TRUST AND VERIFY

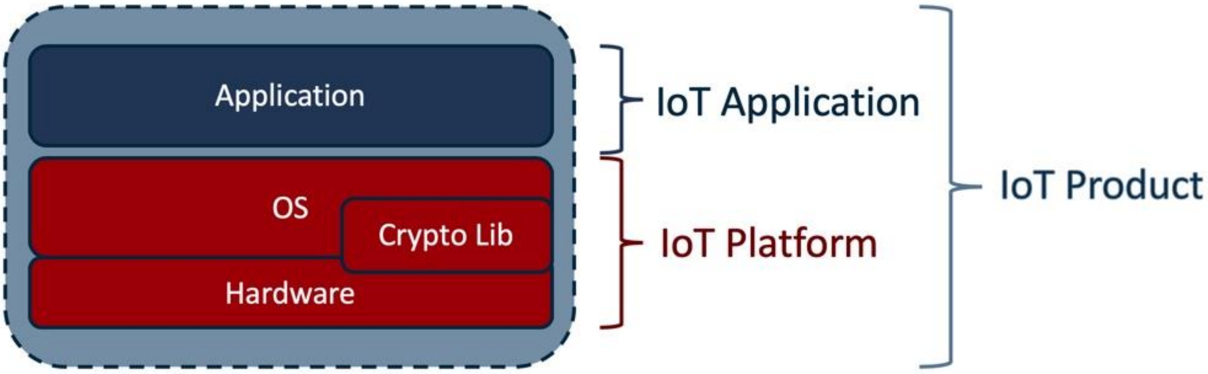
TrustCB SESIP Scheme Procedures

Version 1.3.1

Contents

1 Scheme introduction

TrustCB has operates SESIP (Security Evaluation Standard for IoT Platforms) 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.

This document describes the security evaluation and certification process to be followed.

1.1 TOE-type overview

This scheme applies to a hardware/software TOE providing an operating environment for an IoT Application. The functional and assurance requirements must all be taken from [SESIP].

1.2 Intended audience

This document is publicly available and is mandated for the following involved parties:

1. Scheme owner
2. Developer (Sponsor)
3. Evaluator (Lab)
4. Certifier (TrustCB)

1.3 Terminology

The terminology of RFC 2119 is used in this document, as follows:

- "shall" or "must" indicates mandatory requirements

- "should" indicates a strong recommendation, deviation of which must be discussed with and approved by the scheme
- "can" or "may" denotes an option

1.4 Contact details

All requests or enquiries related to the security evaluation should be addressed by email to: SESIP@trustcb.com.

2 SESIP overview

This section provides an overview of the Security Evaluation Standard for IoT Platforms (SESIP), including the objectives of the scheme, roles and responsibilities for all parties, and a high-level description of the evaluation process.

2.1 Objective

The objectives of the scheme are:

- To provide a trustworthy assessment of the security of the IoT platforms, such that this can be re-used in fulfilling the requirements of various commercial product domains.
- To provide a clearly defined secure operating environment for an IoT Application, which together form an IoT Product.

This scheme leverages and streamlines the CC evaluation process by focusing on specific threats that IoT Platforms are exposed to, in the context of industry standard designs and processes.

To maintain a consistent and state-of-the-art level of assurance, experienced evaluation labs are appointed to perform the evaluation activities.

A dedicated certification body (TrustCB-SESIP) is appointed to perform the certification activities.

2.2 Roles

There are four main roles in this scheme, as follows:

- **Scheme owner**: operator of SESIP (in this case TrustCB).
- **Developer**: organisation responsible for submitting the TOE for evaluation and certification.
- **Evaluator**: Lab evaluating the TOE
- **Certifier**: Certification Body certifying the work of the Evaluator

The responsibilities associated with each role are identified in the following subsections.

2.2.1 Scheme Owner (TrustCB)

TrustCB, intending to protect the trustworthy and re-usable assessment of the security of the IoT, as owner of this security scheme:

- Shall maintain the scheme documentation and procedures.
- Shall maintain the list of current certificates.
- Shall accredit the certifier.
- Shall maintain the definitive list of accredited evaluating laboratories and the certification body.
- Shall make final decisions on any discussions and conflicts within the scope of this scheme.

