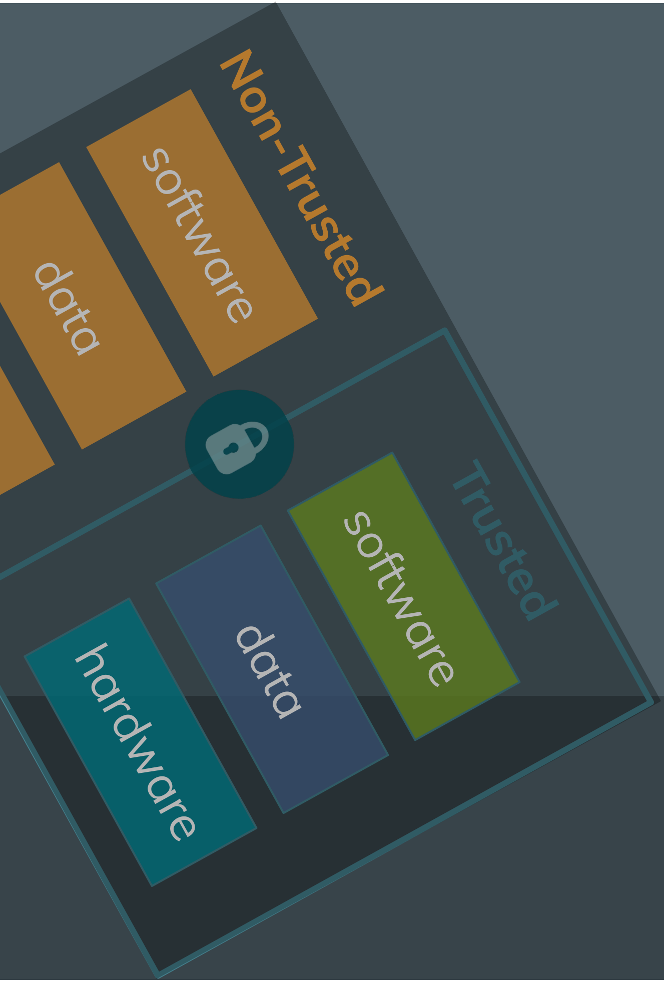


Open Source Secure world software

Trusted Firmware

Update June 2019

SPONSORED BY: arm

HOSTED BY: Linaro

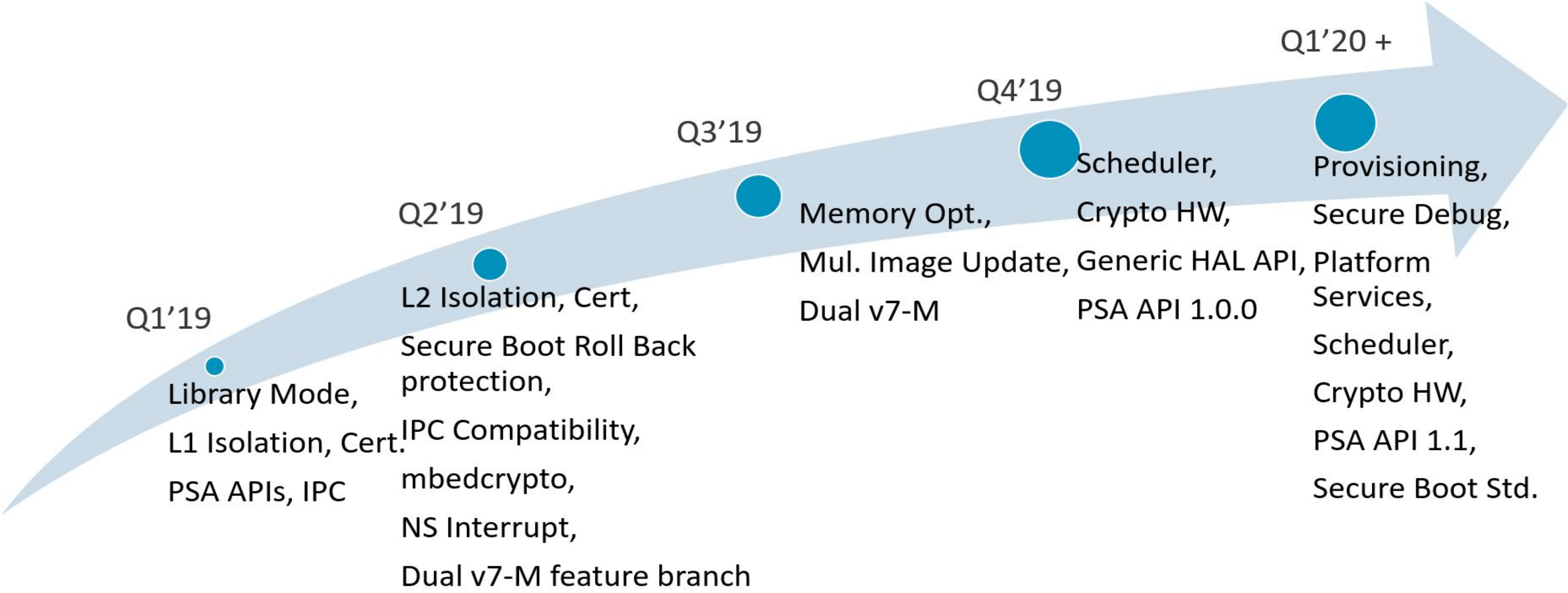
Trusted Firmware-M - June 2019 Progress

- Following TF-M v1.0-RC1 tag created end of May’19 for PSA Level2 certification, following have been merged
  - * SPE Preemption by NSPE
  - * Secure IRQ Support
  - * Updates for mbedcrypto 1.1.0

- Added support for MPS3 AN524 FPGA platform

- Dual CPU support with Level1 Isolation made available in feature-twincpu branch
- Design posted in mailing list for Internal Trusted Storage and HW key usage in secure boot.

