TRUST AND VERIFY

TrustCB Scheme Procedures for SESIP

Version 2.0

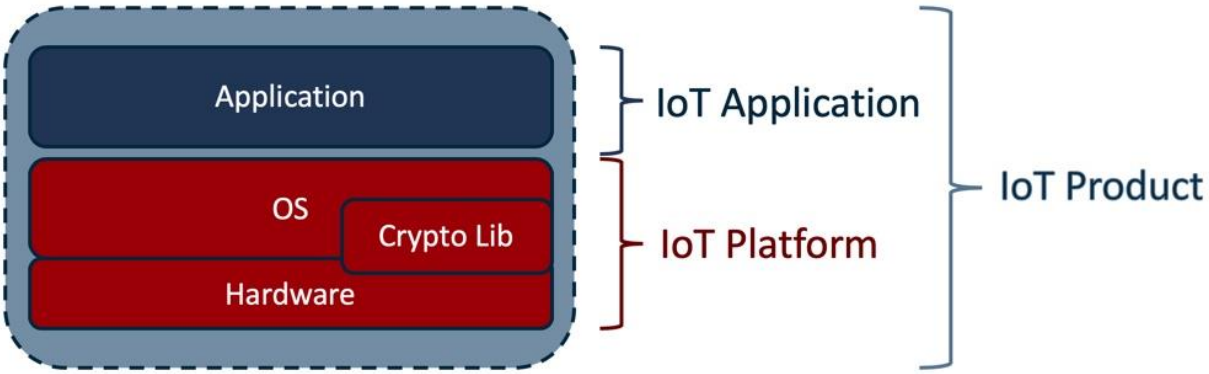
Contents

1 SESIP

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

1.1 Introducing the SESIP scheme

TrustCB wrote the first versions of the standard "SESIP" (Security Evaluation Standard for IoT Platforms) and now operates a SESIP scheme to enable implementers of IoT platforms to demonstrate that a specific Target of Evaluation (TOE) provides specific functionality and services for use by an IoT application than can be installed on the platform and to protect platform assets against state-of-the-art attackers.



An IoT Platform is the hardware/software providing an operating environment for an IoT Application. IoT Platforms parts can be developed and evaluated separately, for example by evaluating the cryptographic library, an OS, hardware, and then combining them. In terms of the Common Criteria, the IoT Platform (part) identified in the ST is our TOE.

An IoT Application is the software running on the IoT Platform adding domain-specific functionality. An IoT Platform together with an IoT Application in total form an IoT Product, providing the user with a complete functionality. From the platform point of view, there is only one IoT Application, even if this IoT Application is separated in many different applications parts from the IoT Application developer point of view.

The primary source of information and the TrustCB scheme procedures and documents can be found at https://trustcb.com/iot/sesip/.

1.2 SESIP Contact details

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

1.3 SESIP TOE-type overview

Security functionality provided by a platform is expressed using the SESIP catalogue. Commonly provided set of functionality are covered in SESIP profiles issued by TrustCB, such as ICA Telecom Level 3, IEC62443, Javacard, etc. It should be noted that, when available for a particular TOE type, the Security Target template must be used to produce the Security Target (e.g. the template "Security Target for Platform").

1.4 SESIP Process

The SESIP Protection Profiles contain mandatory application notes that are to be applied in the performance of the CC assurance activities on a given TOE. These application notes allow for optimizations in the assurance activities approved by TrustCB.

Prior to the submission phase, the developer has contracted a licensed evaluation lab and together with that lab has filled in the application form. A signed copy of the application form, together with a draft Security Target, must be sent by email to sesip@trustcb.com.

In the case of application for a SESIP1 certification, the signed application form ([SESIP1-AF]) includes a quotation, as these certifications are a fixed price. In that instance, TrustCB will issue an invoice for payment of the certification fee upon acceptance of the application.

In the case of application for a SESIP2-SESIP5 certification, TrustCB will respond with a quotation for certification for acceptance by the certification sponsor. Upon receipt of acceptance of the quotation, TrustCB will issue an invoice for the payment of the certification fee.

The evaluation phase can commence once that quotation has been accepted and the certification fee paid.

1.4.1 Evaluation Phase

The default process for evaluations under the SESIP scheme is for a two stage Evaluation Phase.

1.4.1.1 Evaluation Review Phase 1

In the first evaluation review phase the evaluator must apply all security assurance requirements specified in the Security Target that relate to gaining sufficient understanding of the TOE and associated development/manufacturing procedures to support the development of the test and lifecycle verification plans, starting with the ASE: Security Target evaluation assurance requirements.