2.2.2 Developer

The developer:

- Shall arrange any contracts with the evaluator and certifier, including payment for the activity and confidentiality requirements. The developer shall support the independence and impartiality of the evaluator and certifier. The timing and amount of payment must not be dependent on the evaluation/certification outcome. The evaluator and certifier must have full access to relevant developer and evaluation evidence.

- Shall apply for (re-)certification under the scheme for a specific product, by filling out the application form and sending it to the certifier.
- Shall arrange that any evidence necessary is made available to the evaluator (and if necessary the certifier). This should include samples of the product, the guidance documentation of the product, the site audit result(s) (for CC: site certificates or Site-Audit Reuse Sheets/STAR reports), the ETR for composition (for CC certified hardware/platforms), and any underlying hardware/platform documentation required.
- Shall NOT claim nor imply that a product is certified, before issuance of the certificate by the certifier for that exact product.
- Shall NOT claim nor imply that a product is certified after expiry or revocation (suspension, withdrawal or termination) of the certificate.
- Shall inform the evaluator of any information (including known possible weaknesses and attacks) relevant to the evaluation of the TOE.
- Shall inform all parties (including the scheme owner) immediately if any vulnerability of the TOE becomes known during the validity period of the certificate. The developer may discuss possible vulnerabilities with the evaluator and certifier to determine whether they are actual vulnerabilities prior to contacting the scheme owner. Such discussion shall delay informing the scheme owner by at most 30 days from the moment they became known to any party. Any unresolved discussion shall be taken to the scheme owner.
- Shall archive the developer evidence for at least three years after expiry of the certificate.
- Shall, in case of dispute over whether a product sold as the certified product is genuinely the certified product, support the verification against the stored evidence and samples, as well as any further fact finding required to resolve this.
- Should inform the scheme owner of potential improvements of the scheme documentation, including the security analysis.

2.2.3 Evaluator

The evaluator is an accredited ISO/IEC17025 laboratory, licensed by the certifier for to perform evaluation activities. ISO/IEC15408 and ISO/IEC18045 must be included in scope of the ISO/IEC17025 accreditation.

The evaluator is responsible for performing all evaluation activities (including vulnerability analysis and security testing) needed to ensure that the product protects the IoT Platform assets against current state-of-the-art attacks up to the claimed SESIP level.

The evaluator:

- May assist the developer in the application process.
- Shall ensure the evaluator’s independence of the developer, the certifier and the scheme owner.
- Shall determine whether the developer evidence provided meets the requirements as set in the scheme documentation.
- Shall provide the certifier with reports from each evaluation review phase (e.g. report of developer self-assessment analysis, test plan and vulnerability analysis).
- May await approval of reports by the certifier prior to proceeding to the next evaluation review phase (proceeding without approval runs a risk of subsequent evaluation activities not being judged sufficient, at the potential time and costs risk of the evaluator/developer).
- Shall inform the developer of the fact that reports from an evaluation review phase have been submitted to the certifier.
- Shall perform all evaluation activities, including appropriate (depending on the IoT Platform assurance package claimed) vulnerability analysis and security testing, needed to ensure that the

samples of the product protect the IoT Platform assets against the current state-of-the-art attacks as defined in the scheme documentation specified in [SESIP_DL].

- Shall answer the questions from the certifier.
- Shall provide the developer and the certifier with the ETR describing the evaluation activities and conclusion that the product meets the requirements.
- May provide the developer with extra details on the test results outside the scope of this process.
- Shall inform all parties immediately if any vulnerability of the TOE becomes known during the validity period of the certificate. The developer may discuss possible vulnerabilities with the evaluator and certifier to determine whether they are actual vulnerabilities prior to contacting the scheme owner. Such discussion shall delay informing the scheme owner by at most 30 days from the moment they became known to any party. Any unresolved discussion shall be taken to the scheme owner.
- Shall archive the developer evidence, evaluation evidence and samples for at least three years after expiry of the certificate. Note that the raw measurement data is not considered evaluation evidence and hence is excluded from the archiving requirement.
- Shall, in case of dispute over whether a product sold as the certified product is genuinely the certified product, perform the verification against the stored evidence and samples.
- Should inform the scheme owner of potential improvements of the scheme documentation, including the security analysis.

