



# PSA APIs

## Overview

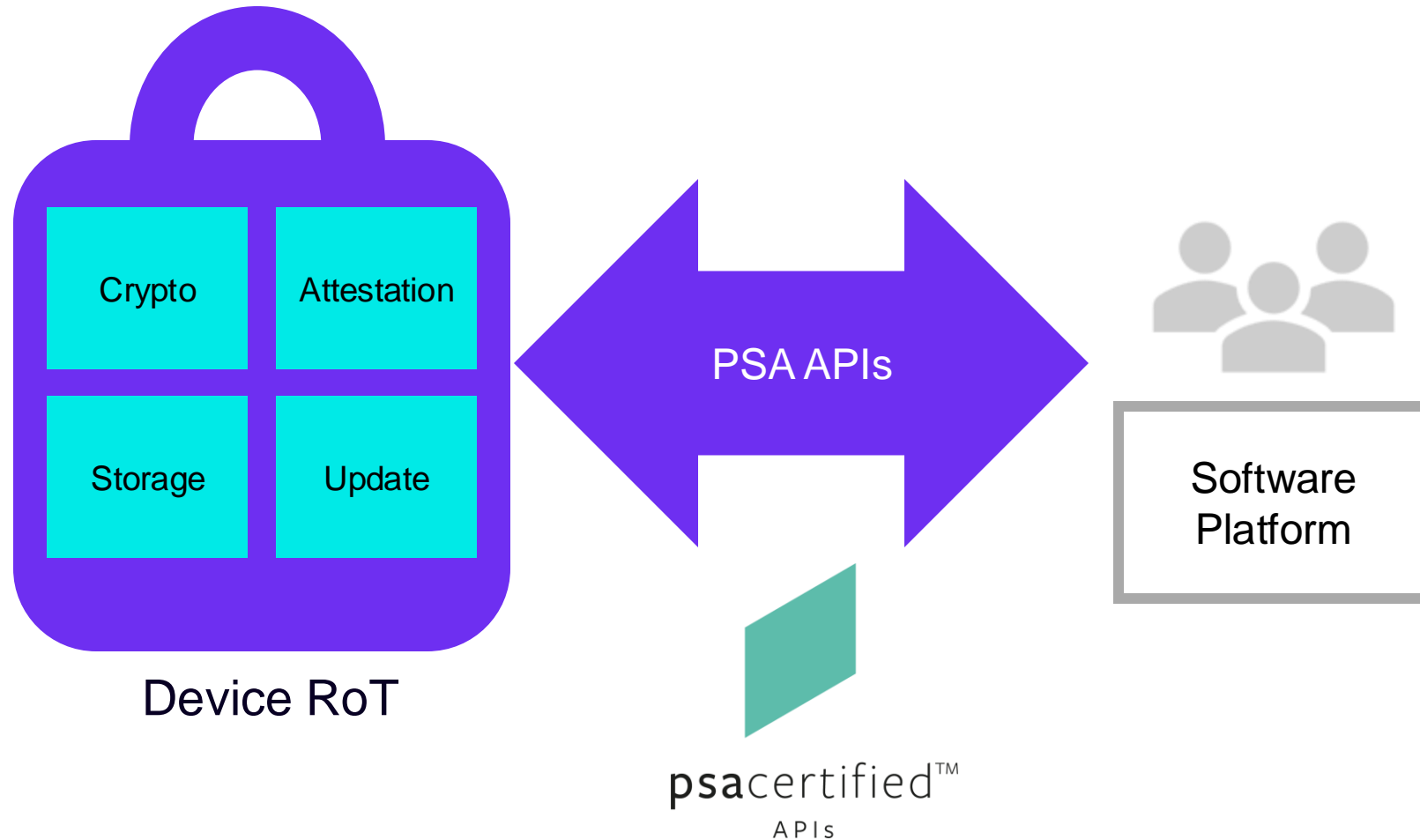
N. Devillard - Arm  
2025-04-03



# 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
- ...

→  
Consume



→  
Based on

- 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

ARM-software / psa-api (Public)

Notifications Fork 29 Star 61

<> Code Issues 37 Pull requests 11 Discussions Actions Projects 1 Security Insights

main 4 Branches 16 Tags

Go to file Code

About

athoelke Merge pull request #244 from athoelke/crypto-1.3-rc1 93d4204 · 2 weeks ago 463 Commits

