



TRUST AND VERIFY

TrustCB Shared Scheme Procedures

Version 2.6

Contents

1	Introduction	4
1.1	Schemes referencing the TrustCB Shared Scheme Procedure	4
1.2	Intended audience	4
1.3	Terminology	4
1.4	Contact details	4
2	Security evaluation and certification overview	5
2.1	Objective.....	5
2.2	Roles and responsibilities	5
2.2.1	Scheme Owner (TrustCB/external-organisation).....	5
2.2.2	Developer.....	6
2.2.3	Evaluator.....	6
2.2.4	Certifier (TrustCB).....	7
3	Evaluation and Certification Process	9
3.1	Submission phase	9
3.2	Evaluation phase.....	11
3.2.1	Decomposition of Evaluation Phase.....	12
3.2.1.1	Evaluation Phase 1	13
3.2.1.2	Evaluation phase 2	13
3.2.2	Evaluator reporting	14
3.2.3	Reporting requirements	15
3.2.4	Evidence created outside of the responsibility of the evaluating laboratory	15
3.2.4.1	Composition with another valid certificate	15
3.2.4.2	Evidence provided by the developer.....	15
3.2.5	Site Audits	15
3.3	Certification phase	16
3.3.1	Certifier review	16
3.3.2	Certification advice.....	16
3.3.3	Certificate issuance and publication	16
3.4	Certificate validity	17
3.5	Common graphics, logos and marks used on TrustCB issued Certificates	18
3.6	Certificate maintenance	18
3.6.1	Certificate renewal (extension)	18
3.6.2	Maintenance of the certified TOE that does not impact the certified security claim	19
3.6.3	Changes to a certified TOE that impact the certified security claim (recertification)	19
3.6.4	Administrative re-issue of the certificate.....	19
3.6.5	Certificate suspension and withdrawal.....	20
3.7	Variant certifications.....	20



3.8	Test result re-use.....	20
3.9	Composition aspects: re-use of other certificates	20
3.10	Certifier reporting.....	20
4	Reference Materials	21
	Annex A Revision History	22

1 Introduction

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

TrustCB is an expert Certification Body offering accredited certification services for scheme owners of Common Criteria (ISO15408 + CEM ISO18045) based schemes.

This Shared Scheme Procedure describes the certification framework developed and used by TrustCB in its Certification Body operations to provide efficient IT security certifications with predictable timescales.

1.1 Schemes referencing the TrustCB Shared Scheme Procedure

This Shared Scheme Procedure is applicable to the following schemes:

- MIFARE Scheme
- FeliCa Approval for Security and Trust (FAST) certification scheme
- PSA Certified
- TrustCB SESIP Scheme
- GSMA eSA
- NSCIB and eIDAS
- EUCC, as defined by Commission Implementing Regulation (EU) 2024/482 of 31 January 2024

Each of these schemes has an additional scheme specific procedure detailing any deltas from this Shared Scheme procedure. In case of conflicting information between the Scheme specific procedure and the shared scheme procedure, the scheme specific procedure always takes precedence.

Scheme specific procedures are posted to the scheme webpage on the TrustCB website <https://trustcb.com>.

1.2 Intended audience

This document is publicly available and is intended 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 laboratories are appointed to perform the evaluation activities¹.

2.2 Roles and responsibilities

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

2.2.1 Scheme Owner (TrustCB/external-organisation)

The Scheme Owner², 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.
- Shall maintain the definitive list of licensed evaluation laboratories and the certification body.

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 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 inform the evaluator of any information (including known possible weaknesses and attacks) relevant to the evaluation of the TOE.
- 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 all parties (including the scheme owner) immediately if any vulnerability of the TOE becomes known during either the evaluation or during the validity period of the certificate.

If the vulnerability becomes known after a certificate has been issued, the scheme owner shall also be informed. 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 may delay the informing of the scheme owner by at most 30 days from the moment the vulnerability became known to any party. Any unresolved discussion at the end of the 30 days 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 (TrustCB)

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 the 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 laboratories³.
- 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 choosing.

