TRUST AND VERIFY

TrustCB Scheme Procedure for Site Certification

Version 1.1

TRUST AND VERIFY

Contents

1 Site Certification Scheme

This document is an annex to TrustCB Shared Scheme Procedures (current version) [TrustCB-SP] detailing specific details for the TrustCB site certification scheme.

1.1 Introducing the Site Certification scheme

TrustCB Site Certification Scheme is designed to assess and certify development and production sites involved in Common Criteria and EUCC product certifications. Building on the foundations of the NSCIB Site Certification framework, it provides confidence that a site's security processes, configuration management, and vulnerability handling are implemented and maintained to the standards expected for EUCC, Common Criteria, and other high-assurance standards. The scheme aligns with internationally recognised methodologies (EUCC), ensuring that results can be reused across public and private certification schemes.

The primary source of information for the Site Certification scheme, including these TrustCB scheme procedures, can be found at the TrustCB webpage for Site Certification.

1.2 Site Certification Contact details

The Site Certification Scheme contact address at TrustCB is Site_cc@trustcb.com.

1.3 Scope of the Site certification scheme

The TrustCB Site Certification scheme applies to all development and/or production sites that play a role in any phase of the design, development, manufacturing, or maintenance lifecycle of integrated circuits (ICs), operating systems (OS), or application software intended for security evaluations under Common Criteria or EUCC. This includes semiconductor fabs, design centres, firmware and software development sites, secure personalisation, integration facilities, test facilities and data centres.

In summary, any site that handles sensitive assets or contributes to the security-relevant parts of a certified product can be evaluated under the TrustCB Site certification scheme to demonstrate that it operates in alignment with the requirements for EUCC Substantial/High assurance levels.

2 Site Certification Process

The processes of the TrustCB site certification scheme are based on [RDI-NP002]. The Dutch NCCA's involvement in this process is oversight of the scheme, not monitoring of certification per project.

[RDI-NP002] describes in detail three phases of the certification process for EUCC certifications under the Dutch NCCA, intended for ENISA notification

Phase 1: Notification phase

Phase 2: Evaluation and Review Phase

Phase 3: Certification Approval Phase

Considering that neither the EUCC or ENISA recognises site certificates, the following optimisations have been developed for this scheme:

2.1 Notification Phase

2.1.1 Application to TrustCB for the site certification scheme

Before the submission phase, the developer has contracted a licensed evaluation lab (the list of labs can be found at: www.trustcb.com/about-us/labs) and, together with that lab, has completed the application form (available at: www.trustCB.com/site-certification/application form). A signed copy of the application form, together with a draft Site Security Target, must be sent by email to:

site_cc-application@trustcb.com.

TrustCB will respond with a quotation for certification for acceptance by the certification sponsor. Upon receipt of the quotation acceptance, TrustCB will issue an invoice for payment of the certification fee.

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

2.2 Evaluation and Review Phase

The evaluation and review phase is based on [RDI-NP002], with the following modifications:

There are two evaluation meetings in this scheme:

- Site audit verification plan approval (ERM1+ERM2 in [RDI-NP002])
- Site audit result (ERM3 in [RDI-NP002])

The documents required for delivery at each milestone are described in [RDI-NI002]. The following documents apply to the TrustCB site certification:

- Site Security Target
- ASE evaluation results
- The Consultancy/Evaluation Improvement Presentation
- Checklist of all evaluator action items and content and presentation elements relevant for the claimed assurance level
- The ALC Presentation, including ALC verification plan
- The ALC Results Presentation
- STAR (based on [SotA-EUCC-STAR])
- ETR

In case MSSR applies to the site (ALC_DVS.2), the [SotA-EUCC-MSSR] will be used.

Delivery of presentation materials to the assigned Certifier shall be made at least five working days before the Evaluation Meeting, unless otherwise agreed.

The default expectation is that all Evaluation Meetings will be held as physical-only meetings in a location in the Netherlands. A virtual meeting is possible with the agreement of all parties.

2.2.1 Performing site audit

The TrustCB requirements for the site audits are outlined in the [TrustCB-SI-07].

2.3 Certification Approval Phase

A TrustCB site certificate will be issued upon successful completion of the evaluation and review phase . Certification documentation for the TrustCB site certification comprises the TrustCB generated Certificate and Certification Report, together with the developer Site Security Target.

The certificate validity period for the site certificates is Two (2) years from the certificate date. The validity of the STAR follows the guidelines established by the EUCC for STAR validity.

In case of maintenance, the re-issued certificate will be identified through an increase in the certificate iteration identifier and the issuance date (i.e. a certificate with certificate iteration identifier '-01' will be reissued with '-02', and the date entry on the certificate will list the original certificate issuance date and the 2nd issuance date. The certificate expiry date will remain unchanged. The reissued certificate will be posted on the scheme website. The original certificate will also be retained on the website.

2.4 Certification Marks and Logos

The TrustCB issued certificate for a site includes the TrustCB logo, owned by TrustCB B.V.

2.5 References Materials

Unless otherwise stated, the latest published version applies.

Table 1 The site certification scheme Documents

Title	Reference[1]
TrustCB Site Certification Application Form	https://trustcb.com/common-criteria/site-certification/
Technical requirements and scheme methodology:	
TrustCB Shared Scheme Procedures	
[RDI-NP002]	https://www.dutchncca.nl/documents/schemedoc/np/002/eucc-processes-v2.0
[RDI-NI002]	https://www.dutchncca.nl/documents/schemedoc/ni/002/content-and-presentation-of-evaluation-review-meetings-v1.0
[TrustCB-SI-07]	https://trustcb.com/common-criteria/site-certification/
[SotA-EUCC-MSSR]	https://certification.enisa.europa.eu/publications/minimum-site-security-requirements_en
[SotA-EUCC-STAR]	https://certification.enisa.europa.eu/publications/star-methodology_en
Common Criteria for Information Technology Security Evaluation, Parts 1, 2, 3, 4 and 5	CC: 2022 Revision 1
Common Methodology for Information Technology Security Evaluation, Evaluation Methodology	

[1] Latest version applies unless otherwise stated

Annex A Revision History

Version	Date	Description of change
1.0	2025-11-11	Initial release
1.1	2025-12-22	Section 1.1: Correction