LICENSES Initial GitHub release 3 years ago

doc Prepare Crypto and PQC for 1.3 Release Candidate 2 weeks ago

examples Add SP800-108 example to table in examples readme last year

headers Hyphenate "key pair" only when used as a noun modifier 4 months ago

.gitattributes Initial GitHub release 3 years ago

.gitignore Initial GitHub release 3 years ago

CONTRIBUTING.md Initial GitHub release 3 years ago

LICENSE.md Initial GitHub release 3 years ago

README.md Update published versions in README last year

related-projects.md Update related-projects.md (#204) 8 months ago

README License Security

### PSA Certified API Specifications

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

This GitHub repository contains:

- Specification source files
- Reference copies of the PSA Certified API header files
- Examples of usage and implementation of the PSA Certified APIs
- Discussions of updates to the specifications
- Proposed changes to the specifications

Officially released specification documents can be found in the associated [PSA Certified API website](#).

### Specifications

Documentation source and development of the PSA Certified API

[arm-software.github.io/psa-api/](#)

api · **iot** · security · cryptography · attestation · firmware-update

Readme View license Security policy Activity Custom properties 61 stars 16 watching 29 forks Report repository

Contributors 11

Languages C 100.0%

## 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

## 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	<a href="#">HTML</a>	<a href="#">↓ PDF</a>	<a href="#">All versions</a>
Secure Storage API	1.0	<a href="#">HTML</a>	<a href="#">↓ PDF</a>	<a href="#">All versions</a>
Attestation API	1.0	<a href="#">HTML</a>	<a href="#">↓ PDF</a>	<a href="#">All versions</a>
Firmware Update API	1.0	<a href="#">HTML</a>	<a href="#">↓ PDF</a>	<a href="#">All versions</a>
Status code API	1.0	<a href="#">HTML</a>	<a href="#">↓ PDF</a>	<a href="#">All versions</a>

### 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	<a href="#">HTML</a>	<a href="#">↓ PDF</a> <a href="#">All versions</a>

### 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.



This project is maintained by [ARM-software](#)

Hosted on GitHub Pages — Theme by [orderedlist](#)

# Reference implementation

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

The screenshot shows the GitHub repository page for **Mbed-TLS / TF-PSA-Crypto**. The repository is public and has 11 watchers, 5 forks, and 4 stars. The main branch is **main**, with 3 branches and 0 tags. The repository description is "Reference implementation of the PSA Cryptography API". The repository contains the following files and folders:

File/Folder	Description	Last Update
<b>cmake</b>	Rename CMake package TF-PSA-Crypto	2 months ago
<b>configs</b>	Change some "psa crypto" patterns	2 months ago
<b>core</b>	Update against mbedtls::cffd7135c (PR8328)	2 months ago
<b>docs</b>	Update against mbedtls::cffd7135c (PR8328)	2 months ago
<b>doxygen</b>	Remove old driver interface from doxygen doc	2 months ago
<b>drivers/builtin</b>	Update against mbedtls::cffd7135c (PR8328)	2 months ago
<b>include</b>	Update against mbedtls::cffd7135c (PR8328)	2 months ago

The repository also includes a **Readme**, **Apache-2.0 license**, and **Security policy**. The repository is currently being merged by **ronald-cron-arm** with pull request #84.



# Compliance Suite

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

The screenshot displays the GitHub interface for the `ARM-software/psa-arch-tests` repository. At the top, the repository name and 'Public' status are shown. Navigation tabs include Code, Issues (2), Pull requests, Actions, Projects, Security, and Insights. Below these, a summary bar indicates the current branch is 'main', with 8 branches and 17 tags. A search bar and a 'Code' button are also present.

