TRUST AND VERIFY

TrustCB Shared Scheme Procedures

Version 2.0

TRUST AND VERIFY

Contents

1 Introduction

Scheme Owners recognise the benefit of having an accredited third party Certification Body operating and managing their scheme.

Accredited against ISO17065 as a Certification Body by RvA, TrustCB offers such services to scheme owners of schemes that are based on Common Criteria (ISO15408) and CEM (ISO18045). As such, TrustCB operates and maintains a number of schemes on the behalf of scheme owners

This document describes the security evaluation and certification process to be followed for each of these schemes.

1.1 Schemes

TrustCB operates and maintains the following schemes, which are described in the Annexes of this document:

- MIFARE Scheme
- PSA Certified
- SESIP

Each scheme annex is posted to the scheme webpage on the TrustCB website https://trustcb.com.

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: <*scheme*>@trustcb.com, as defined in the Annexes of this document.

2 Security evaluation and certification overview

This section provides an overview of the generic security evaluation and certification scheme processes applied by TrustCB, including the general objectives of the schemes, roles and responsibilities for all parties, and a high-level description of the process.

2.1 Objective

As a certification body, who may be appointed by the scheme owner to perform certification activities, TrustCB operates schemes with the same high-level objectives:

- To protect the customer assets stored in certified products against threats from attack to a specified level of assurance, or state-of-the-art attackers.
- To protect the scheme brands by ensuring that no certified products available on the market are vulnerable to attack to a specified level of assurance by establishing sufficient confidence that the certified products protect the defined assets against threats from (state-of-the-art) attackers
- In the instances where TrustCB is running a scheme for a 3rd party scheme owner: To ensure that the scheme owner (who may also develop products) does not obtain proprietary information from other developers undergoing evaluation in that scheme.

This scheme leverages and streamlines the CC evaluation process by focusing on specific threats that the security products 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[1].

2.2 Roles

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

- **Scheme owner**: operator of the specified scheme.
- **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/external-organisation)

The Scheme Owner[2], intending to protect the customer assets and the scheme brand:

- Shall maintain the scheme documentation and procedures.
- Shall maintain the list of current certificates.
- Shall accredit the certifier.

[1] In the vast majority of cases the labs are licensed by TrustCB, as listed on www.trustcb.com/about-us/labs. In a few cases TrustCB may work with other labs at the request of the scheme owner.

[2] The Scheme Owner may be TrustCB or an external-organisation, as specified in the description of each scheme.

- 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.

In the case TrustCB are running scheme for 3rd party: The schemes operated by TrustCB are designed to keep proprietary information of the developer and evaluator away from a scheme owner who may also be the developer of products. Therefore, unless needed for conflict resolution, the evaluator and certifier shall not provide the scheme owner access to proprietary developer evidence or proprietary evaluation evidence, beyond the evidence submitted to the scheme owner in the due cause of the process. If there is a need to disclose proprietary developer or evaluation evidence to the scheme owner, prior explicit authorization by the developer or evaluator respectively shall be required.

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.

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

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 a test plan where required by scheme methodology.
- May await approval by the certifier prior to conduct of any testing required by the scheme methodology (proceeding without approval runs a risk of testing not being judged sufficient, at the potential time and costs risk of the evaluator/developer).
- Shall perform all vulnerability analysis and security testing when required by the scheme methodology to ensure that the samples of the product protect the assets against attack to a specified level of assurance, or state-of-the-art attackers or the current state-of-the-art attacks, as defined in the applicable scheme methodology (e.g., protection profile).
- Shall provide the certifier with reports from each evaluation phase
- May await approval by the certifier prior to proceeding to the next evaluation 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 phase have been submitted to the certifier.
- Shall perform all evaluation activities, including appropriate vulnerability analysis and security testing, needed to ensure that the samples of the product protect the assets against attack to a specified level of assurance or the current state-of-the-art attacks, as defined in the scheme methodology (which may include those defined in a scheme PP and/or template ST.
- 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 (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, 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

The certifier is a dedicated certification body accredited by the scheme owner for the certification role: TrustCB. The certifier is responsible for determining whether sufficient assurance has been given that the product protects the defined assets against attack to the specified level of assurance, and issuing a certificate to that effect, without disclosing proprietary information of other developers to scheme owner.

Note that the certifier makes this critical decision on behalf of the scheme owner, because the scheme owner will normally copy this decision without further discussion.

