PSA Certified Attestation API 2.0

Document number:	IHI 0085
Release Quality:	Final
Issue Number:	0
Confidentiality:	Non-confidential
Date of Issue:	May 2026

Abstract

This document is part of the PSA Certified API specifications. It defines interfaces to provide an attestation service for the Root of Trust.

Contents

About this document

Release information

The change history table lists the changes that have been made to this document.

Table 1 Document revision history

Date	Version	Confidentiality	Change
June 2019	1.0.0	Non-confidential	First stable release with finalized 1.0 API.
August 2019	1.0.1	Non-confidential	Recommend type byte 0x01 for arm_psa_UEID. Remove erroneous guidance regarding EAT's origination claim.
February 2020	1.0.2	Non-confidential	Clarify the claim number of Instance ID. Permit COSE-Mac0 for signing tokens (with appropriate warning). Update URLs.
October 2022	1.0.3	Non-confidential	Relicensed as open source under CC BY-SA 4.0. CDDL definition added to the appendices. Example header file added to the appendices. Minor corrections and clarifications.
September 2025	1.0.4	Non-confidential	GlobalPlatform governance of PSA Certified evaluation scheme.
May 2026	2.0.0	Non-confidential	Updated attestation token format to the PSA attestation token.

The detailed changes in each release are described in *Document history* on page 18.

PSA Certified Attestation API

License

Text and illustrations

About the license

The language in the additional patent license is largely identical to that in section 3 of the Apache License, Version 2.0 (Apache 2.0), with two exceptions:

1. Changes are made related to the defined terms, to align those defined terms with the terminology in CC BY-SA 4.0 rather than Apache 2.0 (for example, changing "Work" to "Licensed Material").
2. The scope of the defensive termination clause is changed from "any patent licenses granted to You" to "any licenses granted to You". This change is intended to help maintain a healthy ecosystem by providing additional protection to the community against patent litigation claims.

To view the full text of the Apache 2.0 license, visit apache.org/licenses/LICENSE-2.0.

Source code

References

This document refers to the following documents.

Table 2 Documents referenced by this document

Ref	Document Number	Title
[PSM]	ARM DEN 0128	*Platform Security Model*. developer.arm.com/documentation/den0128
[PSA-STAT]	ARM IHI 0097	*PSA Certified Status code API*. arm-software.github.io/psa-api/status-code
[PSA-FFM]	ARM DEN 0063	*Arm® Platform Security Architecture Firmware Framework*. developer.arm.com/documentation/den0063
[C99]		ISO/IEC, *ISO/IEC 9899:1999 — Programming Languages — C*, December 1999. www.iso.org/standard/29237.html
[RFC9783]		H. Tschofenig, S. Frost, M. Brossard, A. Shaw, and T. Fossati, *Arm's Platform Security Architecture (PSA) Attestation Token*, June 2025. tools.ietf.org/html/rfc9783
[RFC2104]		IETF, *HMAC: Keyed-Hashing for Message Authentication*, February 1997. tools.ietf.org/html/rfc2104

Terms and abbreviations

This document uses the following terms and abbreviations.

Table 3 Terms and abbreviations

Term	Meaning
IAK	*Initial Attestation Key*
IMPLEMENTATION DEFINED	Behavior that is not defined by this specification, but is defined and documented by individual implementations. Application developers can choose to depend on IMPLEMENTATION DEFINED behavior, but must be aware that their code might not be portable to another implementation.
Initial Attestation Key (IAK)	Typically, the Initial Attestation Key is a secret private key from an asymmetric key-pair accessible only to the Initial Attestation service within the *Platform Root of Trust*. See *Platform Security Model* [PSM].
Non-secure Processing Environment (NSPE)	This is the security domain outside of the *Secure Processing Environment*. It is the application domain, typically containing the application firmware and hardware.
NSPE	*Non-secure Processing Environment*

continues on next page

Table 3 – continued from previous page

Term	Meaning
Platform Root of Trust (PRoT)	The overall trust anchor for the system. This ensures the platform is securely booted and configured, and establishes the secure environments required to protect security services. See *Platform Security Model* [PSM].
PRoT	*Platform Root of Trust*
PSA	Platform Security Architecture
Secure Processing Environment (SPE)	This is the security domain that includes the *Platform Root of Trust* domain.
SPE	*Secure Processing Environment*

Potential for change

The contents of this specification are stable for version 2.0.

The following may change in updates to the version 2.0 specification:

- Small optional feature additions.
- Clarifications.

