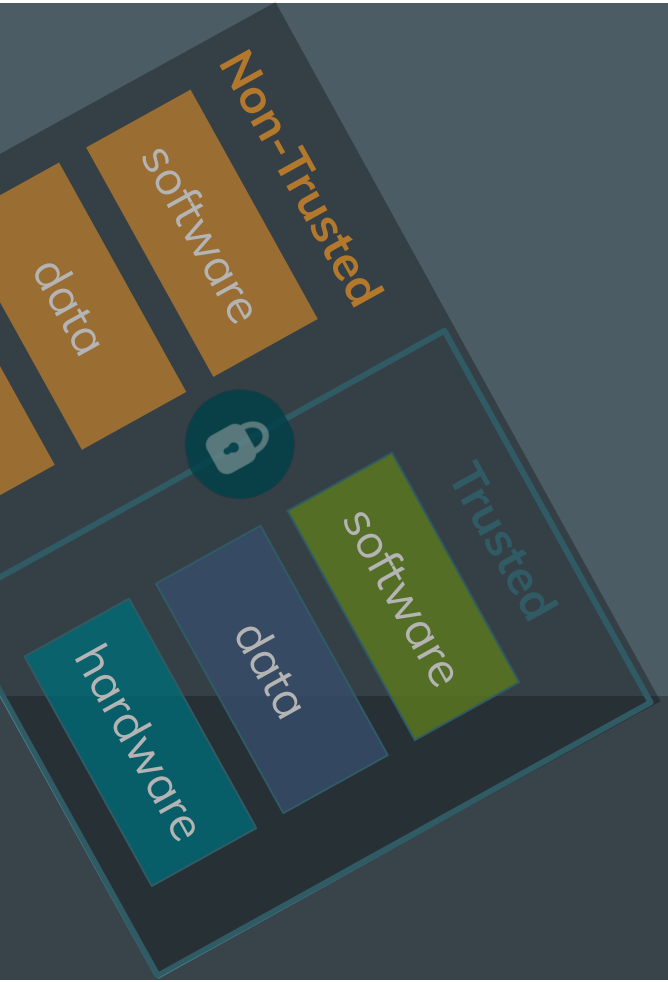


Open Source Secure world software

Trusted Firmware

Update May 2019

SPONSORED BY: arm

HOSTED BY: Linaro

Trusted Firmware

Open governance Community Project since October 2018

Reference implementation of Secure world software for Armv7 & Armv8 architectures (both A/M-Profiles)

Membership of the Trusted Firmware project is open to all

Everyone interested in Trusted Firmware is encouraged to join

Members (May ‘19)

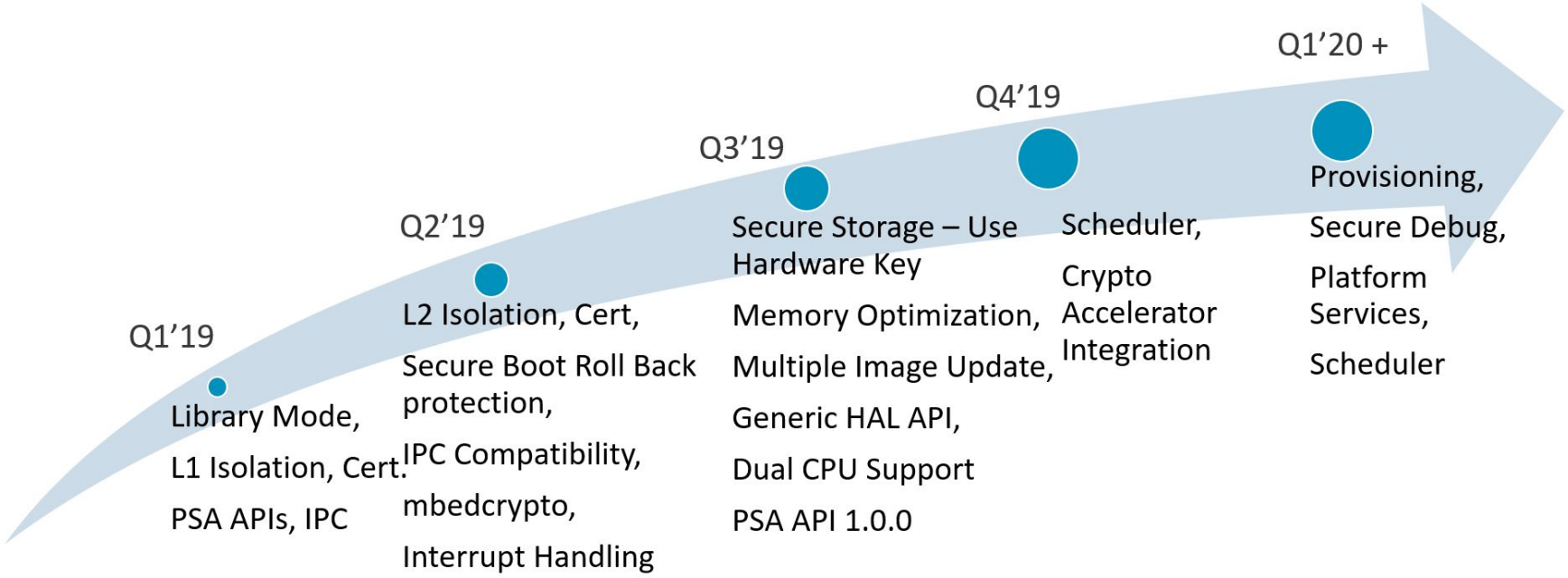
Arm
Cypress
Data I/O
Google
Linaro
Texas Instruments
STMicroelectronics

