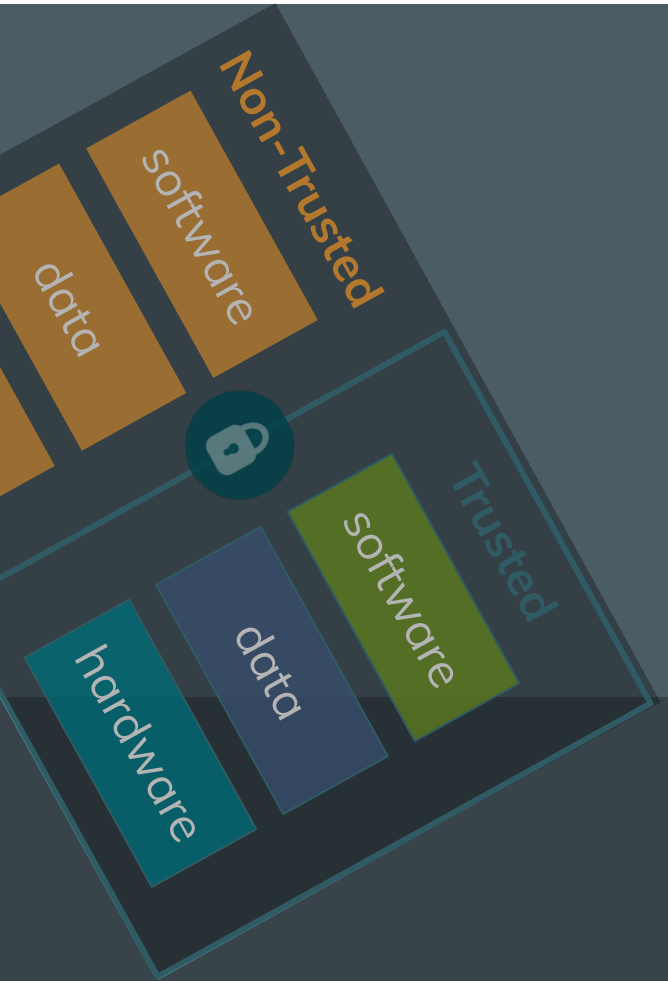


Open Source Secure World Software

Trusted Firmware

Update April 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 (April ‘19)

Arm
Cypress
Data I/O
Google
Huawei
Linaro
Texas Instruments
STMicroelectronics

TrustedFirmware.org

Linaro Connect BKK19

Check out the Project presentation update held at Linaro Connect BKK19 in early April

