EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ACCREDITATION OF ITSEFs AND CBs FOR THE EUCC SCHEME

Philippe Blot
Cybersecurity Certification Sector

20 | 06 | 2024

CONTENT OF THE PRESENTATION

- EUCC requirements related to the accreditation of CABs
- A focus on the 2 state-of-the-art documents related to the accreditation of CBs and ITSEFs

Getting access to up-to-date information: **Homepage - European Union (europa.eu)**

EUCC REQUIREMENTS

- Recital 17

A conformity assessment body is defined as a body that performs conformity assessment activities including calibration, testing, certification and inspection. In order to ensure a high quality of services, this Regulation specifies that testing activities on the one hand, and certification and inspection activities on the other hand, should be carried out by entities operating independently from each other, namely Information Technology Security Evaluation Facilities ('ITSEF'), and certification bodies, respectively. Both types of conformity assessment bodies should be accredited and, in certain situations, authorised.

- Recital 18

A certification body should be accredited in accordance with standard ISO/IEC 17065 by the national accreditation body for assurance level 'substantial' and 'high'. In addition to the accreditation in accordance with Regulation (EU) 2019/881 in conjunction with Regulation (EC) No 765/2008, conformity assessment bodies should meet specific requirements in order to guarantee their technical competence for the evaluation of cybersecurity requirements under assurance level 'high' of the EUCC, which is confirmed by an 'authorisation'

EUCC REQUIREMENTS

- Recital 19

The technical competence of an ITSEF should be assessed through the accreditation of the testing laboratory in accordance with ISO/IEC 17025 and complemented by ISO/IEC 23532-1 for the full set of evaluation activities that are relevant to the assurance level and specified in ISO/IEC 18045 in conjunction with ISO/IEC 15408. Both the certification body and the ITSEF should establish and maintain an appropriate competence management system for personnel that draws from ISO/IEC 19896-1 for the elements and levels of competence and for the appraisal of competence. For the level of knowledge, skills, experience and education, the applicable requirements for the evaluators should be drawn from ISO/IEC 19896-3. Equivalent provisions and measures dealing with deviations from such competence management systems should be demonstrated, in line with the system's objectives.

EUCC REQUIREMENTS

- Article 23 Notification of certification bodies (same applies to ITSEFs)

1. The national cybersecurity certification authority shall notify the Commission of the certification bodies in its territory that are competent to certify at assurance level 'substantial' based on their accreditation.

2. The national cybersecurity certification authority shall notify the Commission of the certification bodies in their territory that are competent to certify at assurance level 'high' based on their accreditation and the authorisation decision.

3. The national cybersecurity certification authority shall provide at least the following information when notifying the Commission of the certification bodies:

(a) the assurance level or levels for which the certification body is competent to issue EUCC certificates;

(b) the following information related to accreditation:

(1) date of the accreditation;

(2) name and address of the certification body;

(3) country of registration of the certification body;

(4) reference number of the accreditation;

(5) scope and duration of validity of the accreditation;

(6) the address, location and link to the relevant website of the national accreditation body; and…

EUCC REQUIREMENTS

- Article 7 Evaluation criteria and methods for ICT products

1. An ICT product submitted for certification shall, as a minimum, be evaluated in accordance with the following:
(a) the applicable elements of the standards referred to in Article 3;
(b) the security assurance requirements classes for vulnerability assessment and independent functional testing, as set out in the evaluation standards referred to in Article 3;
(c) the level of risk associated with the intended use of the ICT products concerned pursuant to Article 52 of Regulation (EU) 2019/881 and their security functions that support the security objectives set out in Article 51 of Regulation (EU) 2019/881;
(d) the applicable state-of-the-art documents listed in Annex I; and
(e) the applicable certified protection profiles listed in Annex II.

EUCC REQUIREMENTS

- Article 7 Evaluation criteria and methods for ICT products

2. In exceptional and duly justified cases, a conformity assessment body may request to refrain from applying the relevant state-of-the-art document. In such cases the conformity assessment body shall inform the national cybersecurity certification authority with a duly reasoned justification for its request. The national cybersecurity certification authority shall assess the justification for an exception and, where justified, approve it. Pending the decision of the national cybersecurity certification authority, the conformity assessment body shall not issue any certificate. The national cybersecurity certification authority shall notify the approved exception, without undue delay, to the European Cybersecurity Certification Group, which may issue an opinion. The national cybersecurity certification authority shall take utmost account of the opinion of the European Cybersecurity Certification Group.

SOA DOCUMENTS RELATED TO ACCREDITATION

- Accreditation of ITSEFs, version 1.6b
- Accreditation of CBs, version 1.6a

GUIDANCE DOCUMENTS

- Authorisation of CABs, version 0.6
- Vulnerability management and disclosure
- Cryptography (ACM), version 0.2

These documents have been submitted to ECCG opinion

THANK YOU FOR YOUR ATTENTION
ANY QUESTIONS?

Cybersecurity Certification Sector
Market, Certification & Standardisation Unit
ENISA, The European Agency for Cybersecurity