Significant additions, or any changes that affect the compatibility of the interfaces defined in this specification will only be included in a new major or minor version of the specification.

Conventions

Typographical conventions

The typographical conventions are:

italic Introduces special terminology, and denotes citations.

`monospace` Used for assembler syntax descriptions, pseudocode, and source code examples.

Also used in the main text for instruction mnemonics and for references to other items appearing in assembler syntax descriptions, pseudocode, and source code examples.

SMALL CAPITALS

Used for some common terms such as IMPLEMENTATION DEFINED.

Used for a few terms that have specific technical meanings, and are included in the *Terms and abbreviations*.

Red text Indicates an open issue.

Blue text Indicates a link. This can be

- A cross-reference to another location within the document
- A URL, for example example.com

Numbers

Numbers are normally written in decimal. Binary numbers are preceded by 0b, and hexadecimal numbers by `0x`.

In both cases, the prefix and the associated value are written in a monospace font, for example `0xFFFF0000`. To improve readability, long numbers can be written with an underscore separator between every four characters, for example `0xFFFF_0000_0000_0000`. Ignore any underscores when interpreting the value of a number.

Feedback

We welcome feedback on the PSA Certified API documentation.

If you have comments on the content of this book, visit github.com/arm-software/psa-api/issues to create a new issue at the PSA Certified API GitHub project. Give:

- The title (PSA Certified Attestation API).
- The number and issue (IHI 0085 2.0.0).
- The location in the document to which your comments apply.
- A concise explanation of your comments.

We also welcome general suggestions for additions and improvements.

1 Introduction

1.1 About Platform Security Architecture

This document is one of a set of resources provided by Arm that can help organizations develop products that meet the security requirements of GlobalPlatform's PSA Certified evaluation scheme 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 www.psacertified.org and find more Arm resources here at developer.arm.com/platform-security-resources and www.trustedfirmware.org.

1.2 About the Attestation API

The interface described in this document is a PSA Certified API, that provides a verifiable report of the state of the platform. The platform attestation service is provided by the *Platform Root of Trust* and is described in *Platform Security Model* [PSM].

The format of the attestation report that is produced by the Attestation API is specified in *Arm's Platform Security Architecture (PSA) Attestation Token* [RFC9783].

> **Note:**
>
> Version 2.0 of this specification is not compatible with any 1.0 version, as a result of the change in format of the attestation report that is generated by this API.

This document includes:

- A set of common use cases. See *Use cases and rationale* on page 9.
- The associated Application Programming Interface (API). See *API reference* on page 12.

The Attestation API can be used either to directly produce verifiable evidence about the platform state in the context of a challenge-response interaction, or as a way to bootstrap trust in other attestation schemes. The PSA Certified framework provides the generic security features allowing OEM and service providers to integrate various attestation schemes on top of the Platform Root of Trust.

You can find additional resources relating to the Attestation API here at arm-software.github.io/psa-api/attestation, and find other PSA Certified APIs here at arm-software.github.io/psa-api.

2 Use cases and rationale

The following subsections describe the primary use cases that this version of Attestation API aims to support. Other use cases are also possible.

The *Platform Root of Trust* (PRoT) reports information, known as claims, that can be used to determine the exact implementation of the PRoT and its security state. If the PRoT loads other components then it also includes information about what it has loaded. Other components outside of the PRoT can bind additional information to the report by incorporating that information, or a hash of it, into the challenge passed to the attestation API. The PRoT signs attestation reports using the *Initial Attestation Key* (IAK).

2.1 Device enrolment

Enrolment is the ability for an online service to enlist a device. For example, a generic connected sensor that becomes part of a company's deployment. As part of the enrolment process, credentials need to be created for each device. However, the devices themselves need to be trustworthy to ensure that credentials are not leaked.

A common solution to this problem is to certify security hardware using third-party labs, who are trusted to deliver worthwhile certifications. By placing trust in evaluation reports (such as Common Criteria or PSA Certified), one can ascertain whether a Root of Trust exhibits important security properties. For example, one important property is the ability to generate a key pair of good quality (using a non-predictable random number generator) and store it in an isolated and tamper-proof area, which provides strong assurance that a device private key is only ever known by that device. Each device instance contains a protected attestation key that can be used to prove that they are a particular certified implementation.

During such an enrolment process, a device might generate a new key pair and create a Certificate Signing Request (CSR) or equivalent, containing:

- The public key of the generated key-pair.
- A proof of possession of the corresponding private key (in general this is the public key signed by the private key). This protects against man-in-the-middle attacks where an attacker can hijack the enrolment to insert their own public key into the device request.
- An initial attestation, in order for the recipient to assess how that particular combination of hardware and firmware can be trusted.