2.2.4 Certifier (TrustCB)

The certifier (TrustCB) is a dedicated certification body accredited by the scheme owner for the certification role. The certifier is responsible for determining whether sufficient assurance has been given that the product protects the IoT Platform assets against current state-of-the-art attacks up to claimed SESIP level, and issuing a certificate to that effect.

The certifier:

- Shall maintain its impartiality.
- Shall license the evaluating laboratories.
- Shall ensure the certifier’s independence of the developer and the evaluator involved in this project.
- Shall verify the certification application form meets the requirements of the scheme documentation, and shall issue an intended certification ID.
- Shall determine whether the results of the evaluation activities reported by the evaluator will likely satisfy the requirements of the scheme documentation.
- Shall inform the developer and the evaluator of the approval of delivered evaluation reports.
- Shall verify that the ETR meets the requirements of the scheme documentation.
- Should ask questions to the evaluator if it is not clear to the certifier from the evaluation reports whether sufficient assurance has been achieved.
- Shall determine whether sufficient assurance has been given that evaluation activities (including, where appropriate, vulnerability analysis and security testing) needed to ensure the product protects the IoT Platform assets against the current state-of-the-art attacks.
    - If the certifier determines sufficient assurance is given, the certifier shall send a certificate with the certification ID to the developer and the evaluator.
    - If the certifier determines that insufficient assurance is reached even after questions to the evaluator, the certifier shall inform the developer and the evaluator of this verdict.
- Shall in all cases inform both the developer and the evaluator of the verdict.