3 Evaluation and Certification Process

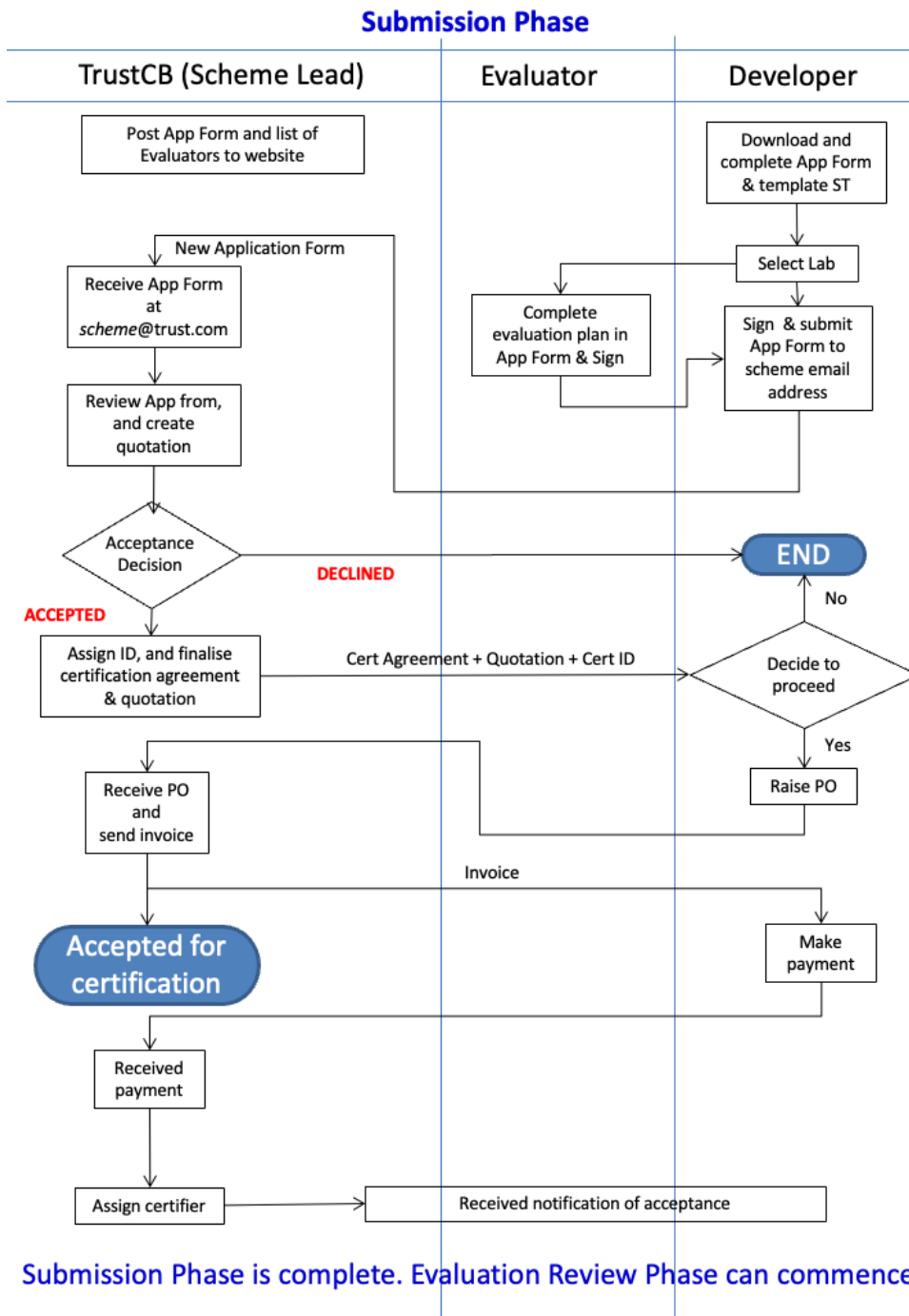
All outsourced evaluation testing activities must be performed in accordance with the requirements of ISO/IEC 17025 and by an Evaluator that has been listed by TrustCB as a Licensed Lab. The list of TrustCB Licensed Labs, and the schemes they have been licensed for, is published on the TrustCB website.