The certifier:

- Shall maintain its impartiality.
- Shall license the evaluating laboratories[3].
- 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 any proposed test plan of the evaluator (required by the scheme methodology) will likely provide sufficient assurance in testing.
- Shall inform the developer and the evaluator of the approval of any such test plan.
- 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 whether sufficient assurance has been achieved.
- Shall determine whether sufficient assurance has been given that all vulnerability analysis and security testing needed to ensure the product protects the assets from attack to a specified level of assurance or against state-of-the-art attackers, as defined by the scheme methodology.
    - If the certifier determines sufficient assurance is given, the certifier shall send a positive certification decision and, where applicable, a certificate with the certification ID to the developer, the evaluator and the scheme owner.
    - 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 certification verdict.
- 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. If the certifier has reasonable suspicion during the assessment that the product fails to protect the assets now against attack to a specified level of assurance or current state-of-the-art attacks, the certificate should be suspended. If the certifier determines that the product fails to protect the assets now against attack to a specified level of assurance or 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.

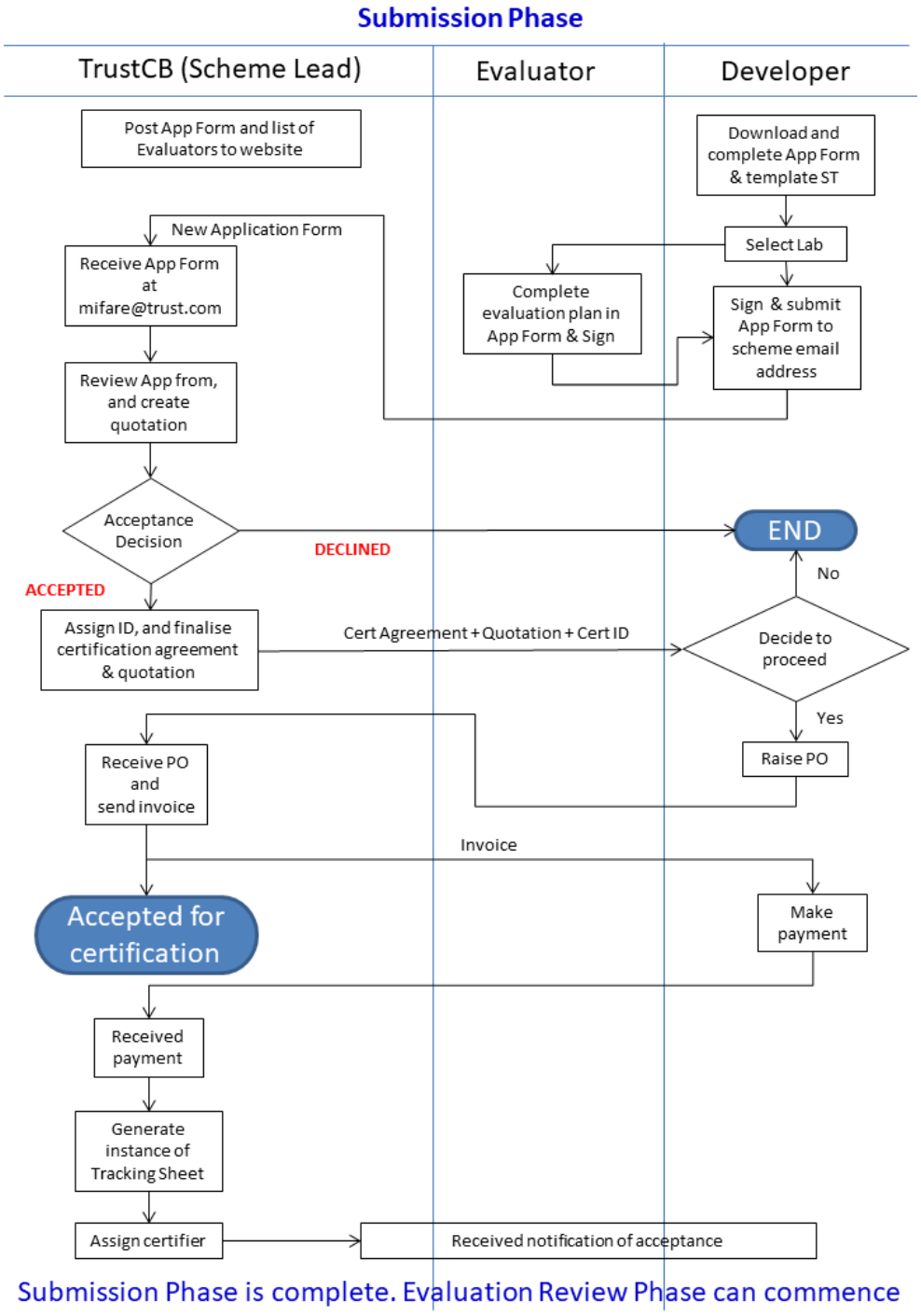
[3] With the exception of the instances when a Scheme Owner requires TrustCB to accept evaluation results from an evaluating laboratory of the scheme owner's chosing.