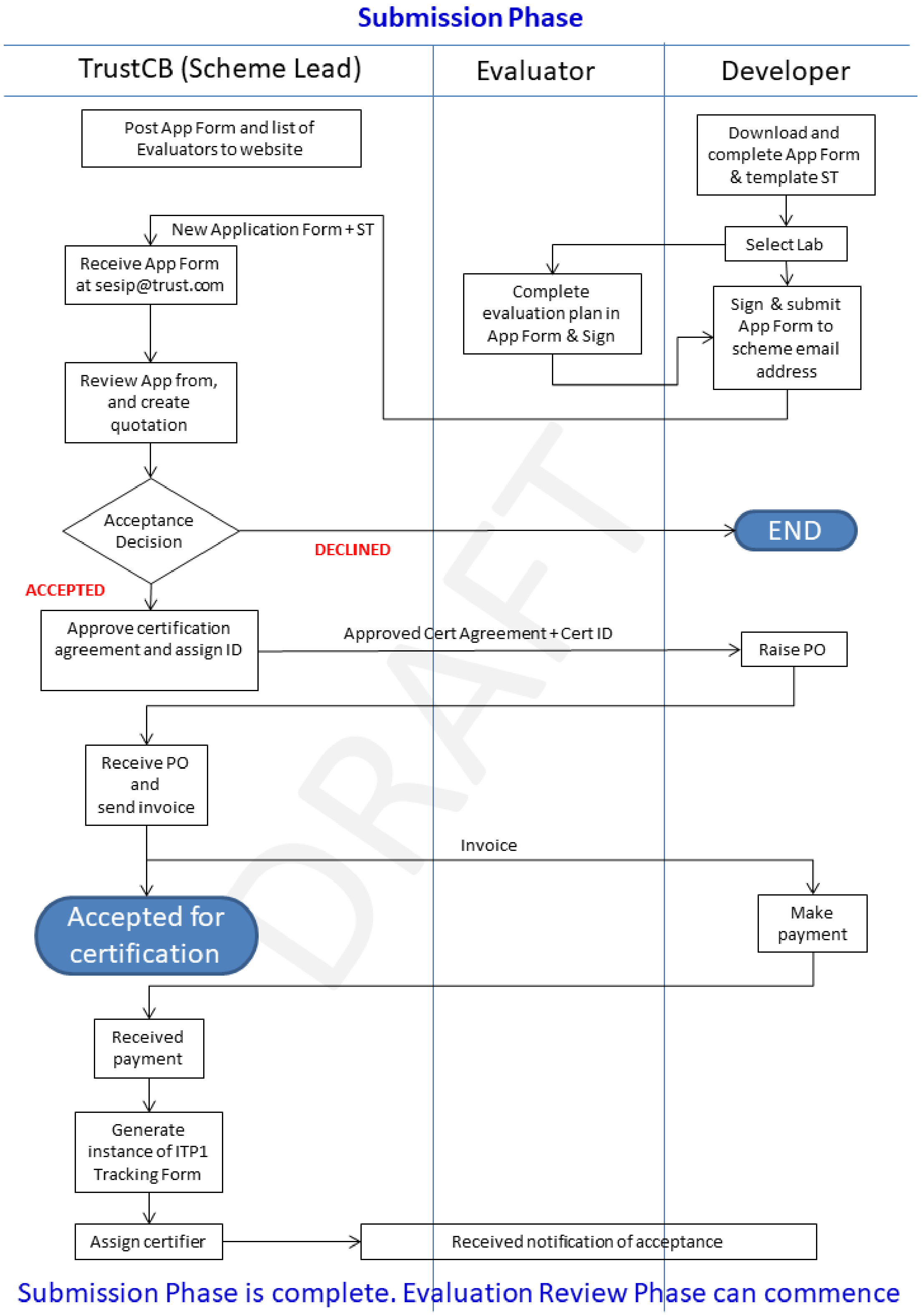
- Shall inform all parties immediately if any vulnerability of the TOE becomes known during the validity period of the certificate. The developer may discuss possible vulnerabilities with the evaluator and certifier to determine whether they are actual vulnerabilities prior to contacting the scheme owner. Such discussion shall delay informing the scheme owner by at most 30 days from the moment they became known to any party. If the certifier has reasonable suspicion during the assessment that the product fails to protect the assets against now current state-of-the-art attacks, the certificate should be suspended. If the certifier determines that the product fails to protect the assets against now current state-of-the-art attacks, the certificate shall be revoked. Any discussion unresolved after at most 30 days shall be taken to the scheme owner.
- Shall, in case of dispute over whether a product sold as the certified product is genuinely the certified product, confirm or deny the verification against the stored evidence and samples by the evaluator.
- Shall inform the scheme owner of potential improvements of the scheme documentation, including the security analysis.

3 Process

3.1 Submission phase

In the submission phase, the developer arranges the application and any contracts with the evaluator. When successfully completed, the evaluation and certification process has started and the intended certification ID is communicated.

Figure 1 Submission phase steps


Submission Phase
TrustCB (Scheme Lead)
Evaluator
Developer
Post App Form and list of Evaluators to website
Download and complete App Form & template ST
Select Lab
New Application Form + ST
Receive App Form at sesip@trust.com
Complete evaluation plan in App Form & Sign
Sign & submit App Form to scheme email address
Review App from, and create quotation
Acceptance Decision
DECLINED
END
ACCEPTED
Approve certification agreement and assign ID
Approved Cert Agreement + Cert ID
Raise PO
Receive PO and send invoice
Invoice
Accepted for certification
Make payment
Received payment
Generate instance of ITP1 Tracking Form
Assign certifier
Received notification of acceptance
Submission Phase is complete. Evaluation Review Phase can commence

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”).

If the certifier determines that an adaptation of the existing scheme procedures or evaluation methodology is needed because the TOE type, scope or other aspects don’t match, or for other reasons additional oversight by the certifier be required, a kick-off meeting and/or other additional meetings may be required.