3.1 Submission phase

In the submission phase, the developer arranges the application and any contracts with the evaluator. Together they complete the Application Form for the proposed TOE and submit it to TrustCB. The information in the application form and declarations made by the developer and lab are the basis for the Certification Agreement with TrustCB.

At the conclusion of this phase, the intended certification ID is communicated (Certification IDs are discussed in section 3.4 below), the certifier is assigned and the certification project becomes active.

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.

Evaluation Review Phase



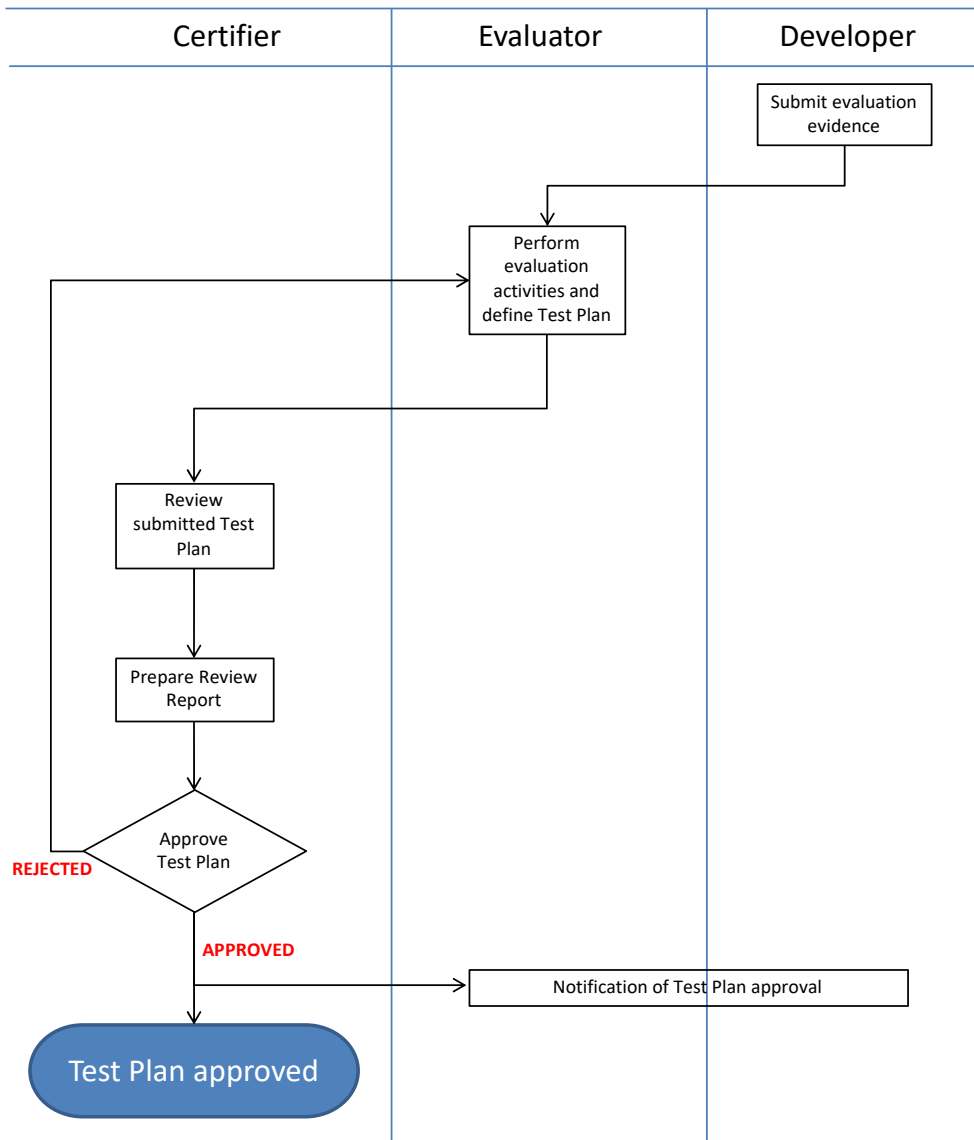
The following sections describe a two stage process to the Evaluation Phase, where the approval of the test plan is the milestone of evaluation phase 1. This milestone needs to be achieved before the evaluator can proceed to the 2nd stage of the evaluation phase.