The Security Target evaluation needs to be performed first as this provides the baseline of all other evaluation activities to be applied for the TOE. The ASE requirements to be applied will depend on the SESIP assurance level claimed in the ST, from a simplified Security Target at SESIP1 to a full (traditional) CC Security Target at SESIP5. The results of the ASE activity should be documented directly in the ASE chapter of the ETR. The methodology for ASE_REQ.3 as described in [SESIP] must be applied.

The other evaluation activities that should be applied in this phase (depending on the SESIP assurance package claimed in the ST) are:

- ADV: Development – all ADV activities specified in the ST should be performed in Evaluation Review Phase 1. This includes source code analysis as required by any ADV_IMP requirement claimed, as there is no sampling of source code to be performed[1].
- AGD: Guidance documents – all AGD activities specified in the ST should be performed in Evaluation Review Phase 1 with the exception of those activities that relate to verification of the guidance provided through use of the product. That activity may be delayed until Evaluation Review Phase 2 if the Evaluator has not received the TOE sample(s) in Evaluation Review Phase 1
- ALC: Life-cycle support – Those ALC activities relating to the analysis of the lifecycle support procedures should be performed in Evaluation Review Phase 1. If the ALC requirements necessitate the evaluator confirm these processes and procedures are applied, then the plan for verification of the procedures is produced in Evaluation Review Phase 1.
- ATE: Tests – Where the ATE requirements oblige the Evaluator to perform independent functional testing, the Evaluator should devise the functional test plan as part of the Evaluation Review Phase 1, building on the understanding of the TOE and its development/manufacture gained from

[1] So there is no need for agreement of the selected source code sample between the Evaluator and Certifier

the conduct of the ASE, ADV, AGD and ALC activities. In addition, if SESIP5 is claimed, those ATE activities relating to the analysis of the developer testing should be performed in Evaluation Review Phase 1. The evaluator should also factor the developer testing performed into the development of the test plan, to focus on any functionality/mechanisms that have not been sufficiently demonstrated in the developer testing evidence.

- AVA: Vulnerability Assessment – During Evaluation Review Phase 1 the evaluator will perform the appropriate rigour of vulnerability analysis, taking into account all appropriate materials and knowledge gained in performing the other Evaluation Review Phase 1 activities. Resulting from this analysis the Evaluator will document the analysis and prepare the penetration test plan.

The reports of these activities are presented by the Evaluator in Evaluation Meeting #1, and agreed by the Certifier before the evaluation proceeds to Evaluation Review Phase 2. The typical inputs for the Evaluation Meeting #1 are listed in the application forms [SESIP1-AF] and [SESIP2-5-AF].

1.4.1.2 Evaluation Review Phase 2

The second evaluation review phase is focused on the evaluator reporting of the results of executing the agreed plans, which were an output of Evaluation Review Phase 1, namely:

- Functional test plan
- Penetration test plan
- Lifecycle verification plan

All results are collated and reported in the Evaluation Technical Report.

The results are then presented by the Evaluator in Evaluation Meeting #2, and agreed by the Certifier. Any comments raised in EM#2 are addressed in the final ETR, which is delivered to the Certifier for approval. Once approval of the ETR has been granted by the Certifier the Evaluation Review phase is complete, and the Certification phase can commence.

1.4.1.3 Composition aspects: re-use of other certificates

A certificate for the underlying hardware platform can be re-used only if it is a valid Common Criteria certificate against [HW-PP], under the SOGIS MRA at EAL4+AVA_VAN.5 or higher. The scope of the underlying certificate must include the: DES, AES and RNG functionality. The hardware platform certificate shall be at most 1.5 years old at the time of issuance of the ETR.

A certificate for the underlying platform as a Java Card platform can be re-used only if there is a valid Common Criteria certificate against Java Card System PP [JC-PP], under the SOGIS MRA at EAL4+AVA_VAN.5 or higher. The Java Card Platform certificate shall be at most 1.5 years old at the time of issuance of the ETR.

All sites involved in the development and production must be audited in compliance to the applicable requirements from those Common Criteria. The site audits shall be at most 2 years old at the time of issuance of the certificate.

1.4.2 Certification Phase

The certificate validity period for SESIP certificates is three (3) years from the ETR issue date. This period can be extended by another 1.5 years (18 months), if required, is accordance with the rules defined in [TrustCB_SP] "*Certificate validity*".

1.5 SESIP Reference Materials

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

Table 1 SESIP Documents

Security Evaluation Standard for IoT Platforms	1.3	[SESIP]
TrustCB SESIP Application Form (SESIP1)	v1.3	[SESIP1-AF]
TrustCB SESIP Application Form (SESIP2-5)	v1.3	[SESIP2-5-AF]