TrustedFirmware.org

Trusted Firmware-M - May 2019 Progress

- TF-M v1.0-RC1 tag created supporting features required for PSA Level2 certification
- New features in the tag
    * PSA Firmware Framework IPC Support
    * Secure Storage, Crypto and Attestation Services working in IPC mode
    * PSA Level2 Isolation
    * mbedcrypto used in the crypto service.
    * Rollback protection in Secure boot.
- Dual CPU enablement in progress - https://git.trustedfirmware.org/trusted-firmware-m.git/?h=feature-twincpu
- Continuous Integration Testing of TF-M patches using MPS2 board - https://ci.trustedfirmware.org/

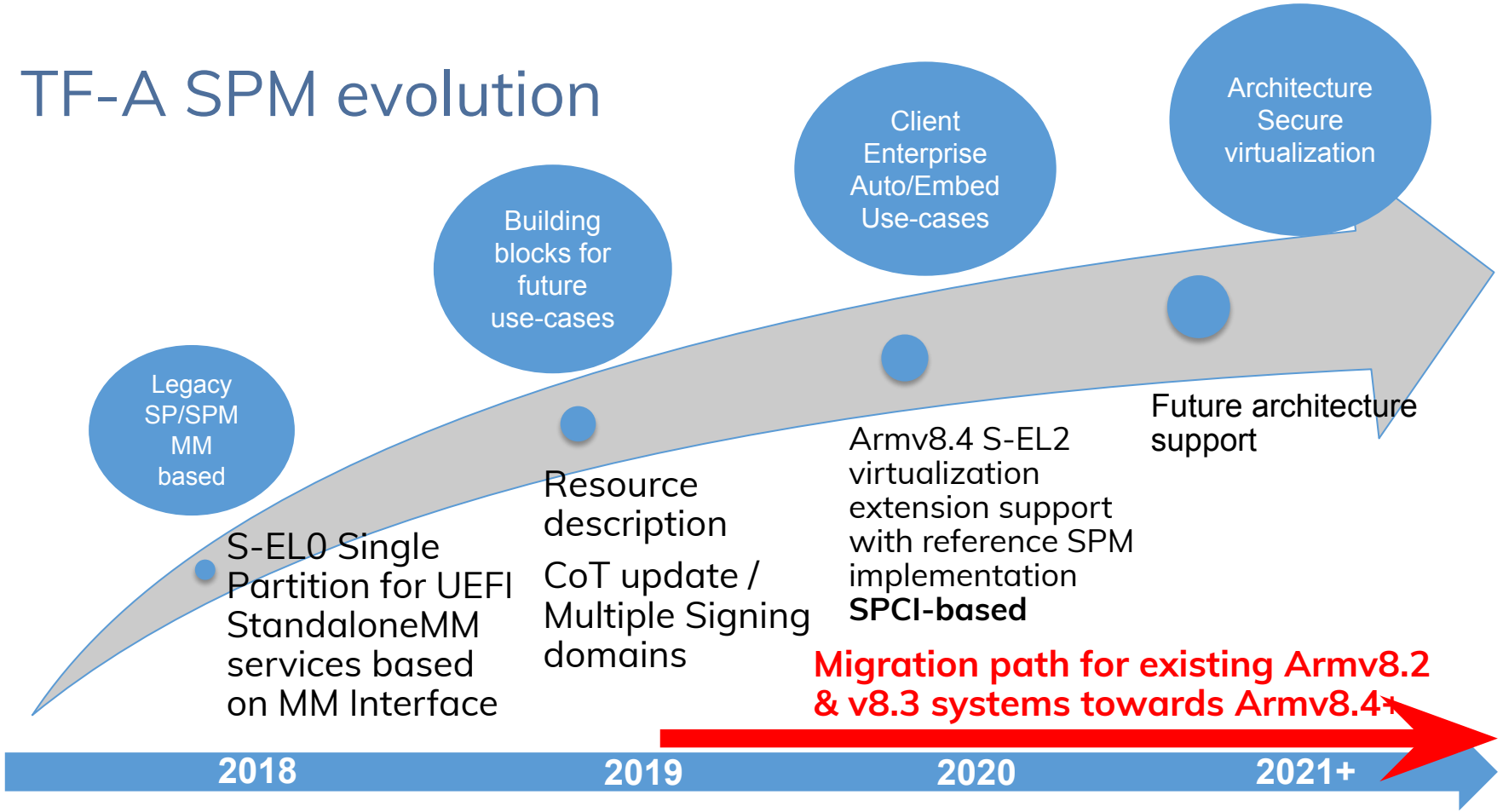
TF-M Roadmap


Q1'19
Library Mode,
L1 Isolation, Cert.
PSA APIs, IPC
Q2'19
L2 Isolation, Cert,
Secure Boot Roll Back protection,
IPC Compatibility,
mbedcrypto,
Interrupt Handling
Q3'19
Secure Storage – Use Hardware Key
Memory Optimization,
Multiple Image Update,
Generic HAL API,
Dual CPU Support
PSA API 1.0.0
Q4'19
Scheduler,
Crypto Accelerator Integration
Q1'20 +
Provisioning,
Secure Debug,
Platform Services,
Scheduler

Trusted Firmware-A – May ’19 Progresses

- Architecture enablement under development
  - Armv8.3 Pointer Authentication use in Secure world (EL3 and lower S-ELs)
  - Armv8.5 Branch Target Identifier (BTI)
  - Armv8.4 Secure EL2 SPM SPCI-based
- Fixed errata for Neoverse-N1 & Cortex-A76
- New platform support: MediaTek mt8183
- Platform Security Requirements under development
  - Attestation and Measured Boot reference flow
  - Multiple Signing Domains and separate Chain of Trust
- Investigations in other areas
  - PSA for IoT A-class devices