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

Evaluation Review Phase (vulnerability analysis)

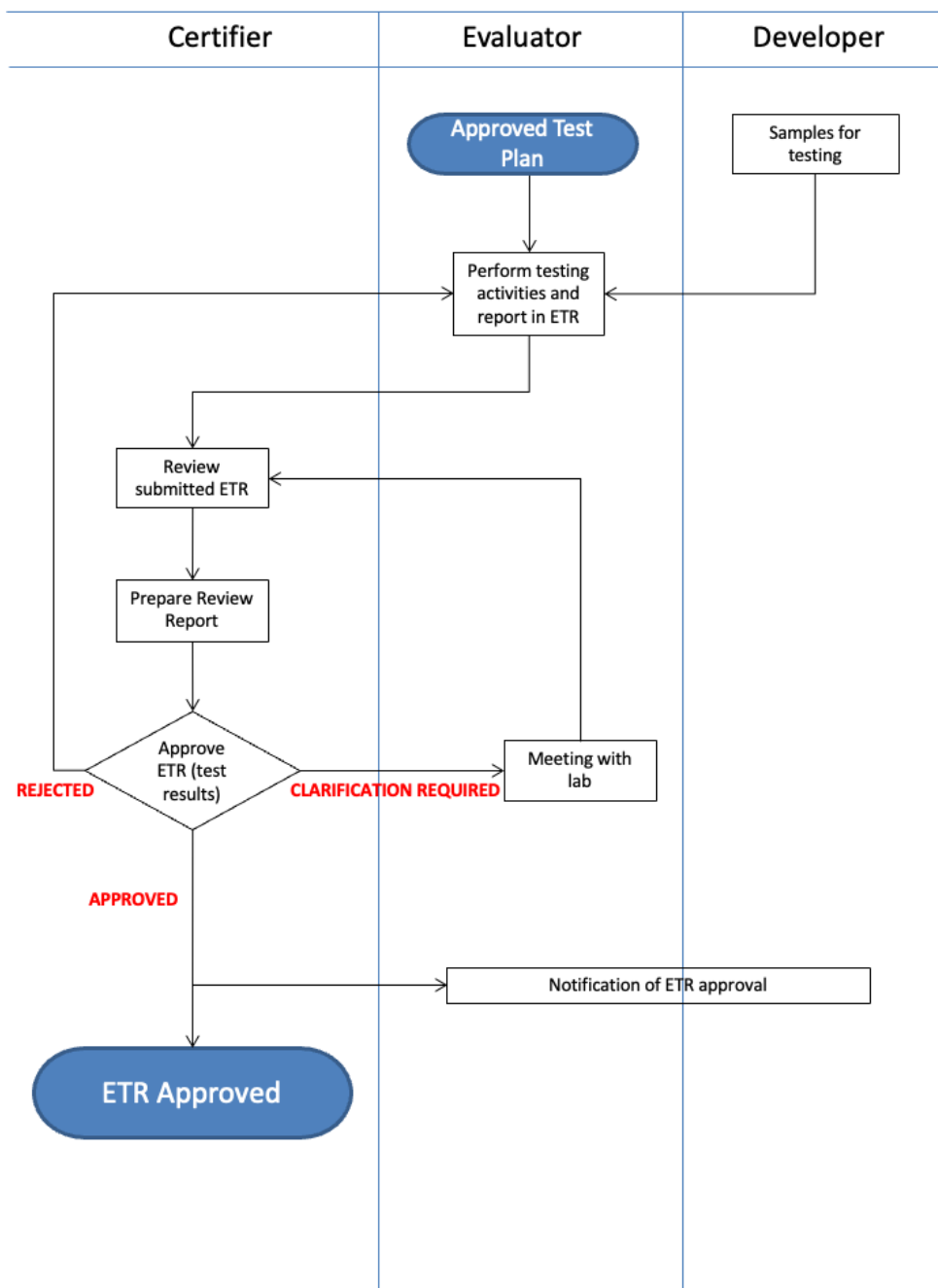


3.2.1.2 Evaluation phase 2

Having successfully completed the 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, the ETR review report will be marked as approved.

Figure 4 Evaluation phase 2 steps

Evaluation Review Phase 2



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.

The evaluator shall forward the complete set of evaluation meeting report(s) to the certifier no less than 5 full working days in advance of the planned evaluation meeting. Practically, this means:

- for example: for an evaluation meeting on a Friday, the complete set of evaluation meeting report(s) must be delivered no later than the Thursday the week before at the latest (assuming no holiday days are in between).
- for an evaluation meeting on a Monday, the delivery must be no later than the Friday 2 weeks before.

3.2.3 Reporting requirements

The evaluator shall report their 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 concludes 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 the report is considered to contain sensitive information about the security and potential security weaknesses of the product, and therefore shall be kept strictly confidential.

3.2.4 Evidence created outside of the responsibility of the evaluating laboratory

The default expectation is for the evaluating laboratory to generate all evidence to demonstrate compliance to the scheme requirements. Scenarios where evidence is created outside of the responsibility of the evaluating laboratory include:

3.2.4.1 Composition with another valid certificate

Refer to section 3.9 of this document. The evaluating laboratory is required to ensure the scheme conditions for the issuance, scope and validity of the certificate with which the TOE is to be composed have to be met.

3.2.4.2 Evidence provided by the developer

Evidence provided by the developer is outside of the accreditation of the evaluating laboratory and must be evaluated by the laboratory against the requirements of scheme.

3.2.5 Site Audits

The Common Criteria specification includes a life cycle component (ALC), parts of which require a site audit. This is typically included in the requirements for Common Criteria based schemes.