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



If the certifier or scheme owner 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 kickoff meeting and/or other additional meetings may be required.

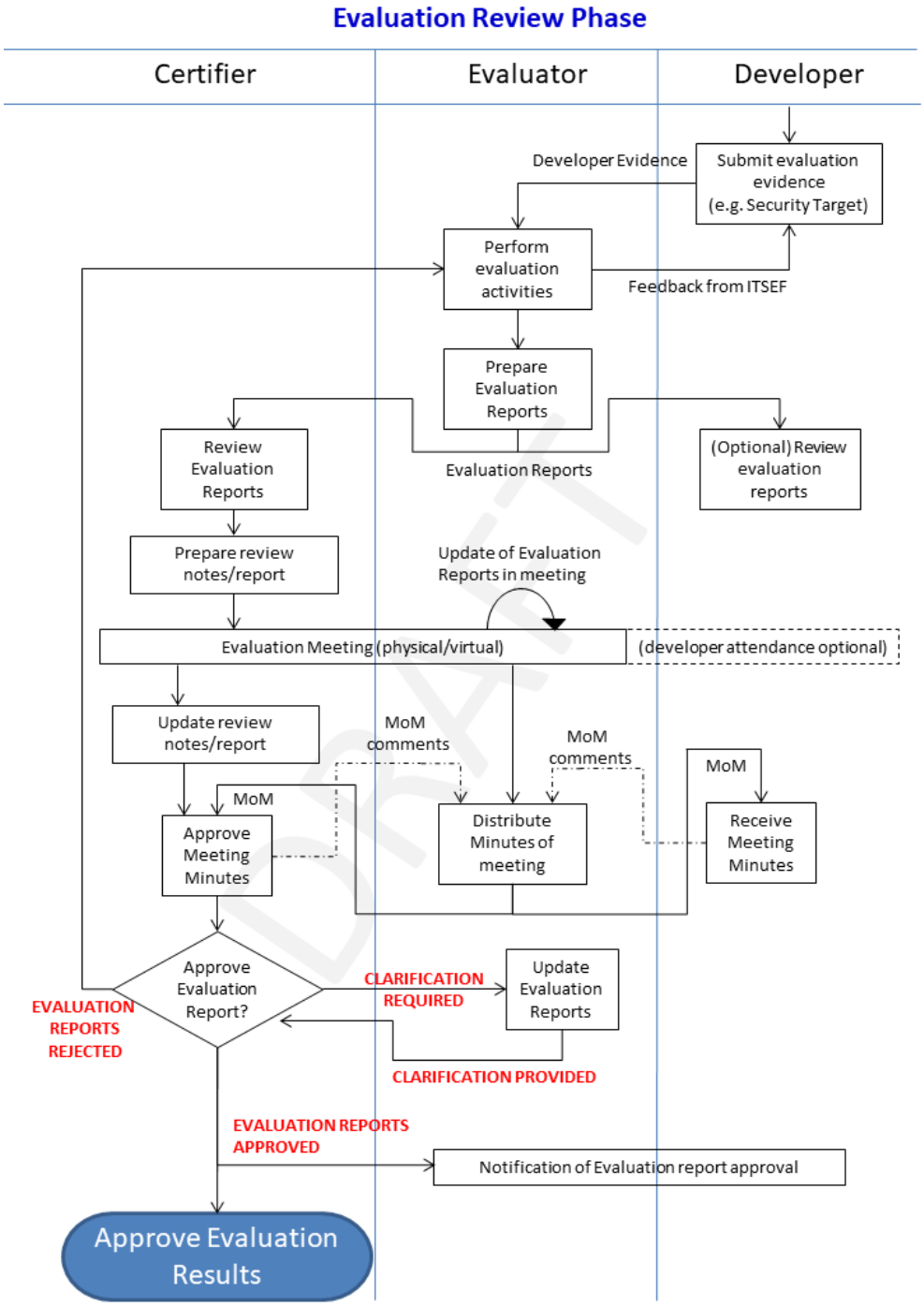
The submission process may be simplified, as specified in evaluation methodology, for those certification tasks at a lower level of assurance. This simplification is typically applied when the evaluation activities are limited to an assessment of a developer self-assessment of the product (e.g. completed questionnaire).