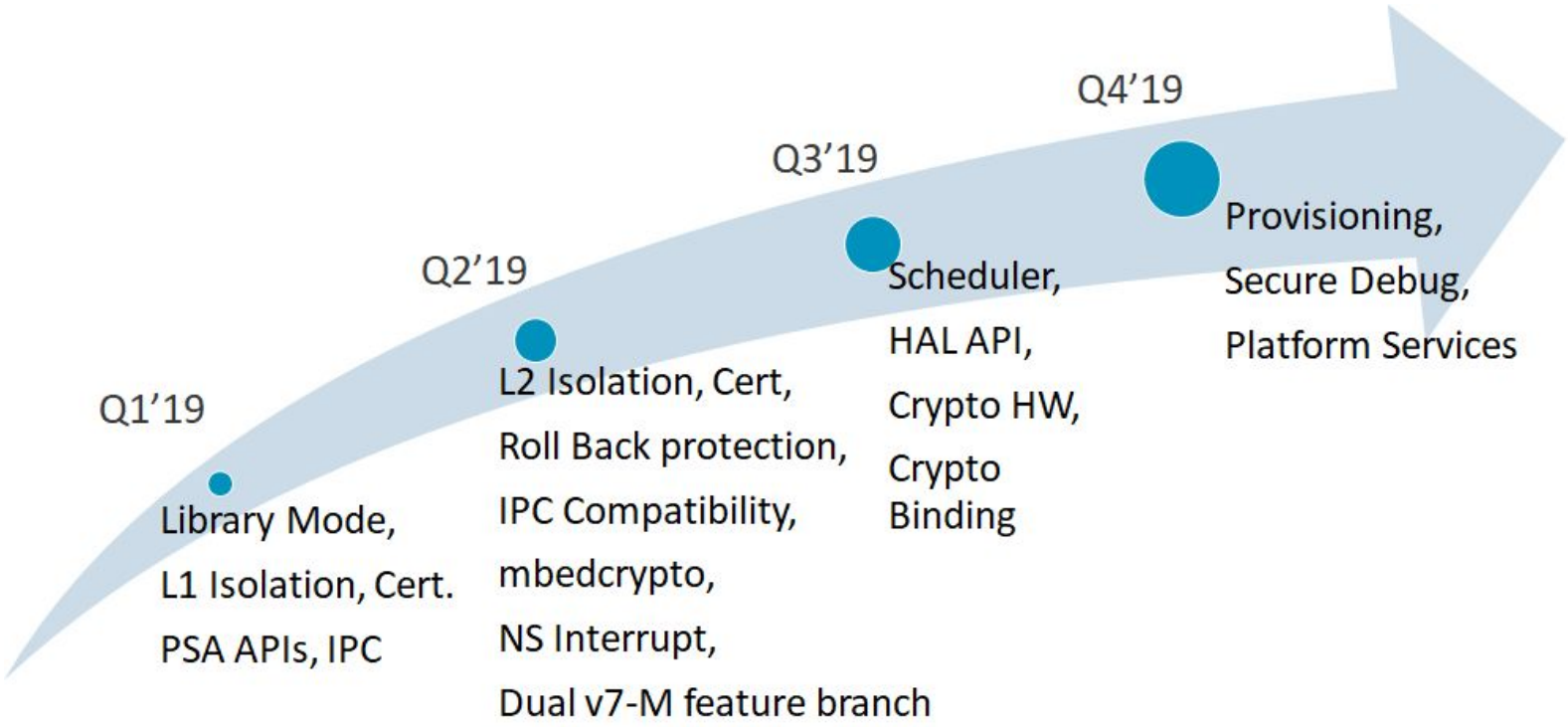
https://connect.linaro.org/resources/bkk19/bkk19-216/

TF-M 1st Birthday Cake!

Trusted Firmware-M - April 2019 Progress

- Celebrated first birthday at Linaro Connect BKK'19
- Initial PSA Level 2 Isolation enabled
- PSA Firmware framework IPC Support for Protected Storage merged, IPC support for Attestation Service under review
- Attestation EAT support completed
- Design proposal for Secure Boot Rollback protection and Non-Secure Interrupt support posted
- Dual CPU enablement in progress
- Open CI Rollout - Jenkins job to create build artifact based on gerrit submissions in place - https://ci.trustedfirmware.org/. Next step is to run the build on MPS2 board

TF-M Roadmap


Q1'19
Library Mode,
L1 Isolation, Cert.
PSA APIs, IPC
Q2'19
L2 Isolation, Cert,
Roll Back protection,
IPC Compatibility,
mbedcrypto,
NS Interrupt,
Dual v7-M feature branch
Q3'19
Scheduler,
HAL API,
Crypto HW,
Crypto
Binding
Q4'19
Provisioning,
Secure Debug,
Platform Services