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,

NS Interrupt,

Dual v7-M feature branch

Q3’19

Memory Opt.,

Mul. Image Update,

Dual v7-M

Q4’19

Scheduler,

Crypto HW,

Generic HAL API,

PSA API 1.0.0

Q1’20 +

Provisioning,

Secure Debug,

Platform Services,

Scheduler,

Crypto HW,

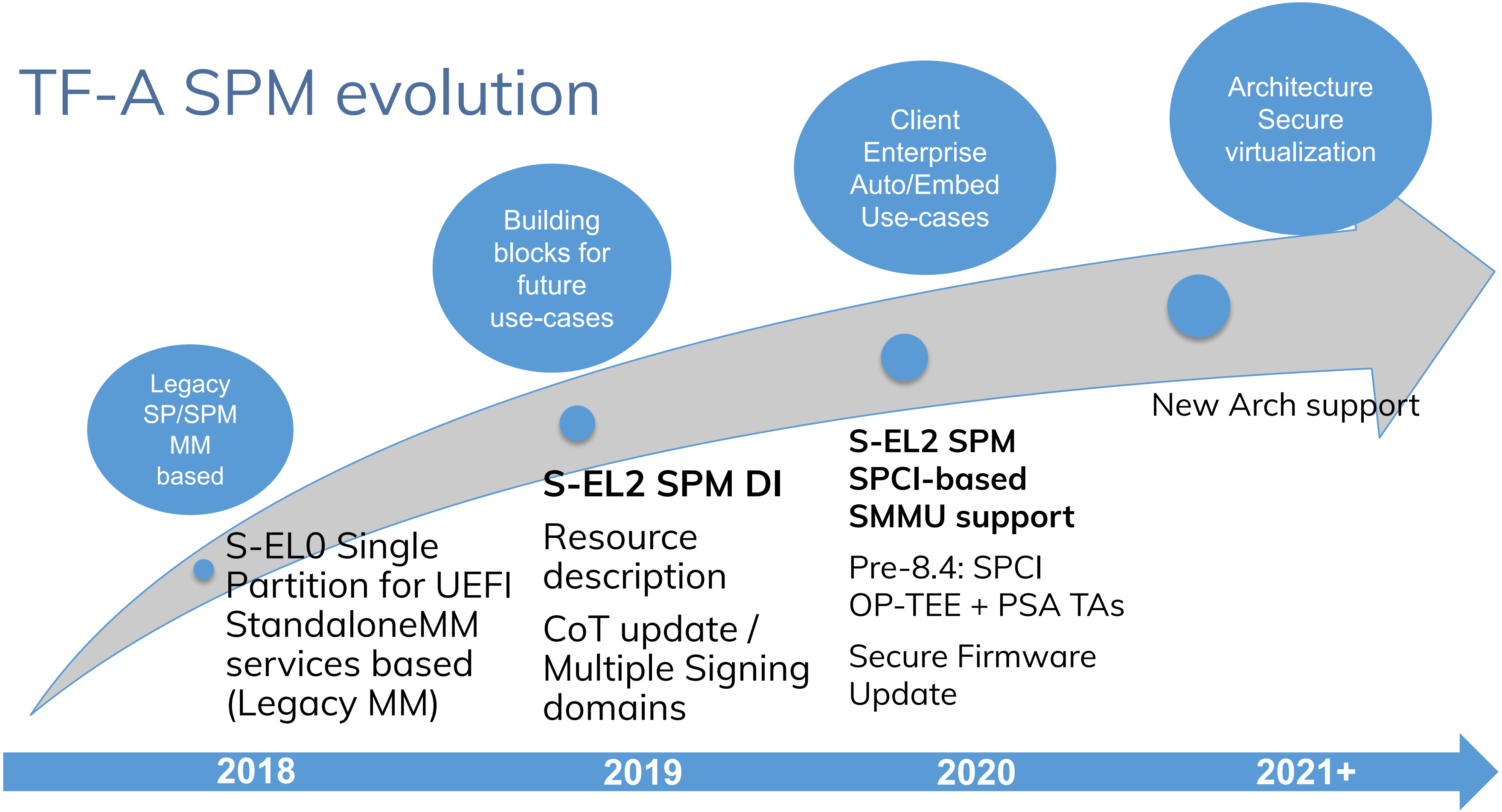
PSA API 1.1,

Secure Boot Std.

Trusted Firmware-A – June ’19 Progresses

- Architecture enablement under development
    - Armv8.3 Pointer Authentication use in Secure world (EL3 and lower S-ELs)
    - Armv8.4 Secure EL2 SPM SPCI-based investigation
- Armv8.5 Branch Target Identifier (BTI) support completed (needs GCC>9)
- GICv3 Driver updates for multi socket GIC redistributor discovery
- 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
    - New I/O Layer support
    - New Build system

TF-A SPM evolution



Legacy SP/SPM MM based