3.2 Evaluation 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 if applicable). The Evaluator is responsible for recording minutes of evaluation meetings and tracking action items arising from evaluation meetings.

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.

Figure 2 Overview of Evaluation phase activities



3.2.1 Decomposition of Evaluation Phase

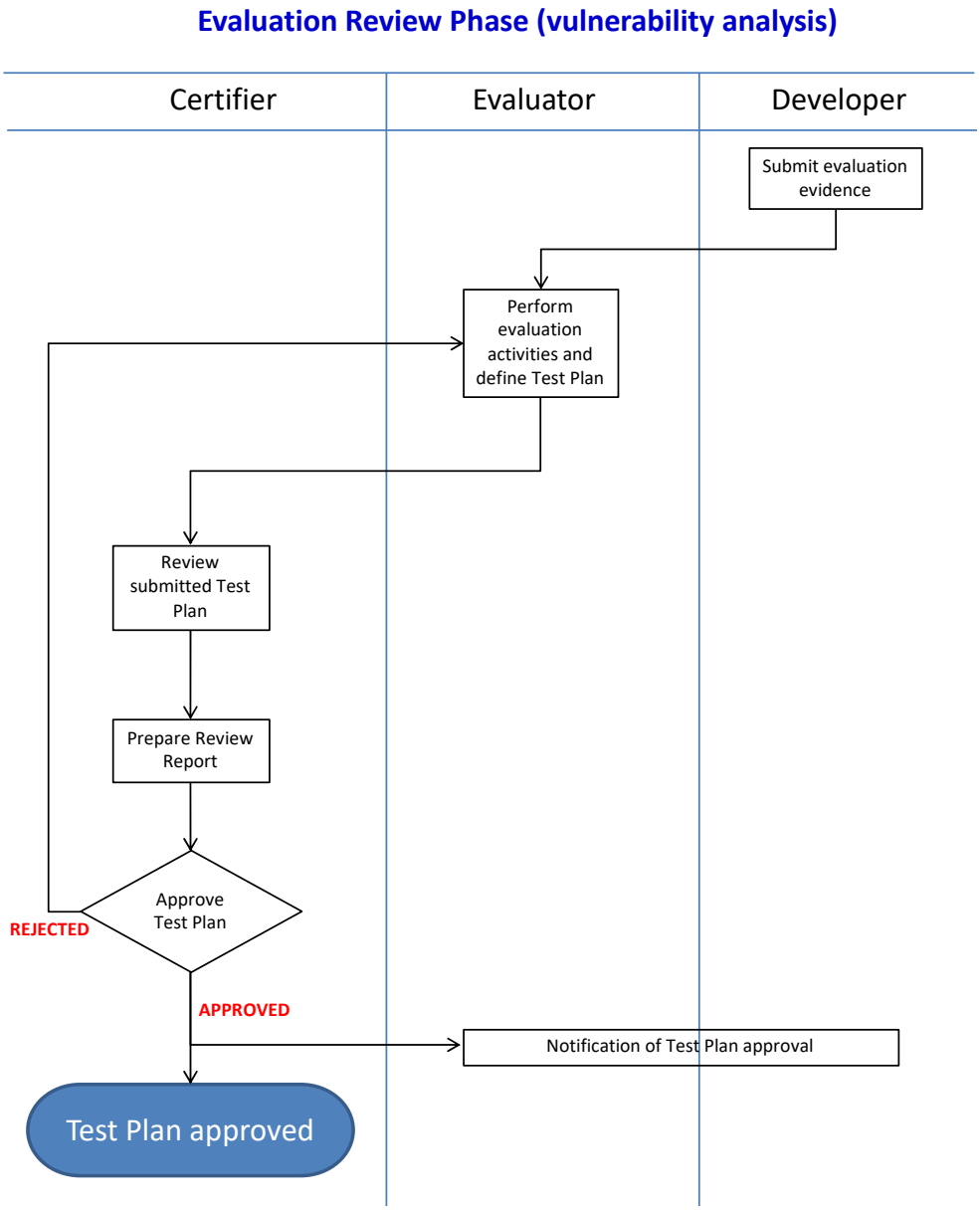
Depending on the assurance level, and therefore what assurance activities the evaluator has to perform, the evaluation Phase may be broken down into a number of sub-phases or stages ("Evaluation Phase x", where x indicates the stage number).

