Common Criteria Recognition Arrangement
Management Committee

Operating Procedures

Title: CCRA and EUCC Co-existence
Maintained by: CCMC
Unique Identifier: 011
Version: 1.0
Status: Final
Date of issue: *2025-March-19*
Approved by: CCMC Februry 17, 2025
Supersedes:

Purpose

Global mutual recognition through the Arrangement on the Recognition of CC certificates (CCRA) has fostered and embodied the core principles of fair competition, cybersecurity cooperation, and eliminating the burden of duplicating evaluations of products and protection profiles. It is open to all nations who abide by these principles, including European Union (EU) member states.

The EU Cybersecurity Certification Scheme on Common Criteria (EUCC) places requirements for issuing Common Criteria (CC) certificates on EU member states which do not fully align with the CCRA. EUCC allows for certifications by commercial bodies without equivalent government oversight as in the CCRA. Government oversight of certifications and labs, voluntary periodic assessments (VPA) of member Schemes, both initial Shadow certification and recurring VPA, and participation in and cooperation through regular CCRA meetings have been key components of mutual trust between the participants of the CCRA.

This document explains the proposed requirements for government oversight and VPAs to allow for EUCC certificates to carry the CCRA mark if they also meet the requirements of the CCRA, mutual recognition of all certificates with the CCRA mark by all CCRA participants, and co-existence between CCRA and EUCC. These procedures are designed to continue until an eventual mutual recognition agreement replaces the CCRA.

Overview

The CCRA is built upon 25+ years of engagement between non-EU and EU CCRA governmental entities. This trust has been built and maintained through activities including regular meetings, participation in VPAs, and collaboration on standards development and interpretation.

The importance of maintaining this trust is necessary for the mutual recognition of CCRA certificates.

In order to extend a similar level of trust to certificates issued by conformity assessment bodies (CABs) under the EUCC for assurance level 'Substantial' or 'High' (when applicable), additional per-certificate oversight by the governmental CCRA participant is necessary should mutual recognition under the CCRA be optionally needed.

For new EU members wishing to become a CCRA authorising participant, the CCRA needs to verify the technical competency of the organisation conducting oversight for them to become part of the CCRA. This follows the existing verification process of the Shadow Certification used by the CCRA for any new certificate issuing participant.

Non-EU and EU CCRA certificates will remain to be recognised in accordance with the CCRA by EU member states who are signatories of the CCRA.

Under Article 5 of the *Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security*, the conditions in which recognition is to occur requires an evaluation facility to be accredited to ISO/IEC 17025 and a certification body can be accredited to ISO/IEC 17065, which is a requirement under the EUCC. It is important to note that the requirements for a CCRA certification body (CB) in this respect is closely aligned to the requirements of the ISO/IEC 17065 standard, as such, the shadow certification and VPA procedures of the CCRA, which are used to assess a certification body, also relies on this standard.

Due to the discrepancies of the above requirements, an additional oversight process is needed to assess items such as review of evaluation applications and experiences with the CC standard and ST and TOE appropriateness as these are not in scope of the ISO/IEC 17065. Minor amendments to the current CCRA VPA and shadow certification procedures will therefore be needed.

More details of the oversight process and proposed changes to the VPA and shadow certification procedures will be described later in this document.

Necessity of government oversight

The CCRA requires one CB per participant. The EUCC allows for multiple CBs per member state. To ensure consistency between CBs across all participants, especially from commercial CBs who have not undergone the verification of the shadow certification procedures, an overarching government organization providing oversight is necessary. This is in addition to the already existing government supervision within the EUCC.

This oversight ensures the mutual understanding and trust between government organisations required by the CCRA continues, and will allow for the operation of multiple CBs by a Participant or of purely commercial CBs.

The trust between CCRA participants built up from government oversight and review is essential, as nations use CC certificates for different purposes including national security, medical, and general commercial use. Commercial testing laboratories require government oversight and validation, despite a certain level of trust required. Commercial CBs must also be given a certain amount of trust, but still require government oversight to verify the results.

Process for achieving optional CCRA recognition

EUCC certificates issued by commercial CABs can optionally seek CCRA recognition through the per-certificate oversight process responsible by the organisation performing the NCCA role.

EUCC certificates that are mutually recognised under the CCRA will be subject to the terms of the CCRA with continuous monitoring and any withdrawal initiated by the CCRA of the mutual recognition of EUCC-based CCRA certificates will only be applicable within the CCRA.

The per-certificate oversight process for CCRA recognition will be conducted based on the trusted public-private certification model deployed by the Netherlands' CC scheme (i.e. NLNCSA) and can be flexible and conducted throughout or at the end of the process. The organisation performing the NCCA role will be responsible for the competency of the commercial CABs and the CCRA additional oversight activities will have minimal impact to all parties involved.

At any point that the CCRA requirements are not met, there is no nullification of the EUCC certificate. If the CCRA uncovers issues during assurance continuity, for example, the CCRA can seek the organisation performing the NCCA role to either remove the CCRA mark and reissue the certificate without it or to revoke the certificate. If EUCC revokes a EUCC certificate, then CCRA will remove the certificate from the CC Portal as well. The same would apply for the period of validity of an EUCC certificate.

Government agency conducting additional oversight as certificate authorising participant

The CCRA (the arrangement) builds on certificates that have been authorised by a participant, essentially confirming that the certification and evaluation processes have been carried out in a duly professional manner. Such authorisation is a sanction by a participant permitting the use of the CCRA mark.

The oversight procedure outlined in this paper is aimed at enabling a CCRA mark being used on an EUCC certificate. It is comparable to the authorisation the CCRA refers to and defines in articles 1, 5 and Annex A of the arrangement text.

