TRUST AND VERIFY

TrustCB Scheme Procedure for SESIP

Version 2.6

TRUST AND VERIFY

Contents

1 TrustCB SESIP scheme

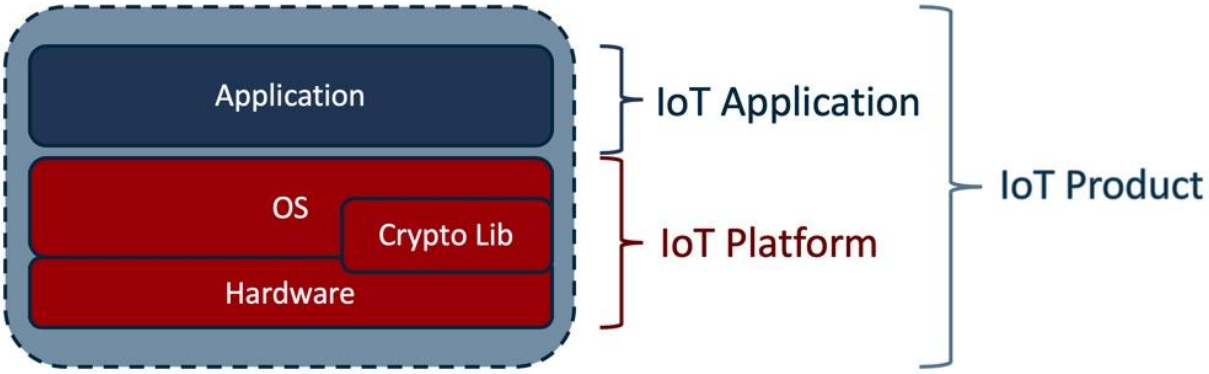
This document, as an annex to TrustCB Shared Scheme Procedures [TrustCB_SP], details the scheme specific details for the TrustCB SESIP scheme.

1.1 Introducing the TrustCB SESIP scheme

TrustCB wrote the first versions of the standard "SESIP" (Security Evaluation Standard for IoT Platforms), which was adopted and issued for Public Release by GlobalPlatform as GP_FST_070. It is now also adopted by CEN and CENELEC as European Standard EN 17927.

TrustCB operates a SESIP certification scheme that can be used to certify an IoT platform referencing either the GP_FST_70 publication of the SESIP methodology or the EN 17927 publication of the SESIP methodology. Both of these SESIP specific methodologies have are based on Common Criteria [CC][CEM].

The TrustCB SESIP scheme enables developers of IoT platforms and applications (IoT Product) to certify that their defined Target of Evaluation (TOE) provides stated functionality and services to protect platform assets against state-of-the-art attackers.



An IoT-Platform, defined as Connected Platform in [SESIP], 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, defined as Connected Application in [SESIP], 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 (Connected 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 TrustCB SESIP Contact details

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

1.3 TrustCB SESIP TOE-type overview

Security functionality provided by a platform is expressed using the SESIP catalogue. Commonly provided sets 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 TrustCB 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.

1.4.1 Submission Phase

Prior to the submission phase, the developer shall have contracted a licensed evaluation lab and, together with that lab, have filled in the TrustCB SESIP application form [SESIP-AF]. A signed copy of the application form, together with a draft Security Target for the TOE, must be sent by email to sesip@trustcb.com.

Note a SESIP optimised Security Target template is available on the TrustCB SESIP scheme webpage, [SESIP-ST]. Use of the template is not mandatory.

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.

1.4.2 Evaluation Phase

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

1.4.2.1 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

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

- 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 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 form [SESIP-AF].

1.4.2.2 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.

1.4.2.3 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.

1.4.3 Certification Phase

The certificate validity period for SESIP certificates is five (5) years from the ETR issue date. This period can be extended by another two (2) years, if required, is accordance with the rules defined in [TrustCB_SP] "*Certificate maintenance*".

NOTE: Certificates issued under the previous two-year SESIP validity period and that are still valid within that validity period may be eligible to be extended to five years on application to TrustCB.

1.5 Certification Marks and Logos

The TrustCB issued certificate for a compliant product evaluated by a laboratory that is GlobalPlatform (GP) logo licensed will include a GP SESIP logo (Certification Mark). The logo will be specific to the level of assurance attained by the product. SESIP logo usage is irrespective of whether the referenced SESIP standard for the evaluation is the GlobalPlatform GP_FST_070 or the CEN CENELEC EN 17927.

The TrustCB Application Form for SESIP, section 1.3.3, further explains the logos used on certificates. The evaluating lab is required to positively confirm, for each submitted SESIP application, that they are GlobalPlatform logo licensed and compliant with any additional GlobalPlatform rules for logo usage. Further details of this confirmation may be found in the application form.

The TrustCB issued certificate for a compliant product evaluated by a lab that is not GlobalPlatform (GP) logo licensed will not include the GlobalPlatform SESIP logo. The applied SESIP level will nevertheless be clear in the certificate.

Note: All laboratories performing evaluations for the TrustCB SESIP scheme must be licensed by TrustCB irrespective of their GP logo usage status. The list of currently licensed labs can be viewed at the TrustCB website, https://www.trustcb.com/about-us/labs/. For further details, contact licensing@trustcb.com.

1.6 References

Title	Reference
TrustCB SESIP Application Form	[SESIP-AF] [2]
SESIP Security Target template	[SESIP-ST] [2]
TrustCB SESIP Scheme Interpretation 1: Re-use of CC certification results	[SESIP-INT1] [2]
Technical requirements and scheme methodology: [5]	
either GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070 or EN 17927:2023 : Security Evaluation Standard for IoT Platforms (SESIP). An effective methodology for applying cybersecurity assessment and re-use for connected products	[SESIP] [3 or 4]
TrustCB Shared Scheme Procedures	[TrustCB_SP][1]

[1] https://www.trustcb.com/about-us/policies-procedures/

[2] https://trustcb.com/iot/sesip/

[3] https://globalplatform.org/specs-library/sesip-methodology/

[4] refer to national CEN standards body

[5] Based on Common Criteria (CC) and Common Evaluation Methodology (CEM)

Note: document versions as stated in the application form, section A.1.

Annex A Revision History

Version	Date	Description of change
2.2	2022-01-25	Updated to reflect modifications to SESIP Application Form
2.3	2022-08-31	Note added to refer to the application form for current versions of the documents defining the TrustCB SESIP scheme
2.4	2024-12-01	Updated to reference EN17927
2.5	2025-05-07	1.1 Clarification that either GP_FST_70 or EN 17927 may be referenced in a TrustCB SESIP certification 1.5 Clarification that the GP SESIP logo can only be used on certificates where the lab is GP logo licensed, with associated references to the Application Form
2.6	2026-01-30	1.4.3 Certificate validity period changed from two years to five years.