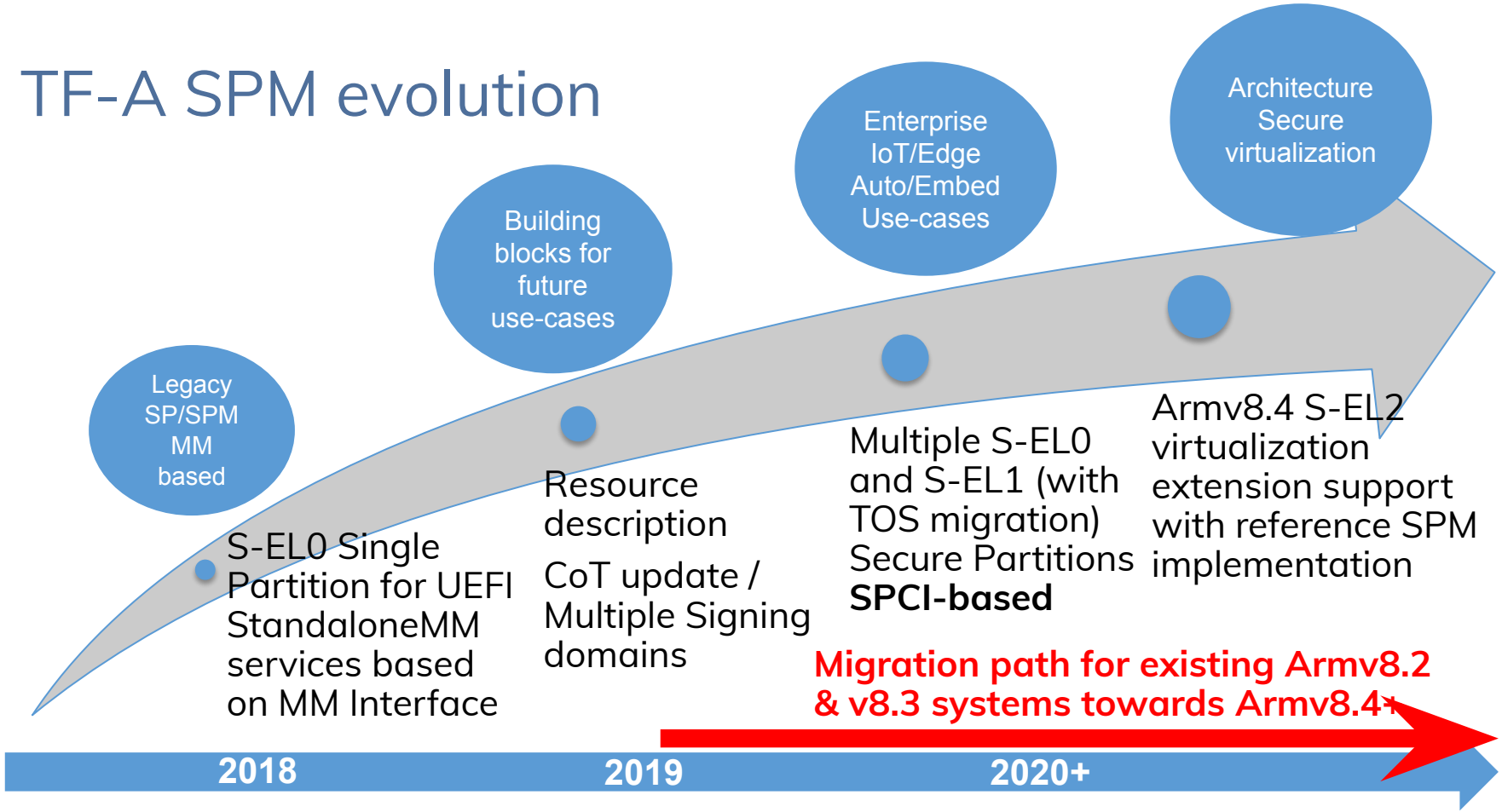
Trusted Firmware-A – April 2019 Progresses

- **v2.1 TF-A & TF-A-Tests release highlights** (read full article)
  - Armv8.3 Pointer Authentication enabled for Normal world
  - Armv8.4 Data Independent Timing and Small Translation Tables support
  - Armv8.5 PSTATE.SSBS Speculation Store Bypass Safe (on Cortex-A76 & Neoverse-N1)
  - New Arm Platforms support
    - Neoverse N1 Edge (RD-N1-Edge) FVP & N1SDP HW Platform
    - Neoverse E1 Edge (RD-E1-Edge) FVP
    - Neoverse Zeus core initial support
  - Dynamic Configuration – Position Independent Executable support for BL31
- **TF-A now fully migrated to new Git/Gerrit infrastructure**:
  - https://git.trustedfirmware.org/TF-A/trusted-firmware-a.git/about/
  - https://review.trustedfirmware.org/