The following sections describe a two stage process to the Evaluation Phase, where the approval of the test plan is the milestone of evaluation phase 1. This milestone needs to be achieved before the evaluator can proceed to the 2nd stage of the evaluation phase.

3.2.1.1 Evaluation Phase 1

In the first evaluation phase, the evaluator reviews the evaluation evidence supplied (e.g. source code, product guides), and generates the evaluation reports (e.g. vulnerability analysis and test plan). These are discussed with the certifier and, if sufficiently clear that it will lead to sufficient assurance, the certifier will approve the evaluation reports that act as a gateway to the next stage of the evaluation phase (e.g. Test Plan).

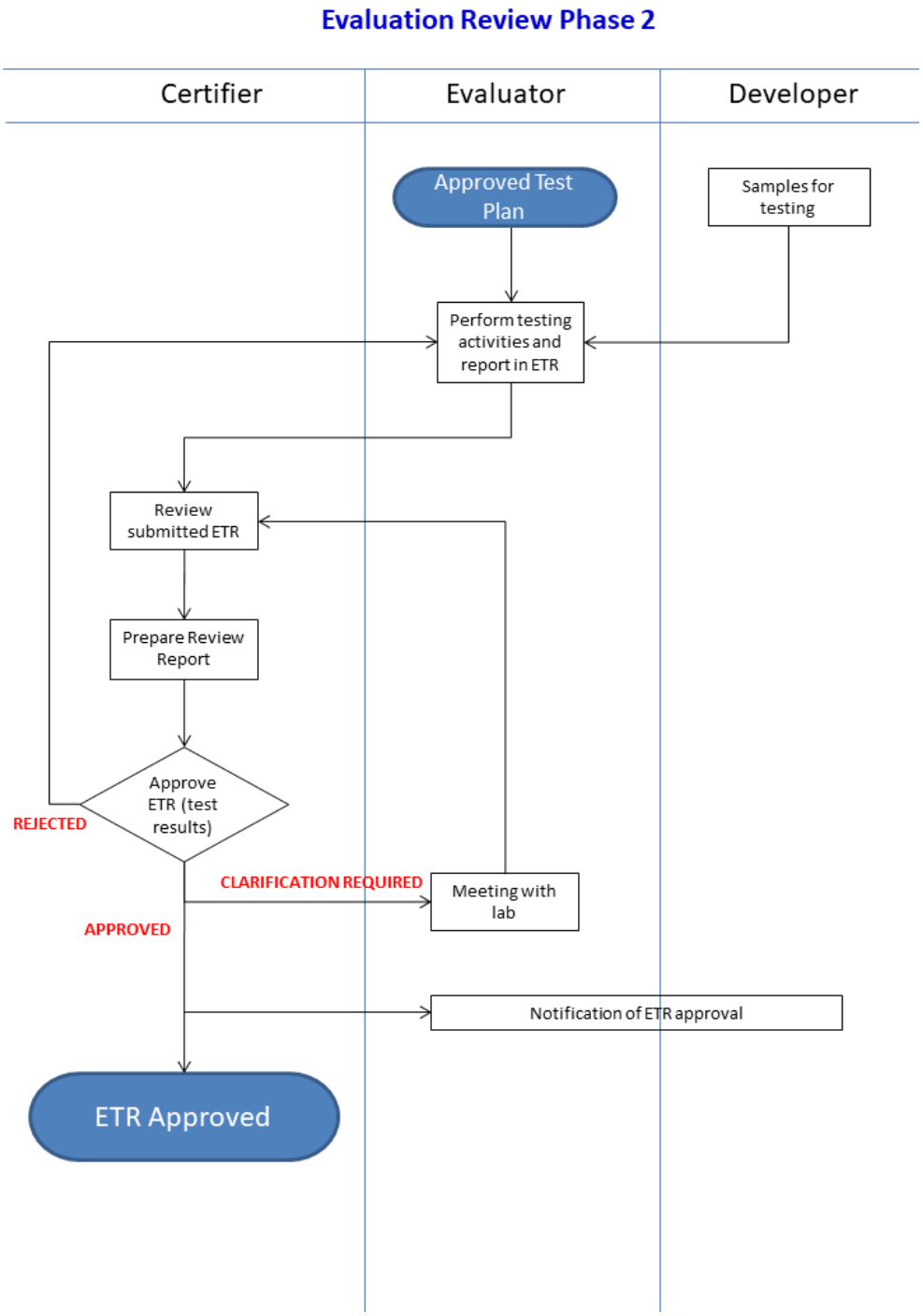
Figure 3 Evaluation phase 1 steps



3.2.1.2 Evaluation phase 2

Having passed the After testing, the evaluator will generate the ETR, may discuss it with the developer, and then presents the ETR to the certifier. If the certifier considers the results to be sufficiently convincing, he will issue a certificate.

Figure 4 Evaluation phase 2 steps



3.2.2 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, as this is a common format of documents already exchanged between these stakeholders in the course of CC.

3.2.3 Reporting requirements

The evaluator shall report his findings in the form of an ETR, and include all certificates, Shared Evaluation Reports, Shared Audit Reports and other evaluation evidence used in the reference list in the ETR.

The version of the standard(s), methodology and all other related scheme documentation applied shall be stated.

The evaluator shall explicitly state:

- The evaluator has determined that the product meets all requirements of the claimed certification scheme.
- 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 the applicable scheme and has high-assurance that the product protects the defined assets against *attack to a specified level of assurance/state-of-the-art attackers* at the time of issuance of this report".

Unless otherwise specified for a given scheme, the evaluator shall use the Evaluation Technical Report for Composition template of SOGIS [ETR] as basis for the reporting.

---

*Note that this document shall **not** be sent to the scheme owner, unless the developer is also the scheme owner.*

Note also that this document is considered to contain sensitive information about the security and potential security weaknesses of the product, and therefore shall be kept strictly confidential.