The main content area is divided into two sections. The top section is a file and commit list:

File/Commit	Description	Time Ago
jk-arm	Merge pull request #368 from SebastianBoe/fix_wdt_address_arm	3 weeks ago
api-tests	Fix base address for the nrf watchdog	3 weeks ago
secure-debug	adding the submodule config	9 months ago
tbsa-v8m	GNUARM.cmake: Support the CROSS_COMPILE setting	3 years ago
.gitignore	missed patch added	3 years ago
.gitmodules	adding the submodule config	9 months ago
LICENSE.md	First commit with just a Readme file	6 years ago
README.md	Merge pull request #357 from ndevillard/main	7 months ago

The bottom section is the README, titled 'Arm Platform Security Architecture : Test Suite'. It includes an 'Introduction' section with the following text:

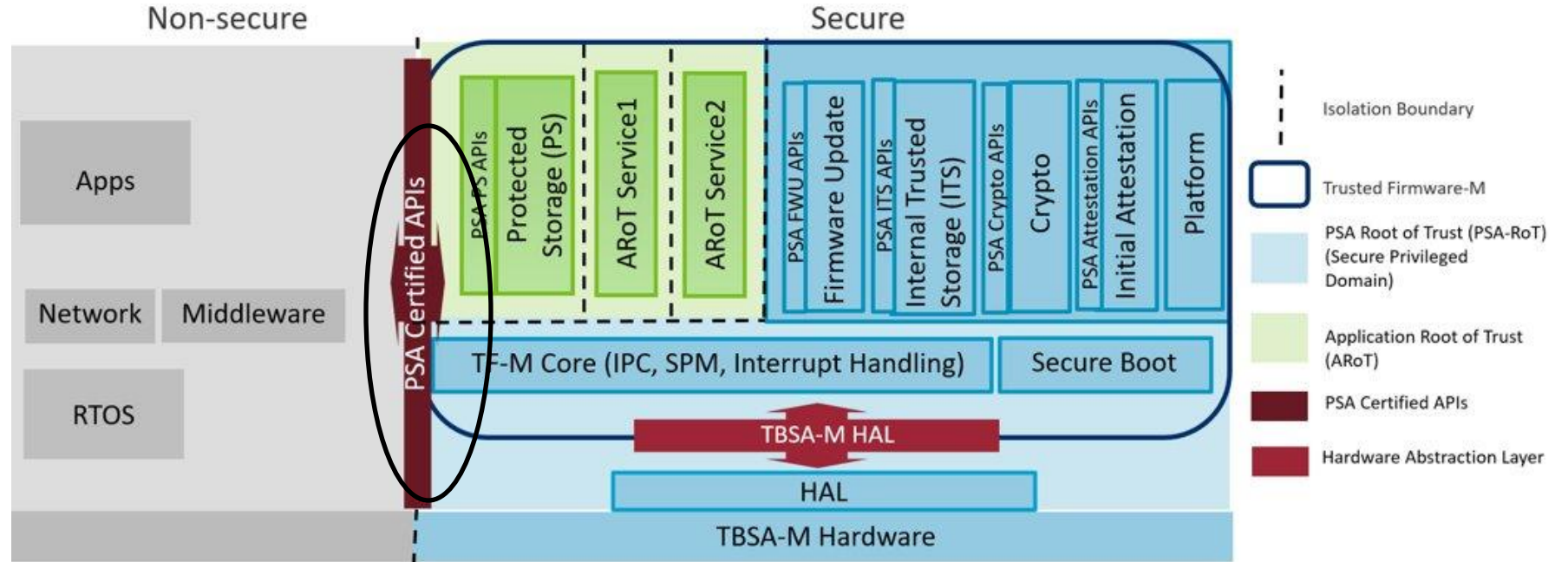
This test suite is one of a set of resources provided by Arm that can help organizations develop products that meet the security requirements of PSA Certified on Arm-based platforms. The PSA Certified scheme provides a framework and methodology that helps silicon manufacturers, system software providers and OEMs to develop more secure products. Arm resources that support PSA Certified range from threat models, standard architectures that simplify development and increase portability, and open-source partnerships that provide ready-to-use software. You can read more about PSA Certified here at [psacertified web](#) and find more Arm resources here at [arm platform security resources](#).

The right sidebar contains repository statistics and links:

- About:** Tests for verifying implementations of TBSA-v8M and the PSA Certified APIs. Links to Readme, Apache-2.0 license, Activity, Custom properties, 61 stars, 20 watching, 99 forks, and Report repository.
- Releases:** 9 releases. The latest release is 'psa arch tests v1.5 (PSA ADA...)' on Jun 6, 2023, marked as 'Latest'. There are + 8 releases in total.
- Packages:** No packages published.
- Contributors:** 40 contributors. A grid of 12 contributor avatars is shown, with + 26 contributors more.

# 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](http://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



# 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

شكراً

ধন্যবাদ

תודה

ధన్యవాదములు

Köszönöm