3.2 Evaluation Review phase

The Evaluator is responsible for delivering the evaluation reports which record the results of the evaluation activities. These reports are reviewed by the Certifier and the review comments communicated to the evaluator in review reports and discussed in an evaluation meeting where applicable. The Evaluator is responsible for addressing the Certifier review comments as well as recording minutes of evaluation meetings and tracking action items arising from evaluation meetings. The meetings may be face-to-face meetings, electronic meetings or virtual meetings, as determined by the Certifier and reflected in the Evaluation Work Plan.

When all Review Report comments have been addressed and any action items closed, the Certifier shall notify the evaluator of acceptance of the evaluation results recorded in the delivered evaluation reports.

The Certifier shall prepare the recommendation for certification decision upon receipt of all evaluation reports, and at that point shall transition to the Certification Phase to receive the Evaluation Technical Report.

There are two Evaluation Review Phases by default. Depending on the evaluation approach agreed during the Submission phase these phases may be combined such that the Evaluator reports are only delivered to the Certifier once the Evaluator activities in both phases have been performed.

The flow of actions for each phase is the same, as show in Figure 2.

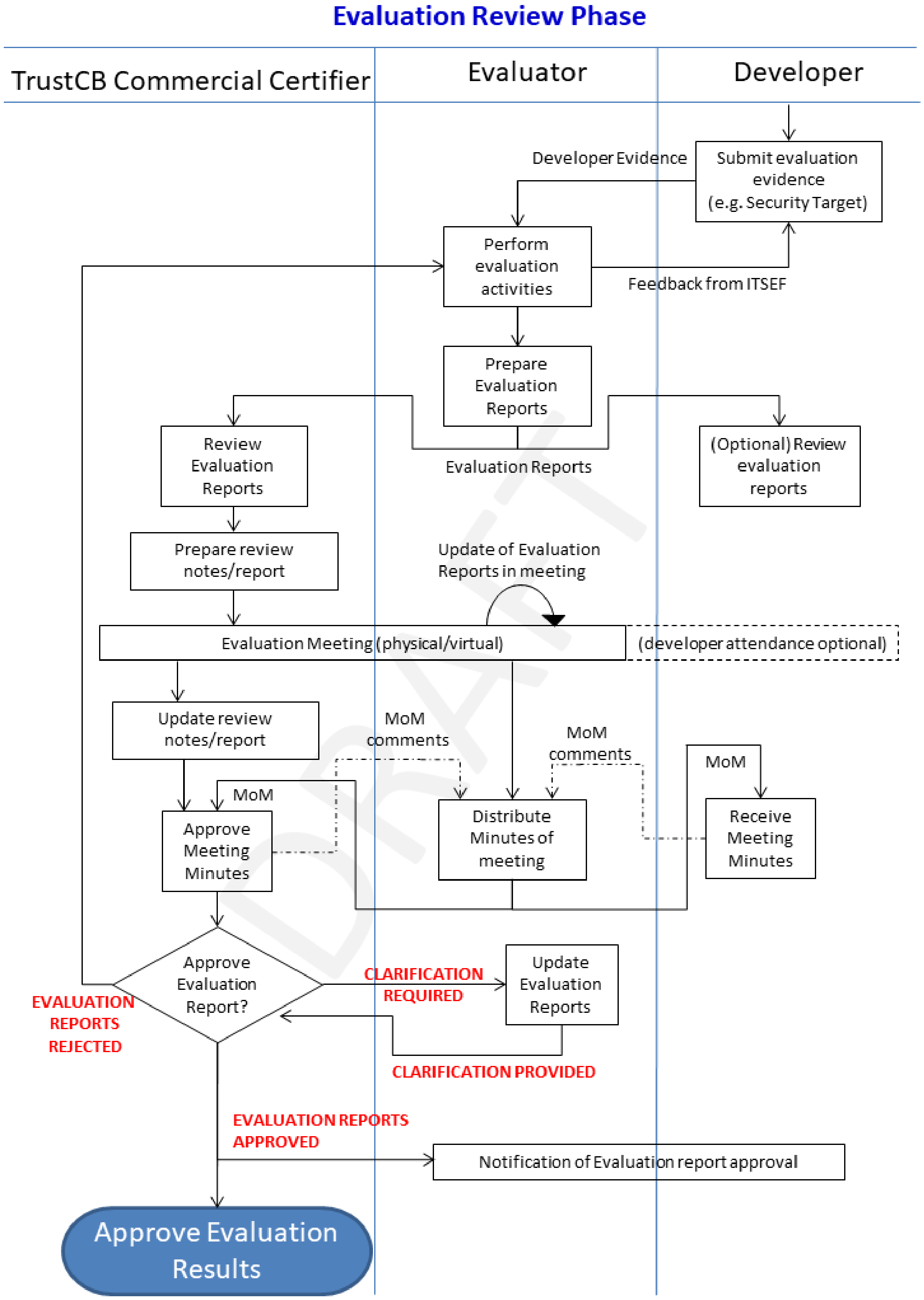
3.2.1 Evaluation Activities

There are five sets of Common Criteria assurance packages defined in [SESIP], which are suitable to evaluate IoT platforms or parts thereof, namely, SESIP1, SESIP2, SESIP3, SESIP4 and SESIP5. These assurance packages contain some CC Part 3 extended assurance requirements (ASE_REQ.3 and ADV_IMP.3[1]) and incorporate refinements to some of the CC Part 3 conformant assurance requirements include in the packages.

The scheme documentation, specified in [SESIP_DL], provides all methodology and application notes that are to be applied in the performance of the CC assurance activities on a given TOE. The evaluation methodology to be applied is described in [CEM] unless otherwise indicated in this document.

[1] **Note**: the ASE_REQ.3 and ADV_IMP.3 are not hierarchical to all other components within their families.

Figure 2 Evaluation review steps


Evaluation Review Phase
TrustCB Commercial Certifier
Evaluator
Developer
Submit evaluation evidence (e.g. Security Target)
Developer Evidence
Perform evaluation activities
Feedback from ITSEF
Prepare Evaluation Reports
