arm

PSA APIs

Overview

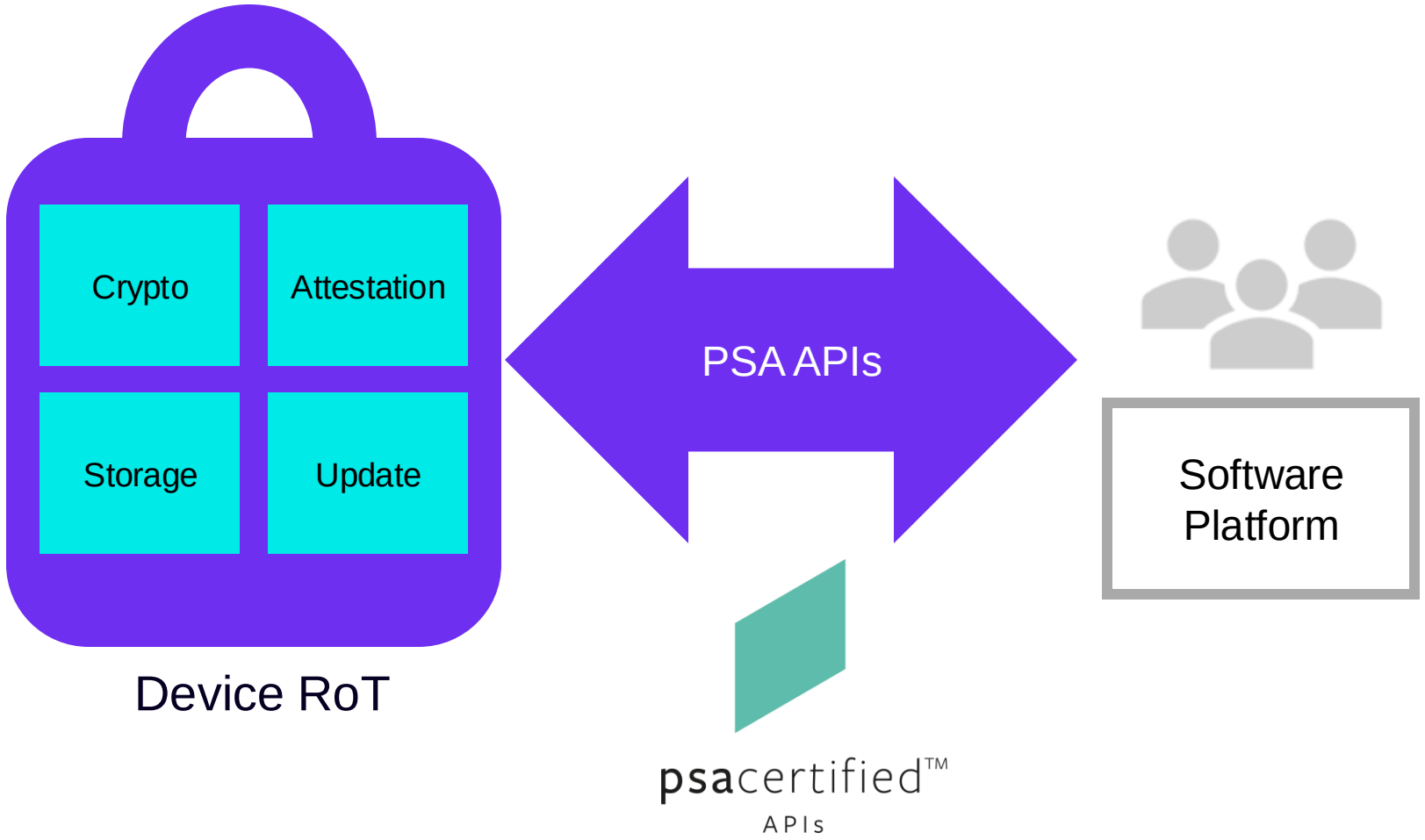
N. Devillard - Arm
2025-04-03

PSA APIs

- A fundamental set of security services:
  - Cryptographic functions to encrypt/decrypt, sign/verify, protect in integrity, manage keys.
  - Secure storage to read/store assets and keys.
  - Attestation to demonstrate device health.
  - Firmware Update for keeping devices up-to-date.