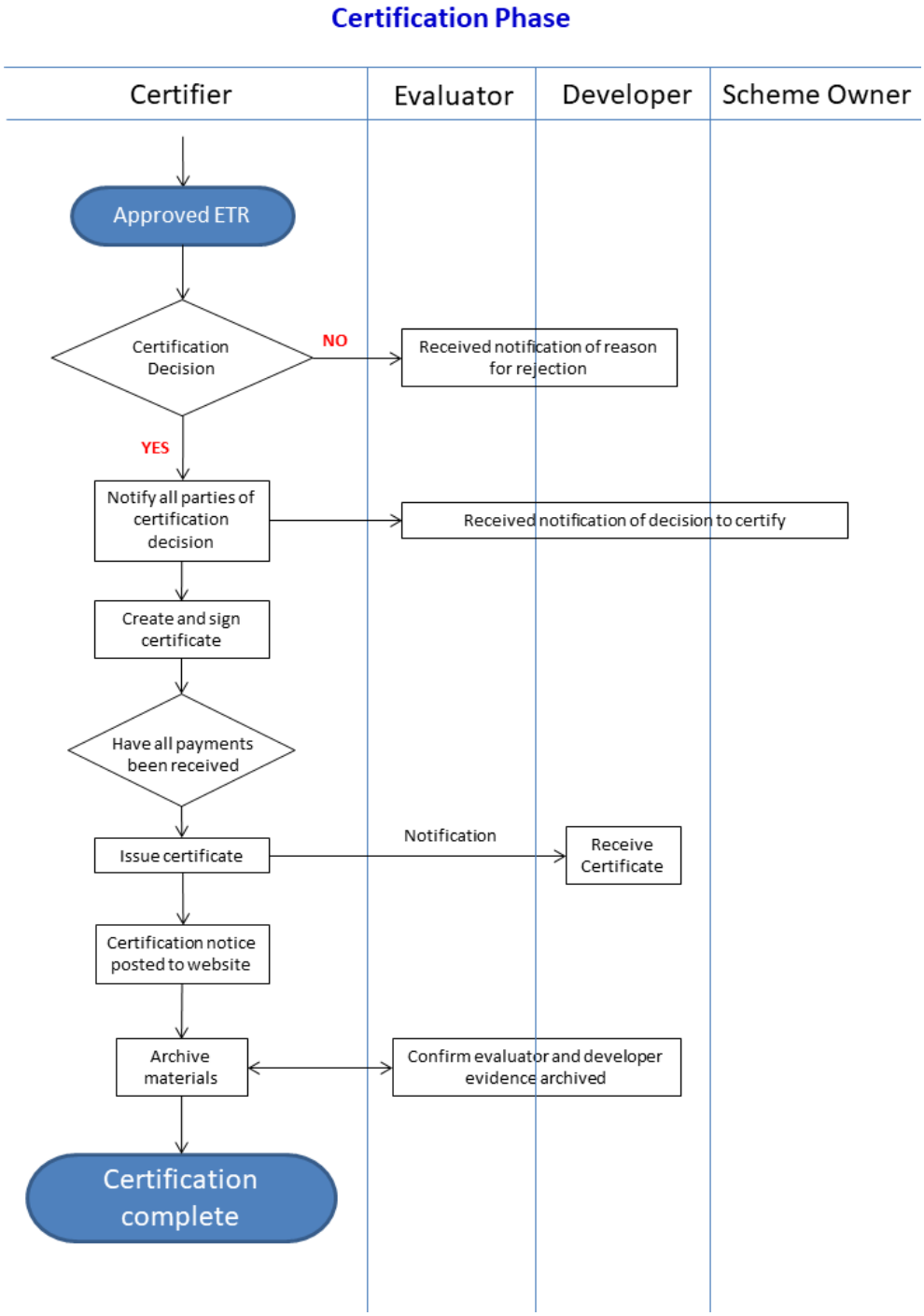
3.3 Certification phase

This phase starts with the delivery of the Evaluation Technical Report, together with any additional reports (e.g., ETRfC, STAR) necessary for the Certified to complete their activities. These reports should also include any materials necessary to facilitate the sharing of evaluation results between Certifiers and Evaluators from different evaluation labs and certification bodies. In addition, relevant Developer documents, such as Security Target, ST-Lite, completed Developer questionnaires, TOE guidance documentation.

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 5 Certification phase steps



3.3.1 Certificate validity

Certificate validity is measured as a defined period of time from the ETR issue date. Typically this period is three (3) years, but it can vary according to the scheme as it is dependent on the expected longevity of the technology type and evaluation results once it is deployed.

The specified period can be extended 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 a further

(typically shorter) period of time, e.g. 18 months. Each time that (renewal) evaluation and certification is performed, the ETR and the certificate showing sufficient resilience against attack to a specified level of assurance, or 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 the original (full) certificate validity period.

The resulting analysis and testing shall, however, always show that the product protects the defined assets against attack to a specified level of assurance, or current state-of-the-art attacks.

The default position regarding the (re-)use of test results for the analysis is that the test results 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 directly relied on 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