Site audits must be performed in a competent way, in compliance with the scheme and standards, including the Joint Interpretation Library document: Minimum Site Security Requirements (available from SOG-IS.org).

The scheme requirements will indicate what the scheme accepts as evidence of a successful site audit; for example, re-use of an existing, valid, Common Criteria based audit report (CC or STAR) or an EMVCo report (SAR). It may also be necessary for a site audit to be performed as a part of the evaluation.

TrustCB recognizes the following scenarios for site audit evidence as a part of an evaluation. In all cases the site audit report must reference the specific location for the activity and must be valid, in accordance with scheme requirements.

TrustCB requires site audit reports intended to be used as evidence for CC based schemes to have been generated under one of the following 4 scenarios:

(1) Site audit performed by TrustCB

Accepted by TrustCB, if confirmed as aligning to scheme requirements.

Note: A Common Criteria based site audit performed by TrustCB would need to be a separate certification activity to a certification activity that is using the Site Audit certificate

(2) Site audit performed and reported by a non-accredited party, witnessed by TrustCB

Accepted by TrustCB, if confirmed as aligning to scheme requirements.

(3) Site Audit report issued by a Certification Body, accredited for this activity

Accepted by TrustCB, if confirmed as aligning to scheme requirements.

(4) Site audit performed and reported by an ITSEF which is accredited for this activity.

At this time, ITSEFS that are accredited by ISO17025 are permitted to perform site audits under the EA TMB Resolution 2022 (09) 01 which may be found in the following document: https://european-accreditation.org/wp-content/uploads/2020/01/EA-INF_17.pdf.

3.3 Certification phase

3.3.1 Certifier review

This phase starts with the delivery of the approved 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 laboratories and certification bodies. In addition, relevant Developer documents, such as Security Target, ST-Lite, completed Developer questionnaires, TOE guidance documentation.