- APIs are a contract between applications and device hardware:
  - No need to learn a new API for every new piece of hardware.
  - Abstract the underlying implementation, allowing for diversity in hardware/software solutions.
  - Portability: run the same application on hardware with various security levels.

PSA APIs – making hardware security easy to use



A consistent set of APIs simplifies developer access to hardware security functions across the industry

PSA APIs for developers, chip vendors, and crypto IP

PSA APIs have been designed for three audiences:

- Software developers
  - API designed to be easy to use, hard to misuse.
  - Complete documentation with examples.
  - Open-source reference implementation available (Apache2 license).
  - No need to learn one proprietary API per type of device or software library.
  - Not Arm-specific, no licensing needed.
- Chip vendors (all APIs)
  - Your hardware security becomes immediately usable.
  - Connect with the software ecosystem.
  - Reference implementations: TF-M for Cortex-M or Trusted Services on OP-TEE for Cortex-A.
- Crypto vendors (Crypto APIs)
  - No need to invent a new proprietary API: target one that is public and maintained.
  - Focus on crypto features like speed, size, or key protection.

PSA Root of Trust – Services

In a nutshell

Crypto

- Symmetric & Asymmetric crypto
- Key handling (Opaque keys)
- Interfaces with hardware drivers

Attestation

- Entity Attestation Token (EAT)
- Device identity
- Works with secure boot and firmware updates

Secure Storage

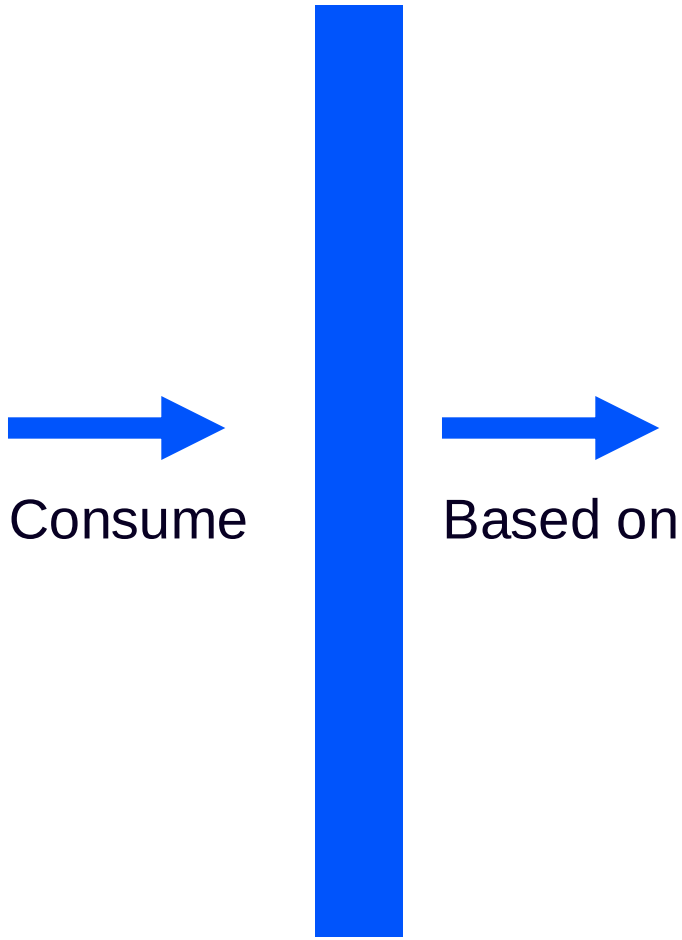
- Encryption
- Integrity
- Rollback protection