S-EL0 Single Partition for UEFI StandaloneMM services based (Legacy MM)

Building blocks for future use-cases

S-EL2 SPM DI

Resource description

CoT update / Multiple Signing domains

Client Enterprise Auto/Embed Use-cases

S-EL2 SPM SPCI-based SMMU support

Pre-8.4: SPCI OP-TEE + PSA TAs

Secure Firmware Update

Architecture Secure virtualization

New Arch support

Open Source Firmware Conference

- **Trusted Firmware sponsoring the OSFC Conference**
  - 3-6 September 2019 - @Google/Facebook premises
  - https://osfc.io/sponsors/trusted-firmware

- **Trusted Firmware & standardised open source Firmware on Arm** talk scheduled on Tuesday 3rd Sept, 5:15pm
  - https://osfc.io/talks/trustedfirmware-org-a-collaborative-effort-into-firmware-security-and-the-path-towards-standardized-open-source-firmware-on-arm

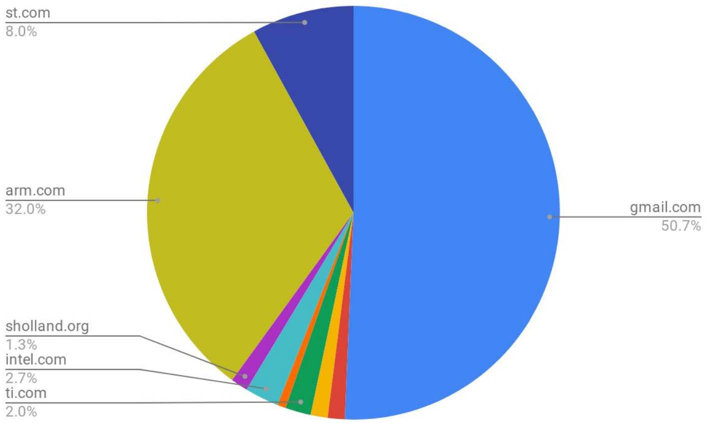
- **Trusted Firmware sponsoring the ELC, Lyon** (Oct 28-30, 2019)