TF-A SPM evolution

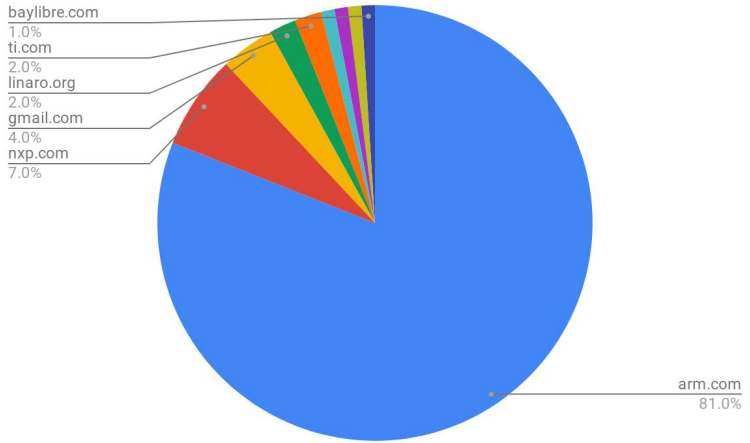


TrustedFirmware TF-A Project Dashboard

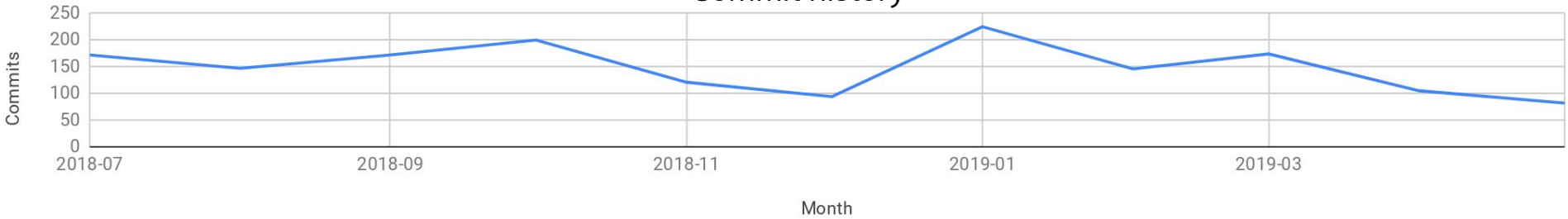
Top Authors this month

paul.beesley	22
soby.mathew	16
john.tsichritzis	13
sandrine.bailleux	12
antonio.ninodiaz	6
leonard.crestez	5
christophm30	4
sami.mujawar	4
alexei.fedorov	4

Commits by domain this month



Commits vs Month

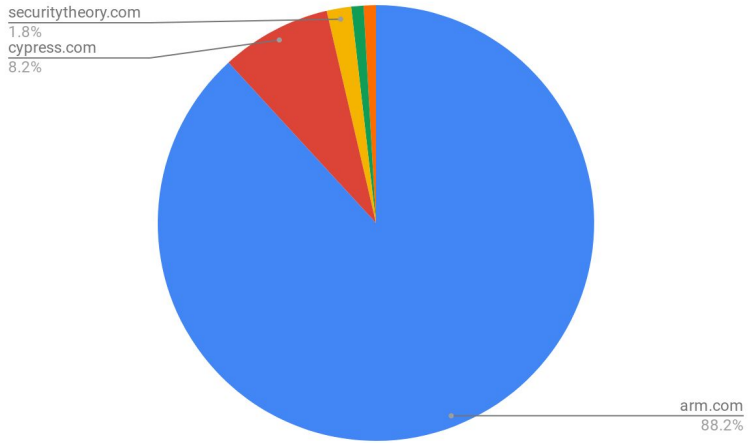


TrustedFirmware TF-M Project Dashboard

