TRUST AND VERIFY

TrustCB Scheme Procedures for PSA

Version 2.0

Contents

PSA Certified 3

Introducing the PSA Certified scheme 3

PSA Certified Contact details 3

PSA Certified TOE-type overview 3

PSA Certified Process 3

Submission phase 3

Evaluation phase 3

Certification phase 4

PSA Certified Reference Materials 4

1 PSA Certified

This document an annex to TrustCB Shared Scheme Procedures version 2.0 [TrustCB_SP] detailing the pertinent details for the PSA Certified scheme.

1.1 Introducing the PSA Certified scheme

Arm Ltd has appointed TrustCB as the Certification Body for PSA Certified.

PSA Certified is the independent security evaluation scheme for Platform Security Architecture (PSA) based IoT systems. It establishes trust through a multi-level assurance program for chips containing a security component called a Root of Trust (PSA-RoT) that provides trusted functionality to the platform.

The Developer role in the PSA Certified scheme may be fulfilled by the Chip vendor, RTOS vendor or the OEM.

The primary source of information on the scheme is at https://psacertified.com.

The TrustCB scheme procedures and documents can be found at https://trustcb.com/iot/psa-certified/.

1.2 PSA Certified Contact details

Scheme contact address at TrustCB is: psacertified@trustcb.com.

Scheme owner contact address is: psacertified@arm.com.

1.3 PSA Certified TOE-type overview

The scope for PSA Certified security evaluation is the combination of the hardware and software components supporting a device. There are three certification scopes, the Chip, the RTOS and the Device. The details of the components in the PSA architecture and the related security certification scopes are provided in [PSA-L1] and [PSA-L2].

1.4 PSA Certified Process

Prior to the submission phase, the developer has contracted a licensed evaluation lab and together with that lab has filled in the application form.

1.4.1 Submission phase

As detailed below, for PSA Certified L1 evaluations the submission phase and evaluation phase are combined into a single interaction with TrustCB.

L2 evaluations following the standard process where the submission is completed separately to the evaluation phase, by sending the completed application form to the TrustCB contact address psacertified@trustcb.com.

1.4.2 Evaluation phase

By default a single-stage evaluation phase is used for PSA Certified L1 evaluations, whereby the evaluator submits the evaluation report at the same time as submitting the application form, and the completed questionnaire and supporting documentation from the developer.

For PSA Certified L2 evaluation, the two-stage approach described in [TrustCB_SP] "*Decomposition of Evaluation Phase*" is to be applied.

Reporting for PSA Certified evaluations does not require application of the Evaluation Technical Report for Composition template of SOGIS [ETR].

For L1 evaluation, in addition to the items specified in [TrustCB_SP] "*Evaluator reporting*" the evaluator must provide a short report indicating:

- Which section of the [PSA-L1] questionnaire has been completed (Chip, RTOS or OEM).
- For each requirement in the Assessment Questionnaire, whether the evaluator has reached a "Pass", "Fail" or "Inconclusive" verdict, together with a short rationale of why that verdict has been assigned.
- An overall conclusion of the evaluator findings.

The details of the Evaluation Technical Report content for L2 are provided in [PSA-EM].

1.4.3 Certification phase

Responsibilities in the Certification phase are split between TrustCB and psacertified.org. PSA certified Certificates are issued on PSACertified.org on the positive advice of TrustCB.

It is the responsibility of psacertified.org to generate and publish the final certificate, under the rules of psacertified.org. This is described in [PSA-L1SBS]. Therefore, certificate validity for PSA Certified products is under the control of PSACertified.org, and the certificate rules described in [TrustCB_SP] "Certificate validity" do not apply.

PSA Certificate information includes the version of the evaluation, the test laboratory and the date of passing. The version of hardware and software for the Target of Evaluation is also specified.

These certificates will be displayed on PSACertified.org for 4 years with a globally unique EAN13-5 number. There is no plan to invalidate or retire certifications.

The viewer of a PSA Certificate should consider the time elapsed since the evaluation was performed, updates to the TOE and review known vulnerability databases when considering the products security robustness and trustworthiness.

1.5 PSA Certified Reference Materials

The documents listed in Table 1 are specific to the PSA Certified scheme operated by TrustCB.

Table 1 PSA Certified Documents

PSA Certified Level 1 Questionnaire, JSADEN0001	V1.2	[PSA-L1]
PSA Certified Level 1 Step-by-step guide, JSADEN005	V1.5	[PSA-L1SBS]
PSA Certified Level 2 Lightweight Protection Profile, JSADEN0002	BET03	[PSA-L2]
PSA Certified Level 2 Evaluation Methodology, JSADEN0003	BET01	[PSA-EM]
PSA Certified Level 2 Attack Method, JSADEN0004	BET01	[PSA-AM]
Arm Platform Security Architecture Firmware Framework and RoT Services – M-profile, ARMDEN0063	V0.10	[PSA-FF]
TrustCB PSA Application Form (L1)	v1.0.1	[PSA-L1-AF]
TrustCB PSA Application Form (L2)	v1.0.1	[PSA-L2-AF]