Firmware Update

- Reduce fragmentation
- Best practices

Crypto: multiple customers, multiple backends

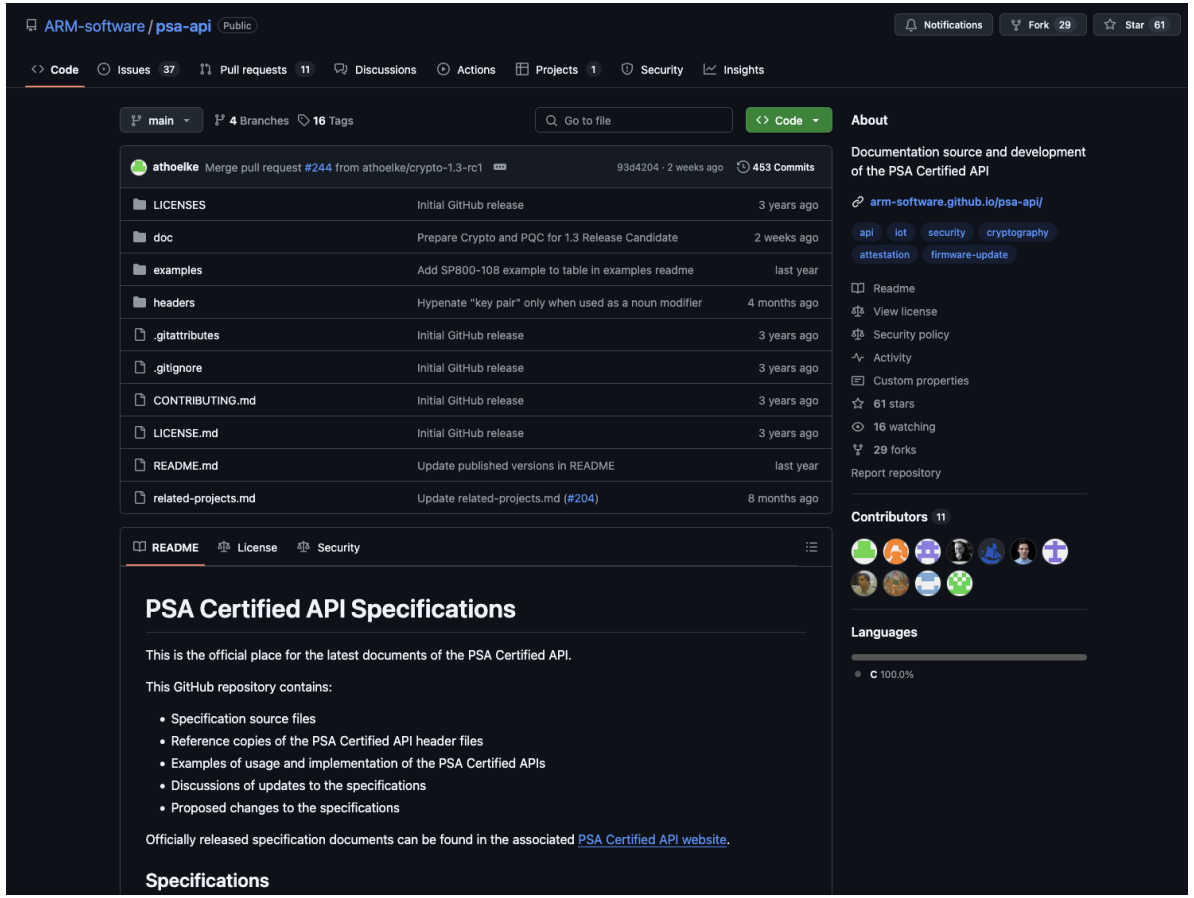
- TLS
- LoRa
- Narrowband IoT
- EAP Authenticators
- Debug Authentication
- Secure Boot
- Firmware Updates
- Attestation
- Secure Storage
- ...