3.3.2 Certification advice

The Certifier shall perform a final review these reports to ensure all the review comments in Review Reports are addressed. When the Evaluator has satisfactorily addressed any remaining comments the Certifier shall record the certification advice and complete the impartiality statement in the ETR review report and submit it to the certificate issuer.

3.3.3 Certificate issuance and publication

The Certificate issuer will ensure all certification activities have been completed and recorded correctly. The Certificate Issuer will then prepare the certification documentation (certificate and, if applicable, certification report).

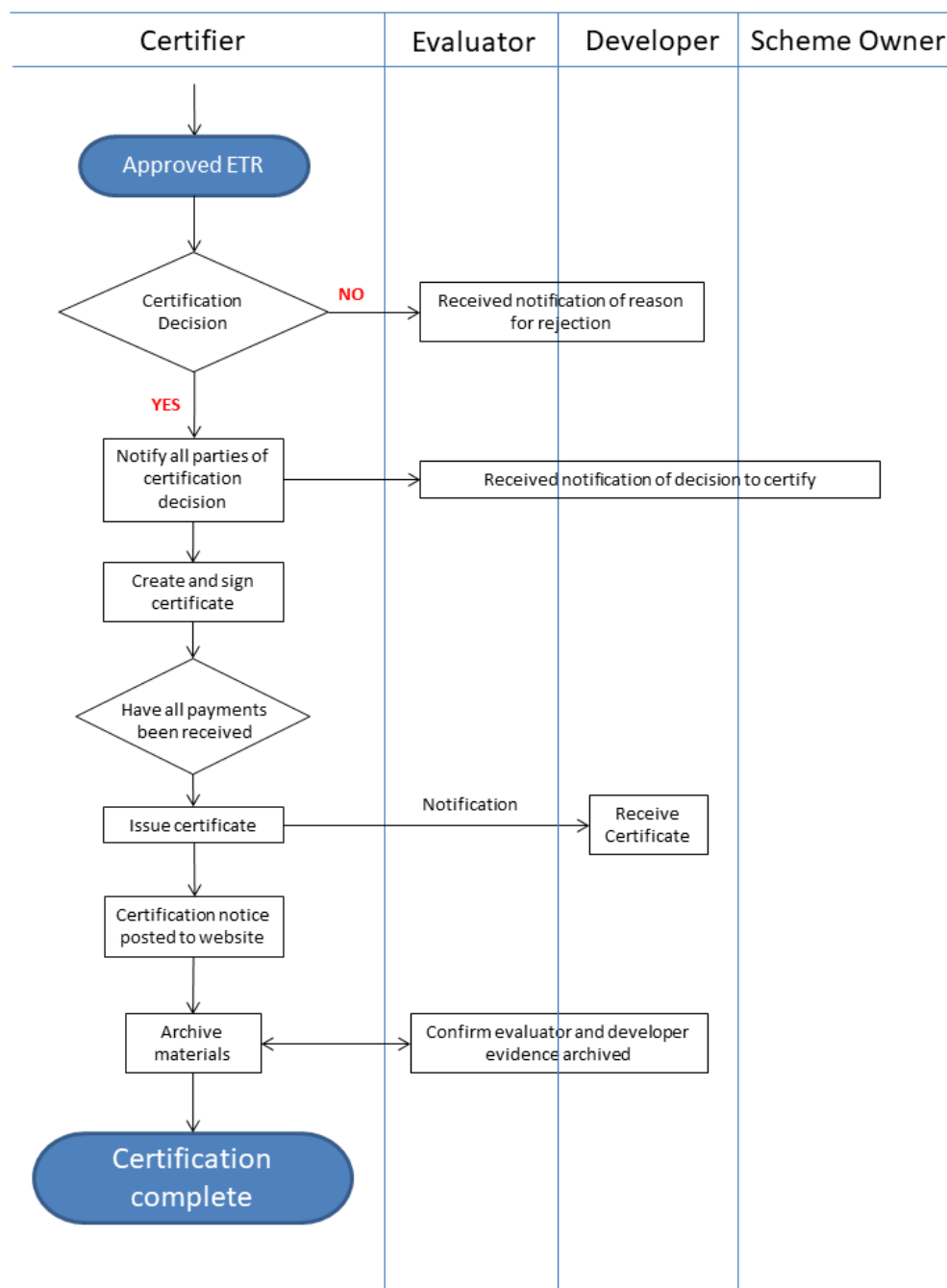
The Certificate shall be published on the TrustCB scheme website (unless the developer explicitly requested otherwise in the application form**), and notification of the publication shall be sent to the Developer and Evaluator. A copy of the certificate shall be sent to the Developer.

