



psacertified™

# PSA Certified APIs Step by Step Compliance Guide



psacertified™  
APIs

Document number: JSADEN006  
Version: 2.0

Author  
PSA JSA Members:  
Arm Limited  
Brightsight B.V.  
CAICT  
Prove & Run S.A.S.  
Riscure B.V.  
Trust CB B.V.  
UL TS B.V.

Authorized by: PSA JSA Members  
Date of Issue: 09/10/2023

Copyright ©2017-2023 Arm Limited or its affiliates. All rights reserved. The copyright statement reflects the fact that some draft issues of this document have been released, to a limited circulation.

## Non-Confidential Proprietary Notice

This document is protected by copyright and other related rights and the practice or implementation of the information contained in this document may be protected by one or more patents or pending patent applications. No part of this document may be reproduced in any form by any means without the express prior written permission of Arm. No license, express or implied, by estoppel or otherwise to any intellectual property rights is granted by this document unless specifically stated.

Your access to the information in this document is conditional upon your acceptance that you will not use or permit others to use the information for the purposes of determining whether implementations infringe any third-party patents.

THIS DOCUMENT IS PROVIDED "AS IS". ARM PROVIDES NO REPRESENTATIONS AND NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE DOCUMENT. For the avoidance of doubt, Arm makes no representation with respect to, and has undertaken no analysis to identify or understand the scope and content of, patents, copyrights, trade secrets, or other rights.

This document may include technical inaccuracies or typographical errors.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL ARM BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF ARM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This document consists solely of commercial items. You shall be responsible for ensuring that any use, duplication or disclosure of this document complies fully with any relevant export laws and regulations to assure that this document or any portion thereof is not exported, directly or indirectly, in violation of such export laws. Use of the word "partner" in reference to Arm's customers is not intended to create or refer to any partnership relationship with any other company. Arm may make changes to this document at any time and without notice.

If any of the provisions contained in these terms conflict with any of the provisions of any click through or signed written agreement covering this document with Arm, then the click through or signed written agreement prevails over and supersedes the conflicting provisions of these terms. This document may be translated into other languages for convenience, and you agree that if there is any conflict between the English version of this document and any translation, the terms of the English version of the Agreement shall prevail.

The Arm corporate logo and words marked with ® or ™ are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved. Other brands and names mentioned in this document may be the trademarks of their respective owners. Please follow Arm's trademark usage guidelines at <http://www.arm.com/company/policies/trademarks>.

Copyright © 2023 Arm Limited (or its affiliates). All rights reserved.

Arm Limited. Company 02557590 registered in England.  
110 Fulbourn Road, Cambridge, England CB1 9NJ.

# PSA Certified APIs Step by Step Compliance Guide

## Getting your product compliant with PSA Certified APIs

### Executive Summary

A Root of Trust (RoT) provides the foundations for device security, it provides a source of confidentiality, trustworthy crypto and integrity that the rest of the system can build upon. Modern System on Chips (SoCs) integrate trusted hardware and trusted firmware to create the RoT but without any standard way to access those functionalities, those trust foundations are difficult for the developer to use.

PSA Certified provides a common set of APIs to achieve the basic operations required for secure services, like hashing, encrypting, signing, protecting stored data, validating a device state, or updating its firmware. A complete description and full specification of those APIs can be found at:

<https://arm-software.github.io/psa-api/>

The corresponding test suite can be found at:

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

Any vendor offering secure service implementations should aim for compatibility with wider standards to ensure those features are used and correctly deployed. Since most secure features are often based on cryptographic primitives, PSA Certified provides its API compliance program with two different scopes:

- PSA Certified Crypto API compliance for crypto vendors seeking Crypto API compatibility: crypto software libraries, accelerators, secure elements, applications running inside a trusted environment.



- General PSA Certified APIs compliance for chip vendors and system software vendors who want to showcase how their products can be used out of the box by developers familiar with the APIs



### Background

PSA Certified APIs compliance is an API compliance program that ensures security functions can be accessed using the PSA Certified APIs. Test suites are provided so that crypto vendors, chip vendors, OS providers and OEMs can check the correct functioning of the APIs and help enable a security ecosystem based on interoperable solutions.

The following is provided as guidance for developers wanting to showcase their PSA Certified APIs compliant solutions on [psacertified.org](https://psacertified.org). If you have further questions of PSA Certified APIs compliance, please contact us via the web site contact links.

PSA Certified APIs compliance requires developers to run the appropriate API compliance test suite on their implementation and submit the results for all APIs they implement.

Vendors are invited to apply for compliance badges according to the APIs they implement.

## PSA Certified APIs Compliance

General API compliance demonstrates that the PSA Certified APIs: Crypto, Storage, and Attestation are implemented. If your product passes the test suite you can showcase it on [www.psacertified.org](https://www.psacertified.org) where the test suites passing will be indicated. Examples of PSA Certified APIs implementations include:

- Root of Trust implementations with PSA Crypto, Secure Storage and Attestation APIs
- Software platforms that support the PSA Certified APIs

The PSA Certified APIs compliance test suites include validation for:

- Crypto API: all functions
- Storage API: Internal Trusted Storage (ITS) and Protected Storage (PS)
- Attestation API

There is currently no validation test suite for the Firmware Update API.