- TF-M
- Trusted Services on OP-TEE
- Formally-proven code
- Optimized for speed
- Optimized for size
- Secure Elements
- Hardware Accelerators
- SIM applet through modem

PSA APIs

[Open-source project open to contributions]



PSA Certified APIs

arm

The official place for the latest published documents of the PSA Certified APIs

View the Project on GitHub
ARM-software/psa-api

This project is maintained by ARM-software

Hosted on GitHub Pages — Theme by orderedlist

PSA Certified APIs

This is the official place for the latest published documents of the PSA Certified APIs.

Specification source files, updates, and discussions, as well as reference headers and example code, can be found in the associated PSA Certified APIs GitHub project.

Test suites to verify a correct implementation can be found in the PSA Certified APIs Test suites.

Specifications

The following specifications are part of the PSA Certified APIs:

Specification				
Crypto API	1.2	HTML	↓ PDF	All versions
Secure Storage API	1.0	HTML	↓ PDF	All versions
Attestation API	1.0	HTML	↓ PDF	All versions
Firmware Update API	1.0	HTML	↓ PDF	All versions
Status code API	1.0	HTML	↓ PDF	All versions

Extensions

Extension specifications introduce new functionality that is not yet stable enough for inclusion in the main specification.

Specification	Extension				
Crypto API	PAKE	1.2 Final	HTML	↓ PDF	All versions

Feedback

If you have questions or comments on any of the specifications, or suggestions for enhancements, please raise a new issue in the PSA Certified APIs GitHub project.

Please indicate which specification the issue applies to. This can be done by:

- Providing a link to the section of the specification on this website.
- Providing the document name, full version, and section or page number in the PDF.

License

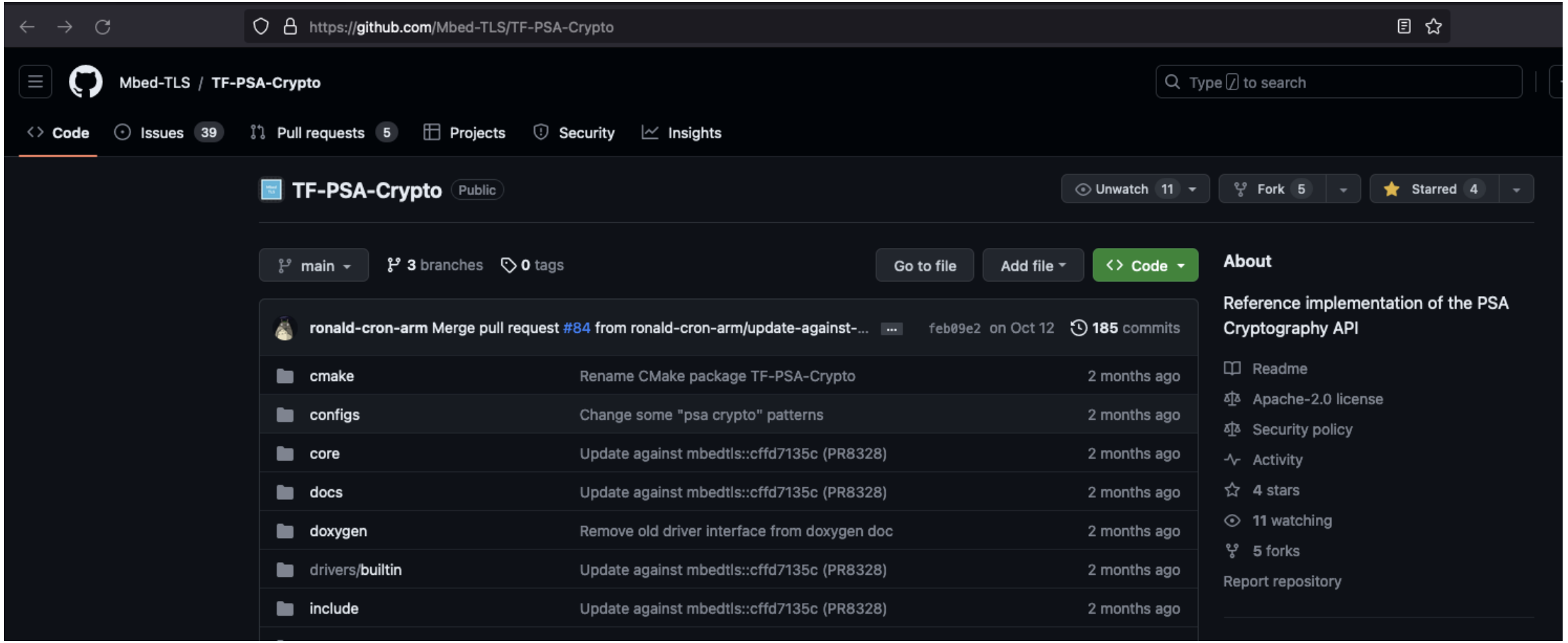
The latest versions of the PSA Certified APIs that are hosted on this website are licensed under the Creative Commons Attribution-Share Alike 4.0 International license and Apache License, Version 2.0. Some earlier versions of the specifications are licensed under a non-confidential license from Arm.