Composition with another certificate (e.g. underlying hardware platform) can only be applied if composition is supported by the methodology of the scheme against which the current TOE is undergoing evaluation and certification. In which case the conditions for the issuance, scope and validity of the certificate with which the TOE is to be composed have to be met.

3.3.3 Certifier reporting

To protect the scheme owner's brand and assets, the certifier shall decide whether or not the requirements of the scheme methodology and other referenced materials have been met and hence a sufficiently high level of assurance has been obtained to ensure that the TOE protects assets against attack to a specified level of assurance, or state-of-the-art attackers.

The certifier shall verify that the evaluator's ETR meets all requirements set in the scheme documents.

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 Certificate Template.

4 Reference Materials

The documents listed in Table 1 may have been cited in this document or used to obtain background information about the schemes operated by TrustCB.

Table 1: Reference documents

Title	Source	Reference
ISO Standard 15408 Common Criteria for Information Security Evaluation Common Criteria version 3.1	1	[CC]
ISO Standard 18045 Common Evaluation Methodology CEM version 3.1	1	[CC]
ISO Standard 14443 Identification cards – Contactless integrated circuit cards – Proximity cards	1	[ISO-14443]
Joint Interpretation Library Application of Attack Potential to Smartcards, Version 2.9	2	[JIL]
Java Card System Open Configuration Protection Profile, v3.0.5, December 2017	3	[JC-PP]
Security IC Platform Protection Profile BSI-PP-0084-2014	3	[HW-PP]
EMVCo Security Evaluation	4	[EMV]

Key:

1 = Available online from ISO standards website (www.iso.org)

2 = Available online from SOGIS (www.sogis.eu)

3 = Available online from CC Portal (www.commoncriteriaportal.org)

4 = Available online from <www.emvco.com>