TRUST AND VERIFY

TrustCB Scheme Procedure for EUCC

Version 2.0

Contents

1 EUCC scheme

This document, as an annex to TrustCB Shared Scheme Procedures [TrustCB_SP], details the scheme specific details for the EUCC certification activities

1.1 Introducing the EUCC scheme

The European Cybersecurity Certification Scheme (EUCC) has been developed and adopted within the EU under Regulation (EU) 2024/482. EUCC provides an EU and internationally recognised means of evaluating and certifying the security aspects of Information and Communication Technology products. The EUCC has been developed under the European cybersecurity certification framework set out in Regulation (EU) 2019/881, the EU Cybersecurity Act (CSA).

The referenced international standard for the scheme is the Common Criteria standard, ISO/IEC 15408 and associated Common Evaluation Methodology ISO/IEC 18045.

The purpose of this document is to describe additional operational processes applied by TrustCB in its role as Certification Body (CAB), licensed and authorised by the *Dutch Authority for Digital Infrastructure (RDI)* for the task of ISO/IEC 17065 Certification Activities up to and including EUCC Evaluation Assurance Level High for ICT security products, as well as for protection profiles, and including the issuance of EUCC cybersecurity certificates which may also be CCRA recognised..

The primary source of EUCC Certification Scheme documents is the Enisa website, https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

The primary source of RDI documents for EUCC is the Dutch NCCA website, https://www.dutchncca.nl/eu-cybersecurity-certification/common-criteria

The primary source of TrustCB managed operational documents for the scheme can be found at https://trustcb.com/common-criteria/eucc/

1.2 EUCC Contact details

The scheme contact address at TrustCB for EUC related enquiries is eucc@trustcb.com.

1.3 EUCC TOE-type Overview

This scheme applies to any IT security product able to be evaluated as a Target Of Evaluation (TOE) by [CC] for the purposes of certification under [EU-EUCC], notification to the RDI and to Enisa.

TOE types that may be classified in one of the following technical domains are required by to be evaluated in accordance with the applicable state-of-the-art documents detailed in [EU-EUCC] Annex I:

- Smartcards and Similar Devices
- Hardware Devices with Security Boxes

2 EUCC Certification Process

The document [RDI-NP002] describes in detail the 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

The details below provide supplementary TrustCB information.

2.1 Notification Phase

2.1.1 Application to TrustCB for EUCC certification

Prior to the notification phase, the certification sponsor will have contracted a TrustCB licensed evaluation lab. Details of TrustCB Licensed labs that are licensed for EUCC can be found on the TrustCB website. The certification Sponsor and contracted lab should complete the application form together. The application form includes obligations and expectations for all parties and is signed and dated by both the certification sponsor and by their chosen evaluation lab.

The Evaluation Work Plan section of the form must be completed by the lab, based on their discussions with the Sponsor. This will form the basis for the Assessment Plan that will be reviewed and confirmed by TrustCB, and also by RDI for applications requesting EUCC assurance level High and or referencing CCRA.

A public PGP key for EUCC applications is available from the TrustCB website if the Sponsor wishes to encrypt the ST and any additional information. The application form itself should remain unencrypted.

2.1.2 Notification to the NCCA

As detailed in [RDI-NP002], the application documentation and TrustCB confirmed Assessment Plan for the following certification types will be delivered by TrustCB to RDI for confirmation as part of this phase:

- Certifications referencing EUCC assurance level
- Certifications (both High and Substantial) referencing CCRA

In accordance with [RDI-NP002] the Certification activity for these certification types can only start once RDI acceptance has been confirmed.

2.2 Evaluation and Review Phase

The evaluation phase is described in [RDI-NP002]. RDI will assign a member of their team to the following certification types:

- Certifications referencing EUCC assurance level
- Certifications (both High and Substantial) referencing CCRA

2.2.1 Cooperation with ITSEFs

A key part of the Netherlands implementation of the EUCC is its phased review approach which enables the assigned certifier to review the ongoing evaluation at Evaluation Review Meetings; stated fixed points in the evaluation process where evidence of conformity is presented to the Certifier.

The cooperation of the ITSEF is essential to enable these Evaluation Review Meetings and to enable presentation to the Certifier of any other information on any EUCC related aspect of the certification in progress or of the lab methods and techniques. TrustCB may also wish to visit the ITSEF for the purpose of the certification decision.

All cooperations shall be documented, either by meeting report or by email, to ensure the impartiality, objectivity and independence of TrustCB can be demonstrated.