Refer to individual documents for license details.

arm

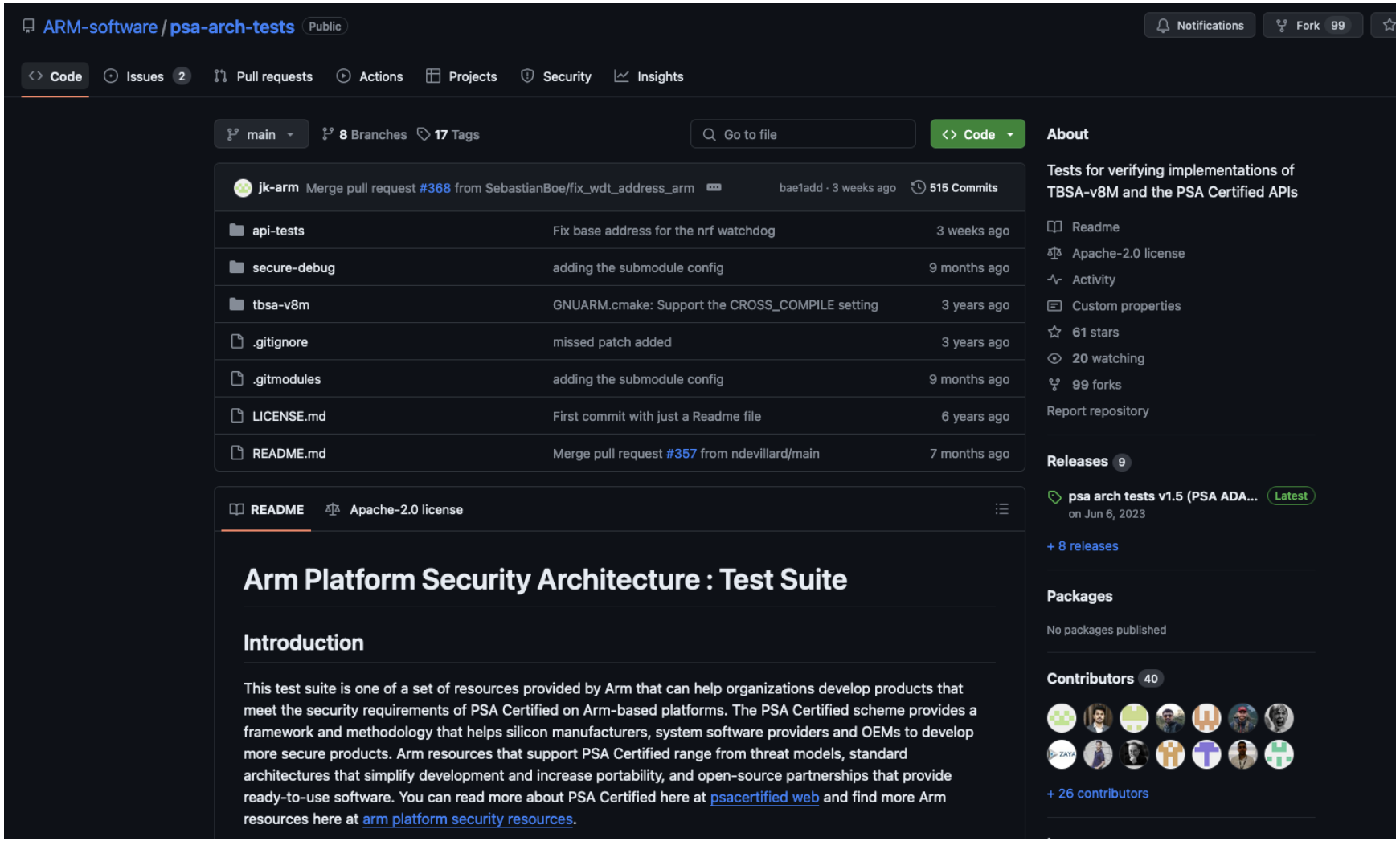
Reference implementation

https://github.com/Mbed-TLS/TF-PSA-Crypto



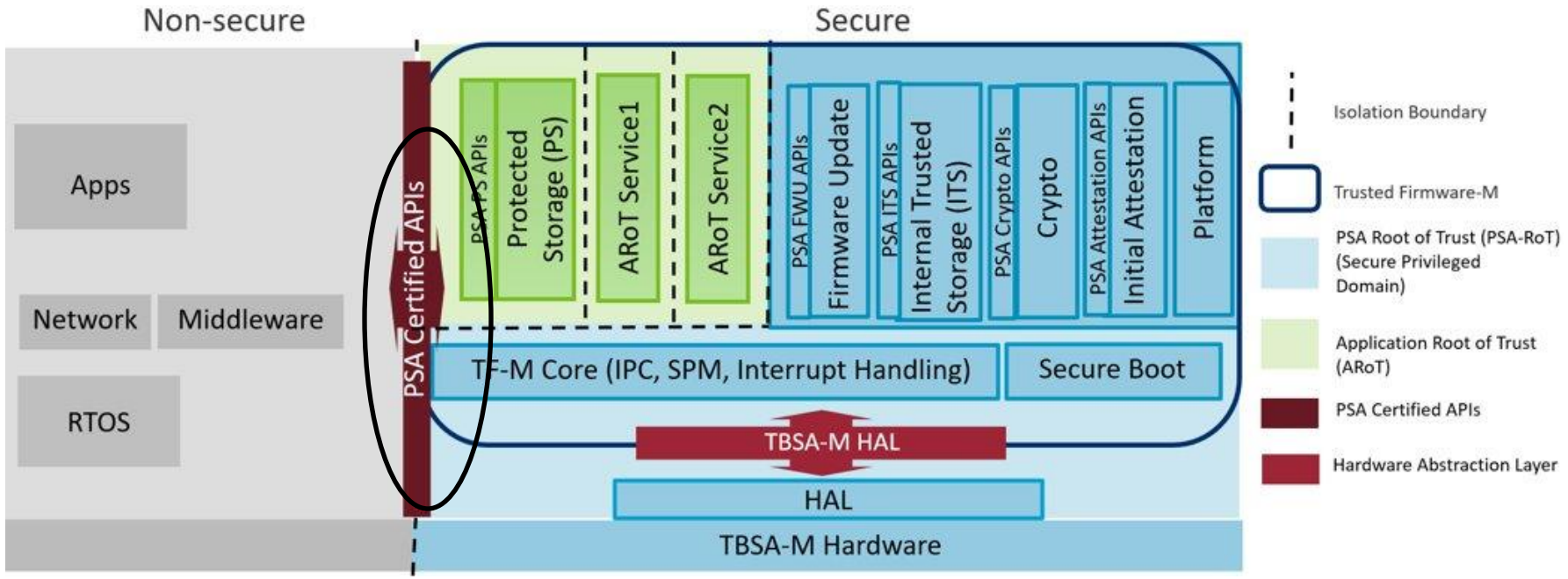
Compliance Suite

https://github.com/ARM-software/psa-arch-tests



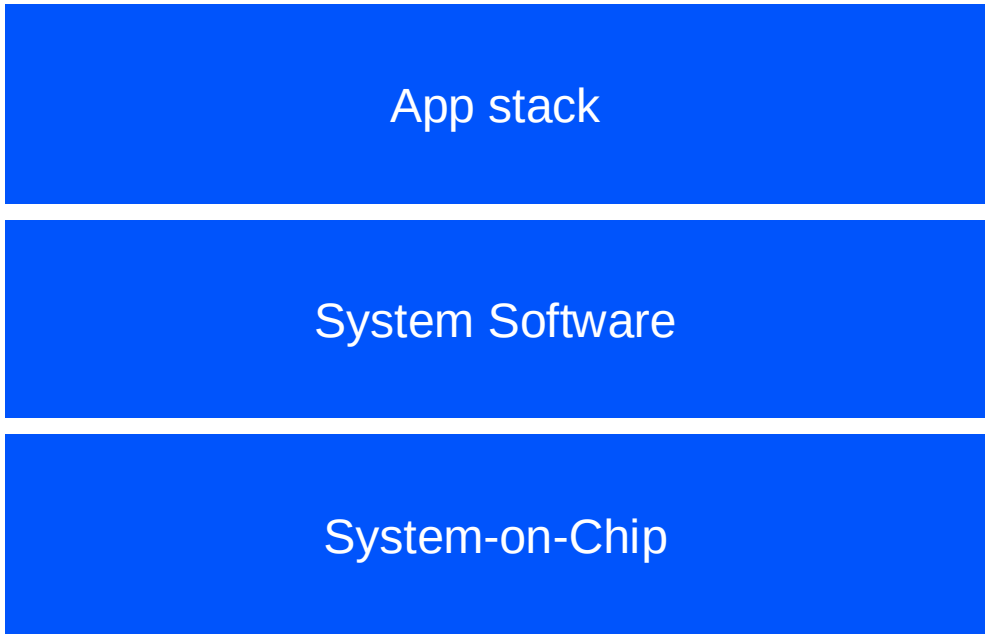
TF-M Reference Implementation for Cortex-M

- TF-M open-source Trusted Firmware for Cortex-M supports PSA Certified APIs
- Developed by www.trustedfirmware.org
- Compatible with PSA Certified Level 2
- Widely adopted
- Profiles for every use case
  - Small, Medium and Large



Open-source Trusted Firmware: TF-M

API adoption