The CSR is then passed to a Certification Authority who can assign it an identity with the new service and then return an identity certificate signed using the private key of the Certification Authority. The Certification Authority may be operated by the company who owns the devices or operated by a trusted third party. Creating extra identities on devices is expected to be a routine operation.

If a device enforces a high level of isolation, where all applications execute within their own Secure Partition, then it allows several mutually-distrustful providers to install their applications side-by-side without having to worry about leaking assets from one application to another.

The attestation identity can be verified in an attestation process and checked against certification information. At the end of the process the credential manager can establish a secure connection to the attested endpoint, and deliver credentials. For example, these may be service access credentials.

2.2 Identifying certification

The combination of a hardware entity and the software installed on that entity can be certified to conform to some published security level.

Manufacturers of devices can advertise a security certification as an incentive to purchase their devices, or because it is a requirement from a regulator. To gain the certification a manufacturer can engage a test lab to verify the hardware and software combination of a device conforms to specific standards. Certification should not be declared by the device, instead it is a dynamic situation where the hardware and software state can be checked against the current known certification status for that combination.

The initial attestation report declares the state of the device to a verification service. The verification service can then:

- Verify the production status of the device identity. For example, to identify whether the device is in an inventory, and whether it is a secured production device or a development device.
- Verify the certification status of a device. This involves checking that all components are up to date, correctly signed, and certified to work together.

2.3 Integrity reporting

A party may want to check the received list of claims against a database of known measurements for each component in order to decide which level of trust should be applied. Additional information can be included, such as the version numbers for all software running on the device. As a minimum, the device provides a hash for each loaded component. Boot measurements are included in order to assess if there are obvious signs of tampering with the device firmware.

Initial attestation requires three services:

- Enrolment verification service enforcing policy as part of service enrolment of the device.
- Production verification service (OEM), providing the production state of an attestation identity
- Certification verification service (third party), verifying that all attested components are up to date, signed correctly, and certified to work together.

It is possible to further separate these roles. For example, there may be a separate software verification service.

These services can be hosted by different parties in online or offline settings:

- The first service requires generating a challenge, reading back the device's token, and validating the signature of the token.
- The second service may periodically log the current security state for all addressable devices and make that information available upon request. It does not require the knowledge of any pre-shared secret or a prior trust exchange with a device vendor. The various databases required for the full verification process may be local, replicated, or centralized, depending on the particular market.

Further information about using existing attestation protocols can be found in [PSM].

3 Initial Attestation report

The attestation report returned by the Attestation API is formatted and encoded as a signed PSA Attestation Token. This is defined in *Arm's Platform Security Architecture (PSA) Attestation Token* [RFC9783].

The PSA Attestation Token is an incompatible evolution of the original attestation format, that was specified in version 1.0 of the Attestation API.

To comply with version 2.0 of the Attestation API, an implementation must only produce attestation reports that conform to [RFC9783].

Table 4 provides specific recommendations for the construction of some of the token claims.

Table 4 Recommended construction of the token claims

Claim	Recommended construction
Instance ID	The construction of the 32-byte key-hash component of this claim depends on the type of *Initial Attestation Key* (IAK): • When using an asymmetric key-pair for the IAK, the Instance ID is a hash of the corresponding public key — `InstanceID = H(IAK)`. • When using a symmetric key for the IAK, it is recommended that the Instance ID is a *double* hash of the key — `InstanceID = H(H(IAK))`.

4 API reference

The Attestation API defines a header file that is provided by the implementation. The header is `psa/initial_attestation.h`.

All the elements are defined in the C language. The Attestation API makes use of standard C data types, including the fixed-width integer types from the ISO C99 specification update [C99].

4.1 API conventions

All functions return a status indication of type `psa_status_t`, which is defined by *PSA Certified Status code API* [PSA-STAT]. The value `0` (`PSA_SUCCESS`) indicates successful operation, and a negative value indicates an error. Each API documents the specific error codes that might be returned, and the meaning of each error.

All parameters of pointer type must be valid, non-null pointers unless the pointer is to a buffer of length 0 or the function's documentation explicitly describes the behavior when the pointer is null. For implementations where a null pointer dereference usually aborts the application, passing NULL as a function parameter where a null pointer is not allowed should abort the caller in the habitual manner.