2.2.2 Delivery of evaluation review meeting documentation

Delivery of presentation materials to the assigned Certifier and the assigned RDI team member shall be made 10 working days ahead of the Evaluation Review Meeting, unless otherwise agreed.

2.2.3 Remote evaluation meetings

The default expectation is that all Evaluation Review Meetings shall be held as a physical only meeting in a location in the Netherlands. A request for a virtual meeting is an exceptional request and requires the agreement of all parties.

If a virtual meeting is agreed, the method of joining that meeting needs to take into account the sensitivity of the material that is to be discussed. The TrustCB confidentiality policies applies at all times, refer to the TrustCB website for details.

For information considered Secret, such as those in most smartcard projects, at AVA_VAN.4 level or higher, *WIRE is the chosen solution*. Refer to **Annex A** on the use of WIRE encrypted communications for remote meetings.

2.2.4 Witnessing of Site Audits

The following considerations apply when witnessing site audits conducted by the lab:

- The lab assigned evaluator shall focus on gathering **evidence that the processes and procedures are being applied**. While it is appropriate to ensure any process described by the interviewee is consistent with that provided in the evidence, the focus is to **gain evidence** that the procedure is in use. For example, by witnessing of, or requesting copies of, items such as records, logs, photos, videos of a process in operation, etc.
- The lab assigned evaluator shall consider **all types of assets** in the audit. Even if the audit is of a software development location, the developers may receive engineering samples on which to test the software, in which case the control of those engineering samples would need to be verified. Similarly, with assets such as tamper proof tape for the packaging of any samples to be returned that needs to be controlled.

A proposal to use video conferencing tools for remote site audits must be agreed between the developer and the evaluating lab. If agreed, the evaluator must provide a justification of why the chosen tool is appropriate for the ALC_DVS level (examples of those used for the audits are Wire, Webex, Microsoft Teams).

2.3 Certification Phase

The certification phase is described in [RDI-NP002].

The certification documentation for the following certification types must be delivered to RDI for confirmation as part of this phase:

- Certifications referencing EUCC assurance level
- Certifications (both High and Substantial) referencing CCRA

2.3.1 EUCC Certification documentation

Certification documentation for an EUCC product comprises the TrustCB generated Certificate and Certification Report, together with the developer Security Target.

The templates used for Certificate and Certification Report generation reflect the EUCC requirements.

The certificate validity period for EUCC certificates is five (5) years.

The confirmed Certification Documentation will be issued to the certification sponsor, the RDI and Enisa

TrustCB will publish all issued certifications on the TrustCB webpage for EUCC issued certificates.

In addition, issued EUCC certificates will be forwarded to Enisa for publication on the Enisa site for EU Cybersecurity Certificates and, where applicable, published on the Certified Products page of the CC portal.

Where a request for "no publication" has been made, a document showing the SHA-256 of the issued certification documentation will be published on the TrustCB webpage for EUCC issued certificates.

2.4 Certificate maintenance – assurance continuity under EUCC

The EUCC provides specific requirements for Assurance continuity and is the primary reference for this activity. Refer to EUCC Annex IV which states the available options for assurance continuity together with the scope and applicability of assurance continuity under EUCC.

3 Certification Marks and Logos

TrustCB does not issue a Certification Mark for EUCC certified products. However, in accordance with the [CCRA] the mutual recognition mark is included on the certificates when this has been requested by the certification sponsor and approved for use by RDI.

4 Reference Materials

Title	Reference
TrustCB Application Form - EUCC	[AF-EUCC] [1]
Technical requirements and scheme methodology:	
Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) In addition, any amendments to that Regulation that are valid at the time of the certification activity	[EU-EUCC] [2]
ISO/IEC 15408 and CEM ISO/IEC 18045, permitted versions at the date of receipt of the application form and applying stated transition periods, where applicable.	[CC], [CEM] [3]
NCCA processes	[RDI-NP002] [4]
TrustCB Shared Scheme Procedures	[TrustCB_SP] [5]

[1] https://trustcb.com/common-criteria/eucc/

[2] https://eur-lex.europa.eu/eli/reg_impl/2024/482/oj, https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

[3] https://www.commoncriteriaportal.org./cc/index.cfm

[4] https://www.dutchncca.nl/eu-cybersecurity-certification/common-criteria/eucc-documents

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

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

Annex A WIRE encrypted communications for remote meetings (Normative)

Wire only supports video calls when there are a **maximum of 4 participants**. This means that a group created for an evaluation meeting should not contain more than 4 accounts (including those to be invited using a guest link). Additional participants may join the call once the video link has been established between the initial 4 participants, but those joining will only be able to participate via audio.