**If the Developer has requested the certificate to not be published, then a placeholder is added to the table of certificates on the website. The placeholder includes the certification ID and in place of the certificate and security target, details of the hash values of both those items are provided, facilitating a consumer of the certificate to verify that

they have been provided with a valid copy of the certificate and ST. The placeholder will contain no information relating to the developer or to the TOE identifier.

Figure 5 Certification phase steps

Certification Phase





3.4 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.

3.5 Common graphics, logos and marks used on TrustCB issued Certificates

The following graphics, logos and marks may be found on TrustCB issued certificates. Scheme specific marks are detailed in either the relevant Scheme Procedure or scheme Application Form

	<p>Common Criteria mark, owned by TrustCB.</p> <p>Used on the certificate as a visual identifier for the Common Criteria Standards upon which the MIFARE scheme requirements are based.</p> <p>This mark is not a certification mark.</p> <p>Use of this mark outside of the issued certificate is not permitted unless authorised by TrustCB.</p> <p>TrustCB reserves the right to take all necessary steps against any misuse of (Registered) Trademarks of TrustCB, as per trademark laws.</p>
	<p>RvA accreditation mark owned by RvA, Raad voor Accreditatie, and required to be used on RvA accredited certificates issued by TrustCB.</p> <p>This mark as used on a TrustCB issued MIFARE certificate is not a certification mark.</p> <p>The use of this mark is strictly governed by the RvA.</p>
	<p>Certificates issued by TrustCB include the TrustCB owned TrustCB logo.</p> <p>The TrustCB logo is not a certification mark.</p> <p>TrustCB reserves the right to take all necessary steps against any misuse of (Registered) Trademarks of TrustCB, as per trademark laws.</p>

3.6 Certificate maintenance

This section details the types of certificate maintenance that may be available. Some maintenance types are scheme dependent and for these the specific scheme procedures should be referenced.

If the certificate maintenance scenario allows for the same Certificate ID to be used then the revision element of the Certificate ID will be incremented for the certificate re-issue and the previous certificate will be superseded. For example, "SESIP-2000099-01" is superseded by the re-issue "SESIP-2000099-02").

3.6.1 Certificate renewal (extension)

Certificate renewal is scheme dependent.

Certificate renewal always requires an associated renewal evaluation. The ETR and associated reports resulting from the renewal evaluation must show that sufficient resilience has been demonstrated against attack to the specified level of assurance and the current state-of-the-art attacks.

The evaluation deliverables are the same as for an initial evaluation.

The successful outcome is a re-issue of the certificate showing the issue date of the initial certificate plus the date of the renewal issue. The expiry date will be the new extended date (as defined by the scheme).

For example (assuming 3 year certificate validity, with renewal ETR issued on 2021-01-12):

Validity	Date of Issue: 2020-10-19	
	2021-01-19	Renewal
	Date of expiry: 2024-01-12	

The revision number of the Certificate ID will be incremented and the previously issued certificate will be superseded by this re-issued certificate.

3.6.2 Maintenance of the certified TOE that does not impact the certified security claim

Certificate reissue for this type of maintenance is scheme dependent.

An application for this type of maintenance must clearly demonstrate why there is no impact on the certified security claim. This evidence will be reviewed by a certifier and a corresponding (maintenance) Review Report prepared with the Certifier analysis and certification recommendation for reissue.