Pointers to input parameters may be in read-only memory. Output parameters must be in writable memory. Output parameters that are not buffers must also be readable, and the implementation must be able to write to a non-buffer output parameter and read back the same value.

4.2 Status codes

The Attestation API uses the status code definitions that are shared with the other PSA Certified APIs.

The following elements are defined in `psa/error.h` from *PSA Certified Status code API* [PSA-STAT] (previously defined in [PSA-FFM]):

```
typedef int32_t psa_status_t;

#define PSA_SUCCESS ((psa_status_t)0)

#define PSA_ERROR_GENERIC_ERROR         ((psa_status_t)-132)
#define PSA_ERROR_INVALID_ARGUMENT      ((psa_status_t)-135)
#define PSA_ERROR_BUFFER_TOO_SMALL      ((psa_status_t)-138)
#define PSA_ERROR_SERVICE_FAILURE       ((psa_status_t)-144)
```

These definitions must be available to an application that includes the `psa/initial_attestation.h` header file.

> **Implementation note**
>
> An implementation is permitted to define the status code interface elements within `psa/initial_attestation.h`, or to define them via inclusion of a `psa/error.h` header file that is shared with the implementation of other PSA Certified APIs.

4.3 General definitions

4.3.1 PSA_INITIAL_ATTEST_API_VERSION_MAJOR (macro)

The major version of this implementation of the Attestation API.

```
#define PSA_INITIAL_ATTEST_API_VERSION_MAJOR 2
```

4.3.2 PSA_INITIAL_ATTEST_API_VERSION_MINOR (macro)

The minor version of this implementation of the Attestation API.

```
#define PSA_INITIAL_ATTEST_API_VERSION_MINOR 0
```

4.3.3 PSA_INITIAL_ATTEST_MAX_TOKEN_SIZE (macro)

The maximum possible size of a token.

```
#define PSA_INITIAL_ATTEST_MAX_TOKEN_SIZE /* implementation-specific value */
```

The value of this constant is IMPLEMENTATION DEFINED.

4.4 Challenge sizes

The following constants define the valid challenge sizes that must be supported by the function `psa_initial_attest_get_token()` and `psa_initial_attest_get_token_size()`.

An implementation must not support other challenge sizes.

4.4.1 PSA_INITIAL_ATTEST_CHALLENGE_SIZE_32 (macro)

A challenge size of 32 bytes (256 bits).

```
#define PSA_INITIAL_ATTEST_CHALLENGE_SIZE_32 (32u)
```

4.4.2 PSA_INITIAL_ATTEST_CHALLENGE_SIZE_48 (macro)

A challenge size of 48 bytes (384 bits).

```
#define PSA_INITIAL_ATTEST_CHALLENGE_SIZE_48 (48u)
```

4.4.3 PSA_INITIAL_ATTEST_CHALLENGE_SIZE_64 (macro)

A challenge size of 64 bytes (512 bits).

```
#define PSA_INITIAL_ATTEST_CHALLENGE_SIZE_64 (64u)
```

4.5 Attestation

4.5.1 `psa_initial_attest_get_token` (function)

Retrieve the Initial Attestation Token.

```
psa_status_t psa_initial_attest_get_token(const uint8_t *auth_challenge,
                                          size_t challenge_size,
                                          uint8_t *token_buf,
                                          size_t token_buf_size,
                                          size_t *token_size);
```

Parameters

`auth_challenge`	Buffer with a challenge object. The challenge object is data provided by the caller. For example, it may be a cryptographic nonce or a hash of data (such as an external object record). If a hash of data is provided then it is the caller's responsibility to ensure that the data is protected against replay attacks (for example, by including a cryptographic nonce within the data).
`challenge_size`	Size of the buffer `auth_challenge` in bytes. The size must always be a supported challenge size. Supported challenge sizes are defined in *Challenge sizes* on page 13.
`token_buf`	Output buffer where the attestation token is to be written.
`token_buf_size`	Size of `token_buf`. The expected size can be determined by using the `psa_initial_attest_get_token_size` function.
`token_size`	Output variable for the actual token size.

Outputs

`*token_buf`	On success, the attestation token.
`*token_size`	On success, the number of bytes written into `token_buf`.

Returns: `psa_status_t`

`PSA_SUCCESS`	Action was performed successfully.
`PSA_ERROR_SERVICE_FAILURE`	The implementation failed to fully initialize.
`PSA_ERROR_BUFFER_TOO_SMALL`	`token_buf` is too small for the attestation token.
`PSA_ERROR_INVALID_ARGUMENT`	The challenge size is not supported.
`PSA_ERROR_GENERIC_ERROR`	An unspecified internal error has occurred.