Review Evaluation Reports
Evaluation Reports
(Optional) Review evaluation reports
Prepare review notes/report
Update of Evaluation Reports in meeting
Evaluation Meeting (physical/virtual)
(developer attendance optional)
Update review notes/report
MoM comments
MoM comments
MoM
MoM
Approve Meeting Minutes
Distribute Minutes of meeting
Receive Meeting Minutes
Approve Evaluation Report?
CLARIFICATION REQUIRED
Update Evaluation Reports
EVALUATION REPORTS REJECTED
CLARIFICATION PROVIDED
EVALUATION REPORTS APPROVED
Notification of Evaluation report approval
Approve Evaluation Results

Iterate phase for next round of evaluation activities or go to the Certification Phase if Evaluation Results Approved includes the final ETR.

3.2.2 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[2].
- 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 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 [SESIP2-5_AF].

3.2.3 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.

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

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.

3.2.4 Evaluator Reporting

The reporting from the evaluator to the certifier is intended to provide the certifier with sufficient information to determine that enough assurance has been gained, without disclosing more proprietary knowledge than is necessary. For this reason, the industry standard Common Criteria ETR is used, as this is a common format of documents already exchanged between these stakeholders in the course of CC. The ETR shall include (by reference) all certificates, Shared Evaluation Reports, Shared Audit Reports and other evaluation evidence used in the production of the ETR.

Note that this document is considered to contain sensitive information about the security and potential security weaknesses of the product, and therefore shall be kept secret between the parties involved in the certification of a given TOE.

The evaluator shall explicitly state:

- The version of the "Security Evaluation Standard for IoT Platforms" ([SESIP]) document applied
- The evaluator has determined that the product meets all requirements of [SESIP].
- In the case "Pass" verdicts have been assigned to all evaluation activities, the evaluator advises the certifier to certify the product, by concluding that the evaluator "has determined that the product meets the requirements of SESIP and has the appropriate level of assurance for the claimed SESIP assurance level that the product protects the IoT Platform assets against state-of-the-art attackers at the time of issuance of this report".