If your product passes the PSA Certified APIs test suites and the test logs are approved by Arm you can use this logo:



## Crypto API Compliance

Crypto API compliance is intended for *vendors of cryptographic solutions* e.g., software libraries, crypto accelerator chips, secure elements with or without tamper-proof storage, and any software or hardware device that provides at least one of the Crypto API functional domains:

Label	Functional Domain
crypto_hash	Hash
crypto_mac	Message Authentication Codes (MAC)
crypto_cipher	Unauthenticated ciphers
crypto_asym_sign	Asymmetric signature and verification
crypto_asym_crypt	Asymmetric encryption/decryption
crypto_aead	Authenticated encryption with associated data (AEAD)
crypto_derivation	Key derivation
crypto_agreement	Key agreement
crypto_rng	Random number generation

Implementations must be able to run stand-alone behind the Crypto API and implement the consistent set of functions required for a given domain. For services requiring key material, a key management service must be able to properly handle keys.

Examples of certifiable implementations:

- Hash computation accelerators
- Cipher acceleration chips
- Secure elements for asymmetric signature and/or verification
- Optimized assembler routines available through the Crypto API
- Crypto-grade Random Number Generation chips

If your product passes the PSA Certified Crypto API test suites and the test logs are approved by Arm you can use this logo:



## Getting Your Product API Certified

### Steps for OS vendor (General API Compliance)

1. Download the [API compliance test suite source code and porting guide](#). There are tests for crypto, attestation and secure storage APIs.
2. Port the API compliance test suite application to the OS.
3. Run and pass the compliance checker tests:
  - a. Integrate the OS with an API Certified device (for example, Musca development board and TF-M).
  - b. Interface OS to the PSA Certified APIs for Crypto, Storage, and Attestation on target device.
  - c. An OS can natively implement a sub-set of the APIs and leverage TF-M implementation for remaining APIs.
  - d. Run the PSA Certified APIs tests and capture the output report including pass/fail end results.
4. Submit the output log of the test suite run with the RTOS product info by emailing it to [psacertified@arm.com](mailto:psacertified@arm.com)
5. Acknowledgement and approval of the test report will be communicated by the scheme manager.
6. An authorized product owner can request to have their PSA Certified APIs RTOS product showcased on [psacertified.org](https://psacertified.org).
7. An authorized product owner can request a trademark license to use the appropriate PSA Certified APIs logo through [psacertified@arm.com](mailto:psacertified@arm.com)

### Steps for Chip or Device Vendor (General API Compliance)

1. Port TF-M (or equivalent) to your chip or implement the PSA Certified APIs according to the API specifications. The security functions in scope are: Crypto (full or partial), Storage (PS or ITS or both), and Attestation.
2. Provide the implementation as part of the reference trusted code for the target chip/device.
3. (Recommended) To ensure RTOS compliance, select an RTOS that has already passed PSA Certified APIs test suites.
4. Port and integrate the RTOS with the compliance checker and the target device with its trusted firmware.
5. Perform test and pass the compliance test suite.
6. Submit the output log of the test suite run with the chip/device product info by emailing it to [psacertified@arm.com](mailto:psacertified@arm.com)
7. Acknowledgement and approval of the test report will be communicated by the scheme manager.
8. An authorized product owner can request to showcase the PSA Certified API compliance chip product on [psacertified.org](https://psacertified.org).
9. An authorized product owner can request a trademark license to use the appropriate PSA Certified APIs compliant logo through [psacertified@arm.com](mailto:psacertified@arm.com)

## Steps for Crypto Vendor (Crypto API Compliance)

1. Implement the PSA Certified API according to the PSA specification. Any consistent subset of the Crypto API is acceptable, e.g.
  - o Signing and verification functions with at least one asymmetric crypto primitive.
  - o Encryption/Decryption functions with at least one symmetric crypto primitive.
  - o Hashing steps with at least one hash primitive.
  - o Key agreement functions.
  - o Key derivation functions.
  - o Random number generation functions.
2. Port the Crypto API compliance test suite to any suitable OS.
3. Run the test suite and isolate the logs pertaining to the subset you implemented.
4. Submit the output log of the test suite run with the chip/device product info by emailing it to [psacertified@arm.com](mailto:psacertified@arm.com)
5. Acknowledgement and approval of the test report will be communicated by the scheme manager.
6. An authorized product owner can request to showcase the PSA Certified API compliance chip product on [psacertified.org](https://psacertified.org).
7. An authorized product owner can request a trademark license to use the appropriate PSA Certified API compliant logo through [psacertified@arm.com](mailto:psacertified@arm.com)

## Showcasing Your PSA Certified APIs Compliant Product

If the product has passed the PSA Certified APIs test suite and the developer wants to showcase the products on [psacertified.org](https://psacertified.org), they should send the following to [psacertified@arm.com](mailto:psacertified@arm.com) along with the test suite output report.

1. Test suite output report
2. Company logo
3. Product name or product family name
4. Short product description
5. Image or graphic to represent the product
6. Link to the product web page (if appropriate)
7. Please state whether your company would like to use the PSA Certified logo and trademarks

If you wish to use the PSA Certified logos and trademarks, a trademark agreement will be sent by return email.

## FAQs

An updated list of Frequently Asked Questions can be found on the github repository for the compliance test suite, at:

<https://github.com/ARM-software/psa-arch-tests/blob/main/api-tests/docs/FAQ-compliance.md>