Therefore, to allow for equivalency in procedures it is necessary for the government agency of the CCRA member conducting the additional government oversight procedure described in this paper to be a certificate authorising participant.

It is foreseen that this should be the same agency in a CCRA member country that also carries out the separate supervisory functions according to the EU cybersecurity act (2019/881) article 58 (the National Cybersecurity Certification Authority, NCCA) in the EU/EEA countries over certifications bodies of the EUCC scheme (EU implementing regulation 2024/482).

If the government agency is not already a certificate authorising participant of the CCRA, it will need to go through the same procedures to become an authorising participant according to the arrangement, including two years as a consuming participant before being able to become an authorising participant.

If only commercial CBs within the EUCC exist in the member country, see Verification of CB/ITSEF Requirements below.

VPA and shadow certification procedures

The purpose of shadow certification is to determine that a Scheme applying for acceptance as a certificate authorising participant into the CCRA complies with the requirements of the CCRA (Annexes B, C and G).

Shadow Certification procedures will align mostly with ISO/IEC 17065 requirements, with additional verification performed by CCRA participants. However, the CCRA requires at least two candidate certifications to be viewed and discussed by an audit team on site, whereas the EUCC has no such requirement.

For commercial CBs under the EUCC seeking the voluntary CCRA mark on a per-certificate basis, they must cooperate with the national organization that is a member of the CCRA (usually the same organization as the NCCA). This cooperation includes the active support of commercial CBs when it comes to possible candidate assessments and on-site audit meetings. Both the commercial CBs and the organization providing government oversight will be the subject of the assessment.

A final assessment of the CCRA requirements covered by ISO/IEC 17065 is in progress. It is assumed that the Shadow Certification Procedures will have to be adapted, especially as there can be several commercial CBs in one country in the EU.

Furthermore the CCRA calls for periodic assessment of member Schemes. The purpose of a VPA is to determine that the constitution and procedures of the CCRA participant under assessment, as well as those of the CBs, continue to comply with the requirements of the CCRA. It is becoming apparent that requirements or concretizations that may go beyond ISO/IEC 17065 are in the area of technical competence that must be demonstrated in two certification procedures and the government oversight procedures. With regard to competence, please refer to the section “Verification of CB/Lab Requirements”.

A final assessment of the VPA requirements covered by ISO/IEC 17065 is in progress. It is assumed that the VPA procedures mostly align as well, with additional verification performed by CCRA participants. Updated VPA procedures should also consider multiple CBs under supervision of an organisation performing the role of the NCCA, such as each one being part of the VPA or a sample of CBs based on recommendation from audit team.

Verification of CB/ITSEF requirements

In the area of CB and ITSEF requirements, EUCC relies primarily on the accreditation and authorization (for level High) of CABs. Accreditation by national accreditation body under IAF is always required, with authorization by the NCCA needed for level High, with CBs accredited against ISO/IEC 17065 and Labs accredited against ISO/IEC 17025. The CCRA includes licensing of ITSEFs, which is not an EUCC requirement for assurance level ‘substantial’. This licensing needs to be applied to CABs (both ITSEFs and commercial CBs) for CCRA certificates in order to meet the CCRA requirements.

Requirements for a CB or an ITSEF that result in particular from voluntary, additional oversight on a per-certificate basis are not covered by ISO/IEC 17065 or ISO/IEC 17025. However, these aspects are relevant for recognition in the CCRA. In addition to the accreditation (and authorization for level High), the organization providing government oversight must take a concrete look at the working methods, CC procedures, and technical competency of the CABs and approve that they are sufficient to meet the CCRA requirements before they are able to issue certificates with the CCRA mark.

Oversight on per certificate basis

EU CCRA participants (usually the same organization as the NCCA) must apply oversight on conformity assessment bodies (both ITSEFs and CBs) for substantial level, if the conformity assessment bodies want to be part of the voluntary CCRA certifications.

The government organisation performing the role of the NCCA is involved in evaluation/certification at application phase, as well as ETR and CR phase.

Application phase: The goal is an efficient certification process in-line with CCRA requirements. Input is the application form, draft ST, and assessment plan. Output is a statement by the CCRA participant that the commercial CB may continue with the certification under the CCRA.

The ETR and CR phase: The goal is verification that evaluation and certification is in-line with the CCRA requirements. Input is all technical reports, certification report, draft certificate, and statement that all action items, including non-conformities. are closed. Output is formal approval by the CCRA participant to the CAB that CCRA marking can be placed on the certificate, which will then be published on the CC Portal by the CCRA participant.

The oversight process is flexible enough to be performed only at the end of the certification process. If the oversight identifies issues, then the certificate will not be allowed to have the CCRA mark, with no affect on the EUCC certificate. It is also possible that this oversight could be performed after the EUCC certificate has already been issued and is part of the assessment under the rules of the shadow certification. The approval by the CCRA participant would be for the EUCC certificate to be reissued by the CB with the addition of the CCRA mark.

Liaison

To ensure these requirements are understood and implemented correctly, any potential issues are identified and addressed as early as possible, and technical communication is direct and easy, the CCRA will nominate a participant to serve as liaison to the EU Commission.

The CCRA members should also consider whether a representative from the EU Commission could participate in some CCRA meetings as a non-voting observer.

Conclusion

Following the recommendations for oversight outlined above will create sufficient confidence that EUCC certificates issued by CABs with oversight provided by the CCRA participant, which also meet CCRA requirements, can be trusted by all participants of the CCRA. This trust will result in mutual recognition by all CCRA participants of these certificates.

The VPA and shadow certification procedures will both be updated to reflect the recommended changes.