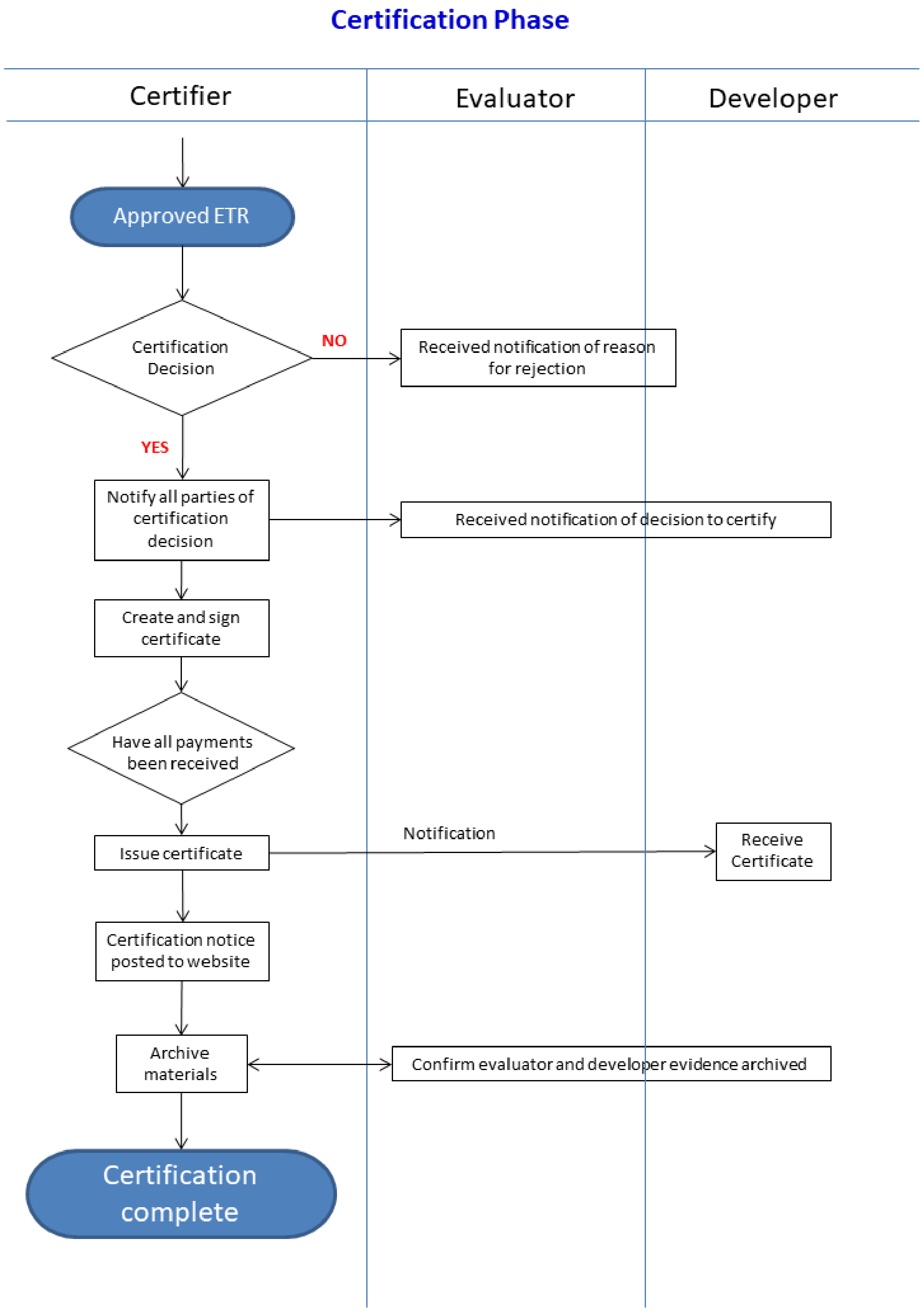
3.3 Certification phase

This phase starts with the delivery of the Evaluation Technical Report, together with any additional reports (e.g., ETRfC, STAR, ST-Lite), which are required to facilitate the sharing of evaluation results between Certifies and Evaluators from different evaluation labs and certification bodies.