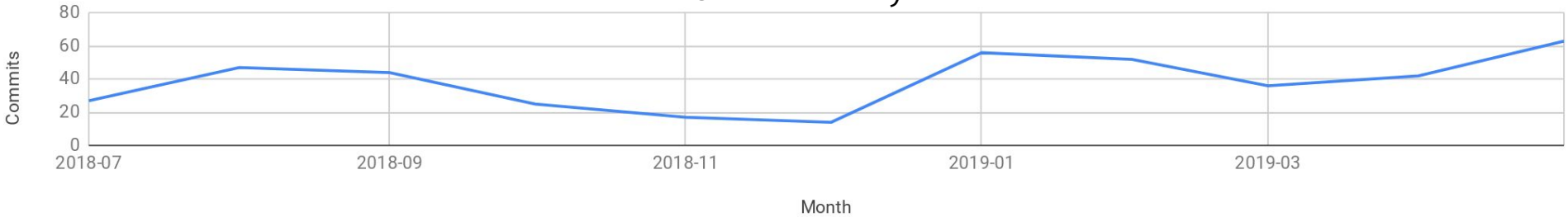
Top Authors this month

edison.ai	14
tamas.ban	14
jamie.fox	13
david.vincze	10
antonio.deangelis	10
chris.brand	9
mingyang.sun	7
summer.qin	7
ashutosh.singh	5

Commits by domain this month



Commits vs Month

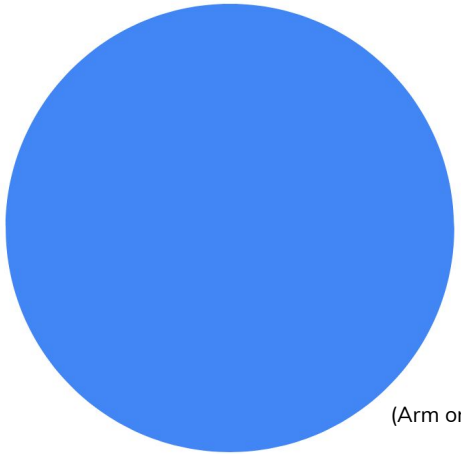


TrustedFirmware TF-A Tests Project Dashboard

Top Authors this month

sandrine.bailleux	6
john.tsichritzis	3

Commits by domain this month



Commit history

arm

Linaro