AWS, Matter, Mbed TLS, IoTeX

FreeRTOS, Zephyr, RiotOS, ProvenCore, Za-ya

Infineon, Nordic, Nuvoton, NXP, Realtek, Renesas, Silicon Labs, ST, Xiaomi

API adoption

- Mbed TLS and TF-M: reference implementations
- Infineon, Silicon Labs, Nordic, and Renesas toolkits use PSA driver API conventions
- ST Micro uses PSA APIs as a front-end to all their Secure Manager services
- NXP SDK, PSA crypto now default Crypto API
- Matter reference code supports OpenSSL, Mbed TLS, and PSA Crypto APIs
- Realtek certified two devices: RTL8720E and RTL8730E
- WolfSSL can consume PSA-compatible crypto backends
- Zephyr OS, Riot OS adopted Crypto API
- PARSEC is packaged in Fedora, SuSE, Yocto, Debian, Ubuntu
- Oberon PSA Crypto uses PSA Crypto APIs as front-end
- Xiaomi Vela
- PSA Crypto APIs mentioned in Adaptive AUTOSAR (24.11) as standard crypto interfaces.

PSA and GlobalPlatform

- PSA is an industry standard for microcontrollers, now expanding beyond.
  We would like GP to encourage its use!

- PSA APIs are currently only discussed in public on github issues.
  Would GlobalPlatform be interested in organizing a Task Force for discussing API evolutions?

arm

Merci
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Thank You
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה
ధన్యవాదములు
Köszönöm