The Certifier shall review these reports and shall record all the review comments in Review Reports, which are then sent to the Evaluator. When the Evaluator has satisfactorily addressed all comments the Certifier shall approve the ETR (and associated reports) and shall prepare the certificate. The recommendation for certification decision reached by the Certifier is documented in the conclusion of the Review Reports (for the ETR and associated reports).

The Certificate shall be published on the TrustCB scheme website (unless the developer explicitly requested otherwise in the application form), and notification of the publication shall be sent to the Developer and Evaluator. A copy of the certificate shall be sent to the Developer.

Figure 3 Certification phase steps


Certification Phase
Certifier
Evaluator
Developer
Approved ETR
Certification Decision
NO
Received notification of reason for rejection
YES
Notify all parties of certification decision
Received notification of decision to certify
Create and sign certificate
Have all payments been received
Issue certificate
Notification
Receive Certificate
Certification notice posted to website
Archive materials
Confirm evaluator and developer evidence archived
Certification complete

3.3.1 Certificate validity

A new certificate is valid for a period of 2 years from the ETR issue date.

This period can be extended by another 2 years (24 months), if required. To extend the validity period, a renewal evaluation must be performed and, if successful, the certificate will be re-issued with an extended validity of another 2 years. Each time (renewal) evaluation and certification is performed, the ETR and the certificate showing sufficient resilience against current state-of-the-art attacks must be provided.

There is no difference in evaluation deliverables for a first evaluation or a renewal evaluation.

The renewal certificate should be issued before the expiry date of the previous certificate for the certificate validity to be maintained. A Renewal certificate will be marked as such by additionally listing the newer issue date.

When the certified product is modified, a new certificate is required. If the same evaluator has performed an earlier evaluation of the same product or can determine the limited impact of changes in the product or underlying hardware/platform compared to a previously certified product, then the evaluator may internally re-use prior analyses and test results. This new certificate is valid for a period of 2 years.

The resulting analysis and testing shall, however, always show that the product protects IoT Platform assets against current state-of-the-art attacks.

All tests (re-)used for the analysis should not be more than 6 months older than the ETR’s issue date. Any tests (re-)used that are older than 6 months but no older than 12 months, may be (re-)used only with the explicit approval of the certifier. No tests used for the analysis should be more than 12 months older than the certificate’s issue date.

3.3.2 Composition aspects: re-use of other certificates

A certificate for the underlying hardware platform can be re-used only if it is a valid SESIP certificate for the same or higher assurance package or 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 functionality defined in the Security Target claimed for the composite TOE which relates to the underlying hardware platform. The hardware 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.

3.3.3 Certifier reporting

The certifier shall determine whether or not the requirements claimed in the Security Target for the given TOE have been met and hence a sufficiently high level of assurance has been obtained to ensure that the TOE protects IoT Platform assets against state-of-the-art attacks.

The certifier shall verify that the evaluator’s ETR meets all requirements set in the scheme documents ([SESIP_DL]).

If the certifier has decided that the product is shown to protect the assets sufficiently, and all requirements in the scheme documentation are satisfied, then the certifier shall issue the certificate using the TrustCB SESIP Certificate Template.

4 Reference Materials

The documents listed in Table 1 may have been cited in this document or used to obtain background information.

Table 4-1: Reference documents

Title	Source	Reference
ISO Standard 15408 Common Criteria for Information Security Evaluation	2	[CC]
Common Criteria and CEM version 3.1	2	[CEM]
Security Evaluation Standard for IoT Platforms	1	[SESIP]
SESIP Scheme Document List	1	[SESIP_DL]
TrustCB SESIP Application Form (SESIP2-5)	1	[SESIP2-5_AF]
TrustCB SESIP Application Form (SESIP1)	1	[SESIP1_AF]
Security IC Platform Protection Profile BSI-PP-0084-2014	3	[HW-PP]

Key:

1 = Available online from TrustCB SESIP scheme website (TrustCB SESIP)

2 = Available online from ISO standards website (www.iso.org) or Common Criteria Portal (commoncriteriaportal.org)

3 = Available online from BSI website (www.bsi.bund.de)