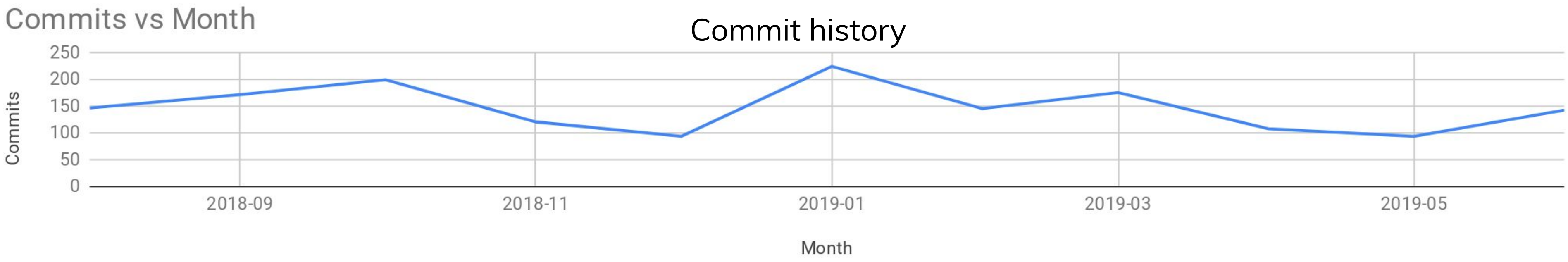
TrustedFirmware TF-A Project Dashboard

Top Authors this month

marek.vasut+renesas	74
john.tsichritzis	21
yann.gautier	12
ambroise.vincent	8
paul.beesley	7
soby.mathew	7
muhammad.hadi	4
afd	3
samuel	2

Commits by domain this month





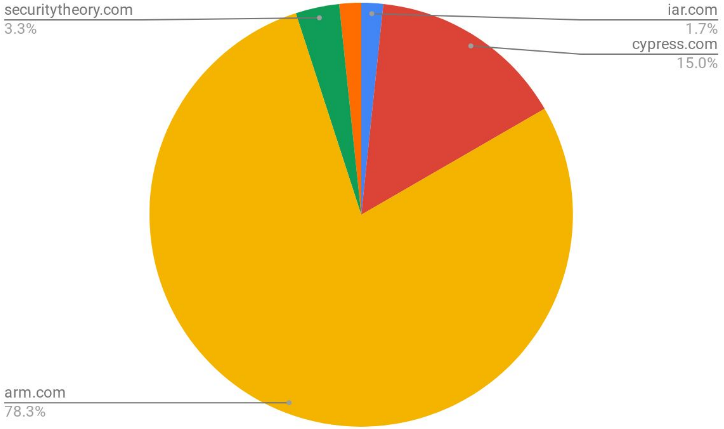
Commit history

TrustedFirmware TF-M Project Dashboard

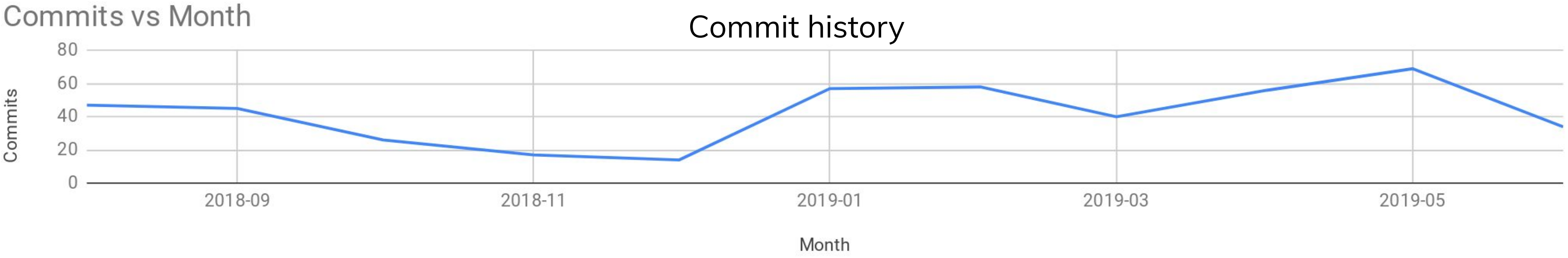
Top Authors this month

david.hu	13
jamie.fox	7
mate.toth-pal	7
ainh	5
antonio.deangelis	4
chris.brand	4
edison.ai	3
tamas.ban	2
lgl	2