Once a video link has been established between 4 participants, even if one participant leaves new participants cannot join via video until the device associated with the participant who has left is removed from the list (a password is required by the account holder to remove a device from the list of devices listed for that account). This means that either it will be necessary to continue with audio input only from those joining after the total of 4 is reached or possibly one of the 4 participants leaves the meeting, their device is removed and then the new participant can join with video support.

Summary of guidance for the use of Wire:

1. For each EM, confirm how many individuals will participate on the call. This should be limited to <= 4 separate accounts (e.g. TrustCB certifier(s), ITSEF account).
    i. There may be multiple attendees joining the call using the ITSEF account, but wherever possible this should be limited to 3 or less individuals from the ITSEF, including the session also hosting the monitoring certifier (if applicable).
    ii. Request developer/sponsor participates only if imperative.
2. In advance of the EM:
    i. Certifier to create a group for the call, adding applicable accounts and creating guest link if necessary.
    ii. When using lab account for a new meeting, remove all devices previously used for that account (entry of account password is required to remove devices associated with the account.).
3. At the beginning of an EM:
    i. Verify fingerprints of all participant devices (see https://support.wire.com/hc/en-us/articles/207693005-How-can-I-verify-my-own-devices- and https://support.wire.com/hc/en-us/articles/207692235-How-can-I-compare-key-fingerprints-).
    ii. Any non-verified device must be verified at the start of the call or removed from the call.
4. During a call:
    i. Standard etiquette of conference calls should be applied, with only the presenter's microphone being active (all other participants, with the possible exception of the certifier, should be muted).
    ii. EVALUATION REPORTS MUST NOT BE DISPLAYED VIA WIRE.
        i. All evaluation reports must be viewed locally by all participants, using a separate, offline machine.
        ii. Screen-sharing must not be used.
        iii. Cameras must only be focused on participants, and not focused on screens/monitors.

Annex B Clarification of the concept of TSFI

The purpose of this annex is to clarify the concept of TSFI

B.1 TSFI Definitions

The definition of TSFI in CC Part 1 is clarified to[1]:

TSF interface (TSFI): a means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF**, such that:**

- **Attackers can possibly access this means, and/or**
- **SFRs are traced to this means**

For the purpose of this definition:

- An attacker is any external entity or non-TSF subject in the TOE that has not been explicitly defined as trusted in the ST
- An attacker can possibly access a means unless either the TSF itself, or the security objectives for the operational environment, or a combination thereof, prevents the attacker from having access

Examples:

- A physical console of a server that can be accessed by both trusted and non-trusted administrators is a TSFI regardless of whether SFRs trace to it
- A physical console of a server that only trusted administrators have access to, and no SFRs trace to it, is not a TSFI
- A physical console of a server that only trusted administrators have access to, and FMT_SMF.1 traces to is a TSFI
- The PCB of a security module that is claimed to meet FPT_PHP.* (and where the physical enclosure encompasses the PCB) is not a TSFI
- The physical enclosure of the security module above is a TSFI

B.2 Splitting of means

In some cases, a developer may want to split a means into two parts, where part of the means is a TSFI, while another part of the means is not a TSFI. This allows the developer to separate the TSFI from the remainder of the means, to make his documentation burden smaller, as he only has to document the TSFI in depth, and not the entire means.

Examples include:

- The physical layer and datalink layer of a firewall, consisting of both hardware and software, where the security objectives of the environment state that the only attackers reside on the Internet, are not TSFI, as these two layers cannot be directly addressed from the Internet. However, the network layer and higher layers are TSFI. Splitting the "network interface" into two parts would be beneficial, as the developer would not have to specify the physical and datalink layers in depth.
- An encrypted IP connection between the TSF and a trusted server over an untrusted network is a TSFI as attackers have access to it. Splitting the interface into:

[1] Additions are in **bold**

- A TSFI specifying the encryption supplied by the TSF (which could be attacked)
- A non-TSFI interface specifying the traffic between TSF and backup server running over the encryption[2] would be beneficial, as the developer would not have to specify the backup protocol in depth.

B.3 Changes required to other parts of the CC

CC Part 3 Annex A.2 is to be considered secondary to this instruction. That is, where this instruction and CC Part 3 Annex A.2 are in conflict, this instruction has precedence.

There are no further changes: all other CC activities are unaffected.

[2] This interface is not accessible to attackers unless the encryption is successfully attacked first, which would already break the SFRs.

Annex C Revision History

Version	Date	Description of change
2.0	2025-07-04	Initial release