Trusted Firmware-A – What's on

- Architecture enablement
  - Armv8.3 Pointer Authentication use in Secure world (EL3 and lower S-ELs)
  - Armv8.5 Branch Target Identifier (BTI)
- Platform Security Requirements
  - Attestation and Measured Boot reference flow
  - Multiple Signing Domains and separate Chain of Trust
- Investigations in other areas
  - PSA for IoT A-class devices
  - Debug Certificates and Arm Debug IPs support
  - Functional Safety requirements

TF-A SPM evolution

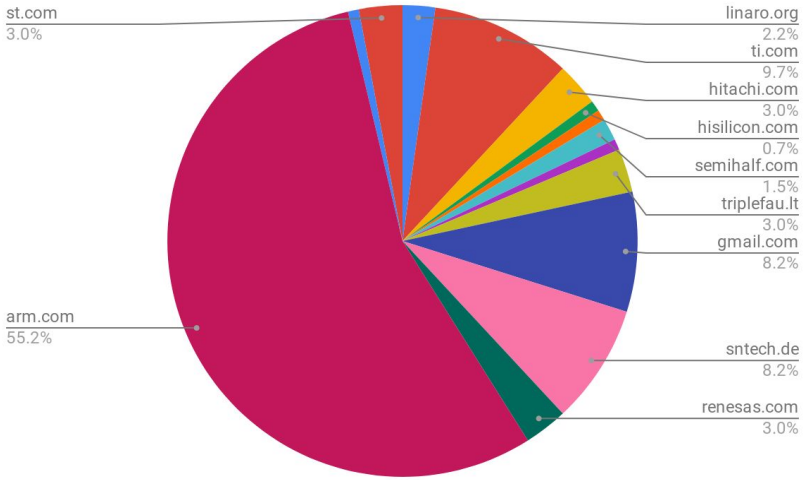


TrustedFirmware TF-A Project Dashboard

Top Authors this month

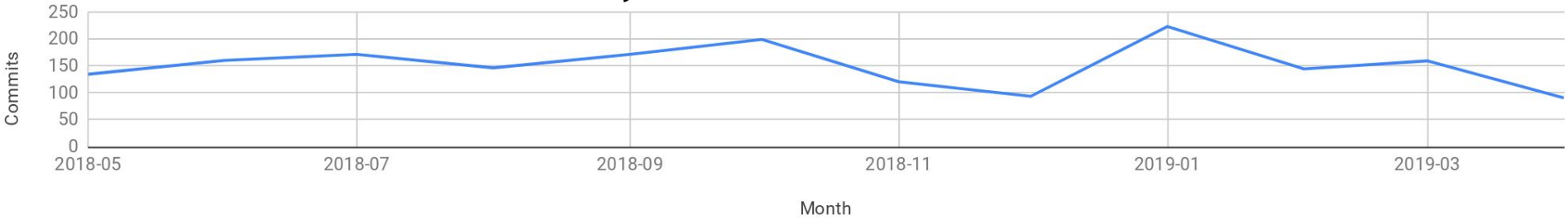
antonio.ninodiaz	33
afd	13
heiko	11
marek.vasut+renesas	9
ambroise.vincent	9
soby.mathew	7
joel.hutton	7
louis.mayencourt	6