Commits by domain this month



Commit history

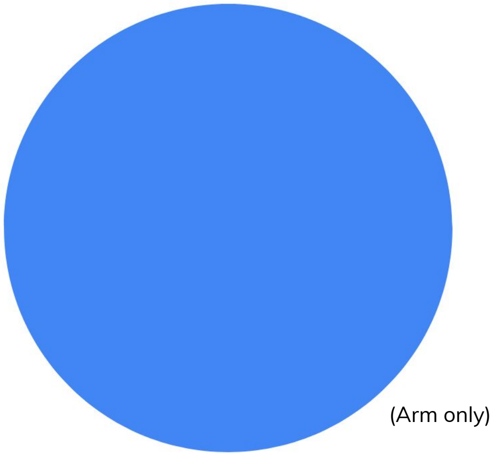


TrustedFirmware TF-A Tests Project Dashboard

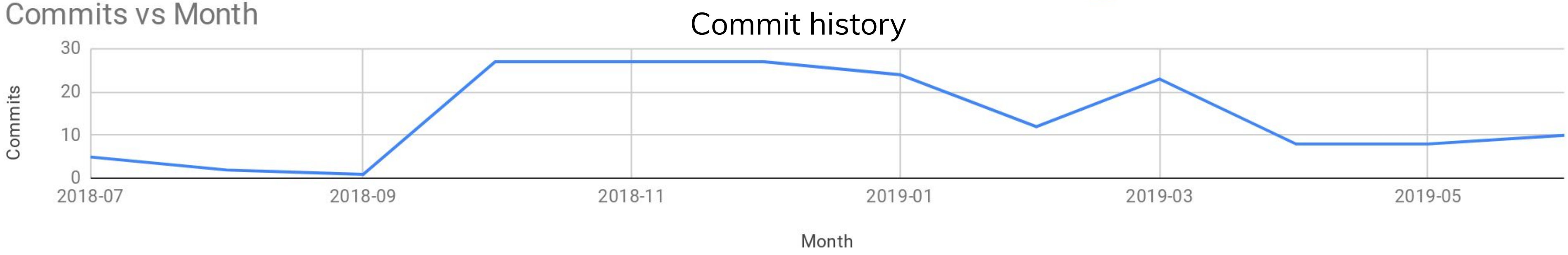
Top Authors this month

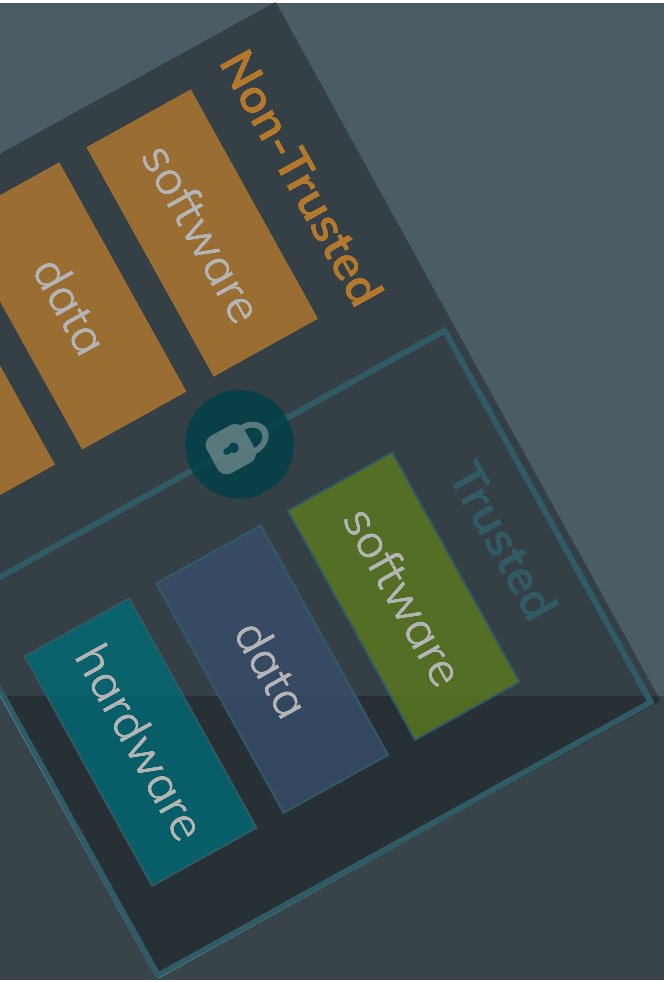
sandrine.bailleux	8
soby.mathew	1
john.tsichritzis	1
madhukar.pappireddy	1
ambroise.vincent	1

Commits by domain this month



Commit history





Non-Trusted

software

data

Trusted

software

data

hardware

arm

Linaro