The successful outcome is a re-issue of the certificate showing the issue date of the initial certificate plus the date of the maintenance issue. The expiry date will remain unchanged.

For example (assuming 3 year validity and the ETR from the original certification issued on 2020-10-12):

Validity	Date of Issue:	2020-10-19	Maintenance
		2021-01-19	
	Date of expiry:	2023-10-12	

The revision number of the Certificate ID will be incremented and the previously issued certificate will be superseded by this re-issued certificate.

3.6.3 Changes to a certified TOE that impact the certified security claim (recertification)

A change to a TOE that affects the certified security claim, including the need for an updated vulnerability analysis, is a recertification.

Recertification always requires an associated evaluation. The evaluation deliverables are the same as for an initial evaluation. The ETR and associated reports resulting from the evaluation will reference the scheme requirements and references that are valid at the time of the application for recertification.

The application may reference elements of the originally certified product for results re-use. The re-use of results and analyses will be dependent on the evaluator having sufficient information to determine the impact of the changes compared to the previously certified product. See also section below on test result re-use.

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

The successful outcome is a certificate with its own Certification ID that is valid for the full certificate validity period, as defined by the scheme rules.

3.6.4 Administrative re-issue of the certificate

The necessity for an administrative re-issue of a certificate is determined by TrustCB for reasons that are unrelated to the assurance activities described in this document.

The resulting certificate will show the initial issue date and the Administrative re-issue date. The expiry date will remain unchanged.

For example (assuming 3 year validity and the ETR from the original certification issued on 2020-10-12):

Validity	Date of Issue:	2020-10-19	Administrative re-issue
		2021-01-19	
	Date of expiry:	2023-10-12	

The revision number of the Certificate ID will be incremented and the previously issued certificate will be superseded by this re-issued certificate.

3.6.5 Certificate suspension and withdrawal

If TrustCB is made aware of an issue that could reasonably mean the product is no longer in conformance with the certification requirements, TrustCB will suspend the certificate pending investigation to determine whether the certificate needs to be permanently withdrawn, needs to be revised (change of scope) or can be reinstated (possibly with conditions or limitations attached).

If a certificate is suspended or withdrawn, TrustCB CEO will inform the sponsor, with any responsibilities or actions needed of the sponsor. The certificate will be removed or marked accordingly. If a decision is reversed or renewed, the sponsor will be informed.

3.7 Variant certifications

When the certified product is modified to create a new product that will exist as a separate product to the originally certified product, a new certificate is required.

A new application must be made and a new Certification ID will be assigned.

The application may reference elements of the originally certified product for results re-use. The re-use of results and analyses will be dependent on the evaluator having sufficient information to determine the impact of the changes compared to the previously certified product. See also section below on test result re-use.

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

3.8 Test result re-use

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.

3.9 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.

3.10 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	1	[CC]
ISO Standard 18045 Common Evaluation Methodology CEM	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, (current version)	2	[JIL]
Java Card System Open Configuration Protection Profile, v3.1, April 2020	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>

Annex A Revision History

Version	Date	Description of change
2.1	2021-06-17	Note added to 3.3.1: certificate issue date unchanged if re-issued for non-assessment related reasons, corrected editorials, clarified certification phase including non-publication of certificate.
2.2	2021-11-05	New section 3.4, certificate maintenance. Subsequent sections renumbered.
2.3	2022-01-25	New section 3.5, Common graphics, logos and marks used on TrustCB issued Certificates. Subsequent sections renumbered.
2.4	2023-04-19	1.1.1 updated 3.2.2 updated: timing for delivery of evaluation materials ahead of an EM 3.2.4 added: evidence created outside of the responsibility of the evaluating laboratory 3.2.5 added: site audits +editorials
2.5	2023-02-26	1.1 EUCC added to document scope
2.6	2024-08-02	2.2.2 Clarified that the developer must share potential vulnerabilities with the evaluators and certifiers during the evaluation process also. 3.6.5 Certificate suspension text added