Commits by domain this month



Commits vs Month

Commit history

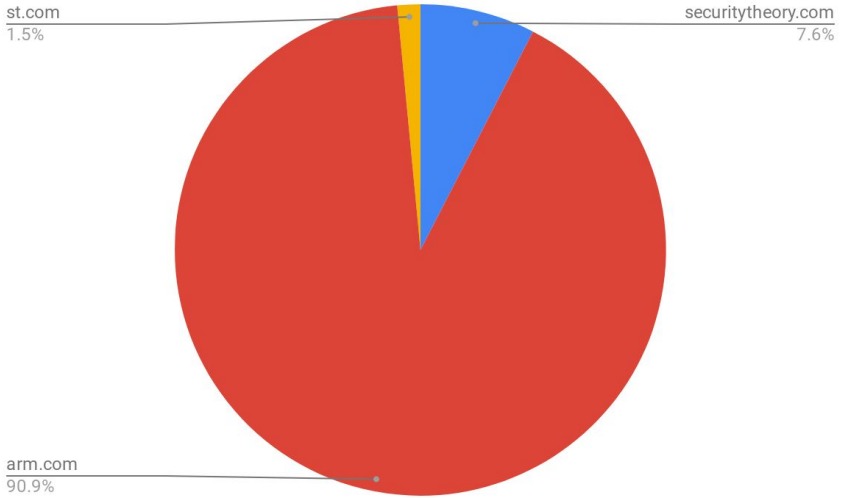


TrustedFirmware TF-M Project Dashboard

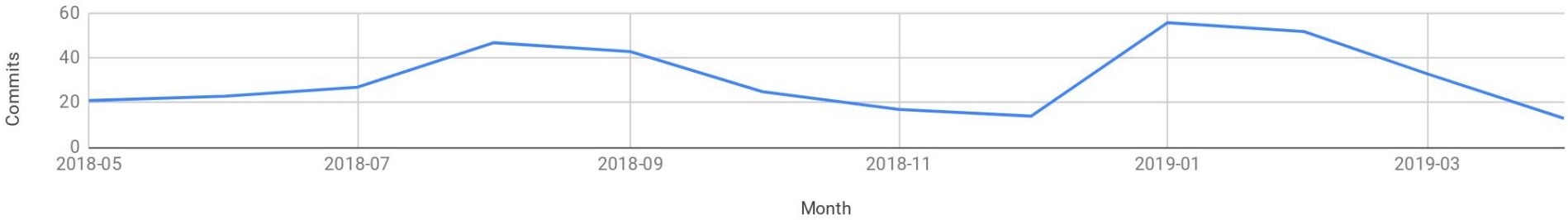
Top Authors this month

edison.ai	19
tamas.ban	7
hugues.devalon	7
ken.liu	6
lgl	5
antonio.deangelis	5
summer.qin	4
jamie.fox	3
kevin.peng	3

Commits by domain this month



Commit history

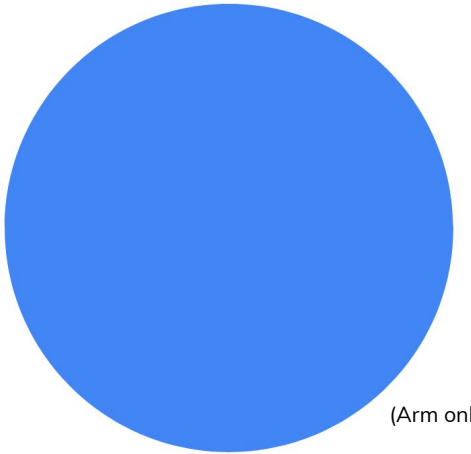


TrustedFirmware TF-A Tests Project Dashboard

Top Authors this month

antonio.ninodiaz	7
joel.hutton	2
sandrine.bailleux	2

Commits by domain this month



Commit history

How to Get Involved

Become a project member

Platinum Board (voting) members define the mission and strategy: $50K/year

General members receive project updates, make requests to the board and may attend monthly calls: $2.5-25K*/year

Maintainers to be appointed from members

* Fee according to company size and type

Contact:

enquiries@TrustedFirmware.org

for more information

TrustedFirmware.org