Description

Retrieves the Initial Attestation Token. A challenge can be passed as an input to mitigate replay attacks.

4.5.2 `psa_initial_attest_get_token_size` (function)

Calculate the size of an Initial Attestation Token.

```
psa_status_t psa_initial_attest_get_token_size(size_t challenge_size,
                                               size_t *token_size);
```

Parameters

`challenge_size`	Size of a challenge object in bytes. This must be a supported challenge size as specified in *Challenge sizes* on page 13.
`token_size`	Output variable for the token size.

Outputs

`*token_size`	On success, the size of an attestation token in bytes when using the specified `challenge_size`

Returns: `psa_status_t`

`PSA_SUCCESS`	Action was performed successfully.
`PSA_ERROR_SERVICE_FAILURE`	The implementation failed to fully initialize.
`PSA_ERROR_INVALID_ARGUMENT`	The challenge size is not supported.
`PSA_ERROR_GENERIC_ERROR`	An unspecified internal error has occurred.

Description

Retrieve the exact size of the Initial Attestation Token in bytes, given a specific challenge size.

Appendix A: Example header file

Each implementation of the Attestation API must provide a header file named `psa/initial_attestation.h`, in which the interface elements in this specification are defined.

This appendix provides a example of the `psa/initial_attestation.h` header file with all of the API elements. This can be used as a starting point or reference for an implementation.

> **Note:**
>
> Not all of the API elements are fully defined. An implementation must provide the full definition.
>
> The header will not compile without these missing definitions, and might require reordering to satisfy C compilation rules.

A.1 psa/initial_attestation.h

```
/* This file is a reference template for implementation of the
 * PSA Certified Attestation API v2.0
 */

#ifndef PSA_INITIAL_ATTESTATION_H
#define PSA_INITIAL_ATTESTATION_H

#include <stddef.h>
#include <stdint.h>

#ifdef __cplusplus
extern "C" {
#endif

#define PSA_INITIAL_ATTEST_API_VERSION_MAJOR 2
#define PSA_INITIAL_ATTEST_API_VERSION_MINOR 0
#define PSA_INITIAL_ATTEST_MAX_TOKEN_SIZE /* implementation-specific value */
#define PSA_INITIAL_ATTEST_CHALLENGE_SIZE_32 (32u)
#define PSA_INITIAL_ATTEST_CHALLENGE_SIZE_48 (48u)
#define PSA_INITIAL_ATTEST_CHALLENGE_SIZE_64 (64u)
psa_status_t psa_initial_attest_get_token(const uint8_t *auth_challenge,
                                          size_t challenge_size,
                                          uint8_t *token_buf,
                                          size_t token_buf_size,
                                          size_t *token_size);
psa_status_t psa_initial_attest_get_token_size(size_t challenge_size,
                                               size_t *token_size);
```

(continues on next page)

(continued from previous page)

```
#ifdef __cplusplus
}
#endif

#endif // PSA_INITIAL_ATTESTATION_H
```

Appendix B: Document history

Date	Changes
June 2019	*1.0.0* • First stable release
August 2019	*1.0.1* • Fixed typos and descriptions based on feedback. • Recommend type byte 0x01 for arm_psa_UEID. • Remove erroneous guidance regarding EAT's origination claim - it should not be used to find a verification service.
February 2020	*1.0.2* • Clarify the claim number of Instance ID • Permit COSE-Mac0 for signing tokens (with appropriate warning) • Update URLs
October 2022	*1.0.3* • Relicensed the document under Attribution-ShareAlike 4.0 International with a patent license derived from Apache License 2.0. See *License* on page iv. • Fix CBOR type of `arm_psa_origination` to text string. Spec and example were in conflict, and the example was correct. • Added CDDL definition to the appendices, which can be helpful to developers. • Instance ID definition for symmetric keys has been improved. The specific constructions are now recommended rather than normative. • Clarified the optionality of map entries in the Software Components claim.
September 2025	*1.0.4* • Updated introduction to reflect GlobalPlatform assuming the governance of the PSA Certified evaluation scheme.

continues on next page

Table 5 – continued from previous page

Date	Changes
May 2026	*2.0.0* • Update the API to use the PSA attestation token, defined in *Arm's Platform Security Architecture (PSA) Attestation Token* [RFC9783]. The token and report format, CDDL definition, and example token are no longer required in this specification.