

EUCC versus CCRA/SOGIS

**EUCC, differences with CCRA/SOGIS
Common Criteria scheme.**

New requirements and improvements

29/10/2024

NURIA CARRIÓ

PUBLIC





Common Criteria

With National Schemes
(CCRA/SOGIS)



EUCC
Cybersecurity Certification

01 SCOPE AND PURPOSE

Scope of the presentation

- 01.1 PURPOSE
- 01.2 WHAT REMAINS...?

02 CONTEXT AND HIGHLIGHTS

What we are going to see...

- 02.1 EUCC: THE NEW SCHEME
- 02.2 STAKEHOLDERS IN EUCC
- 02.3 EUCC TIMELINES
- 02.4 TECHNICAL DOMAINS

03 KEY POINTS AND MAIN DIFFERENCES

Let's start with differences/key points for EUCC/SOGIS-CCRA

- 03.1 NEW OBLIGATIONS and SCOPE
- 03.2 STATE OF THE ART DOCUMENTS
- 03.3 MUTUAL RECOGNITIONS
- 03.4 PROTECTION PROFILES
- 03.4 EVALUATION 'HIGH'
- 03.5 VULNERABILITY DISCLOSURE AND PATCH MNGT
- 03.6 MARK and LABEL



Scope and Purpose



SCOPE

EUCC applies to all ICT products and protection profiles.



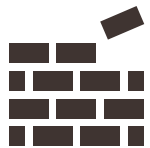
EVALUATION METHODOLOGY

Common Criteria is used. ISO/IEC 15408 and ISO/IEC 18045.



THIRD PARTY ASSESSMENT

CBs, ITSEFs (CABs) are still in place.



DOCUMENTS, TECHNICAL DOMAINS and PPs from SOGIS

Work already in place from SOGIS is reused for EUCC.



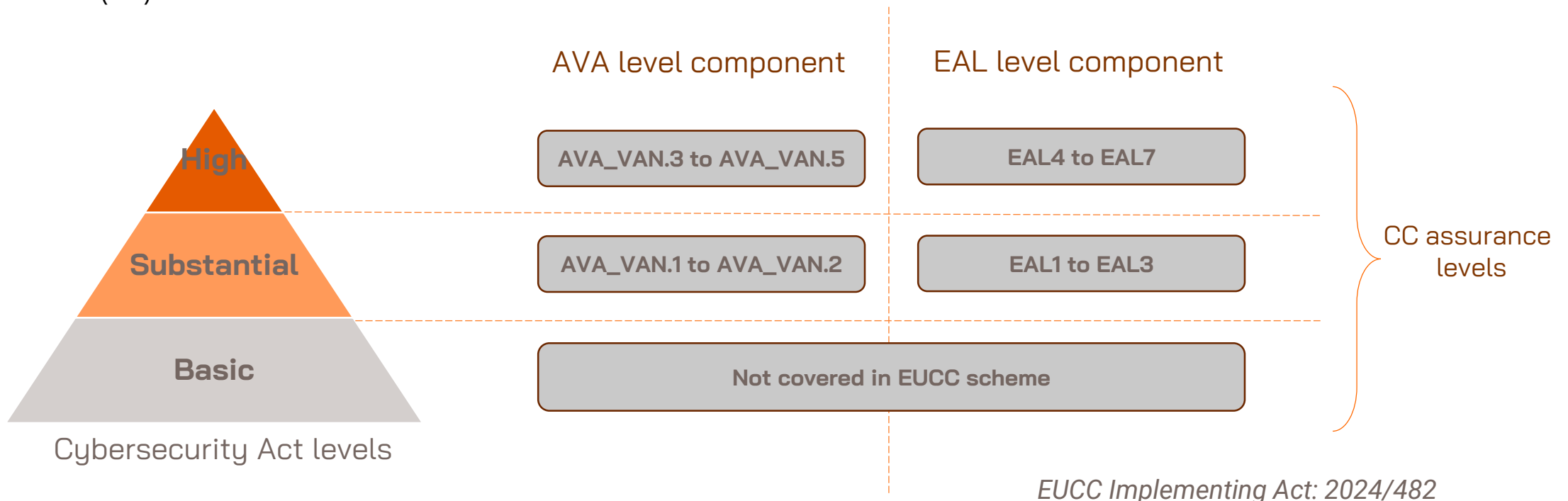
Context and Highlights

Cybersecurity Act (CSA), the base EU cybersecurity regulation

CSA is European framework for the EU cybersecurity certification of ICT products, services and processes.

EUCC is a new scheme developed under CSA regulation umbrella.

- Based on the **Common Criteria standard** (ISO/IEC 15408) designed as a methodology to perform independent security evaluations on ICT devices.
- The assurance levels of EUCC scheme are '**HIGH**' and '**SUBSTANTIAL**' depending on the assurance levels of the Common Criteria standard (CC).



National Schemes as CBs for CCRA/SOGIS, what's new now for EUCC?

- Conducts accreditations for CB and ITSEF under ISO 17065 and ISO 17025.



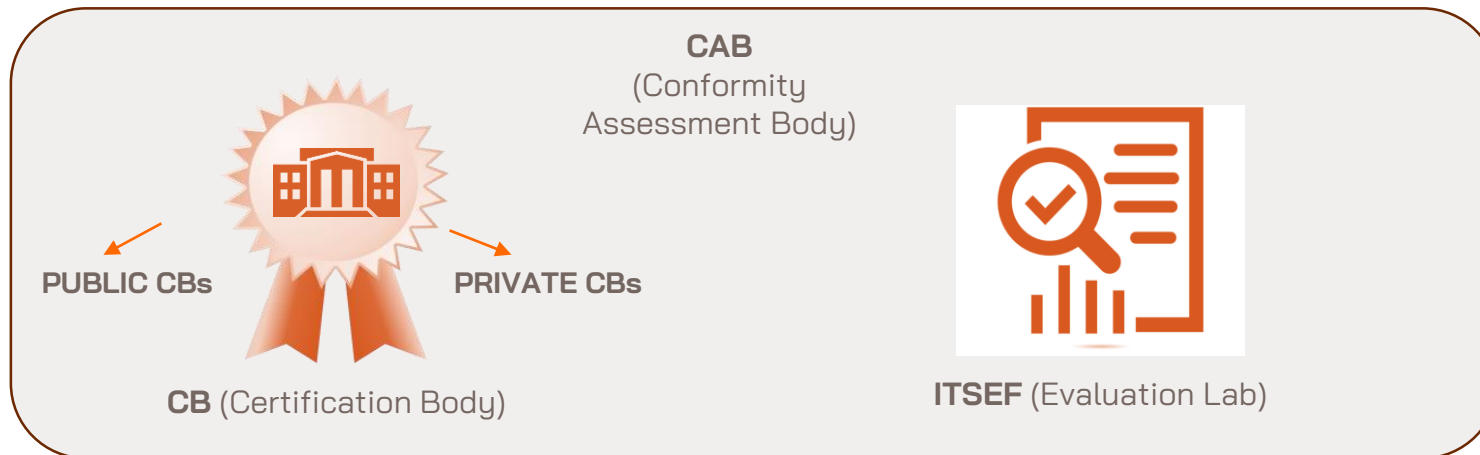
NAB (National Accreditation Body)



NCCA (National Cybersecurity Certification Authority)

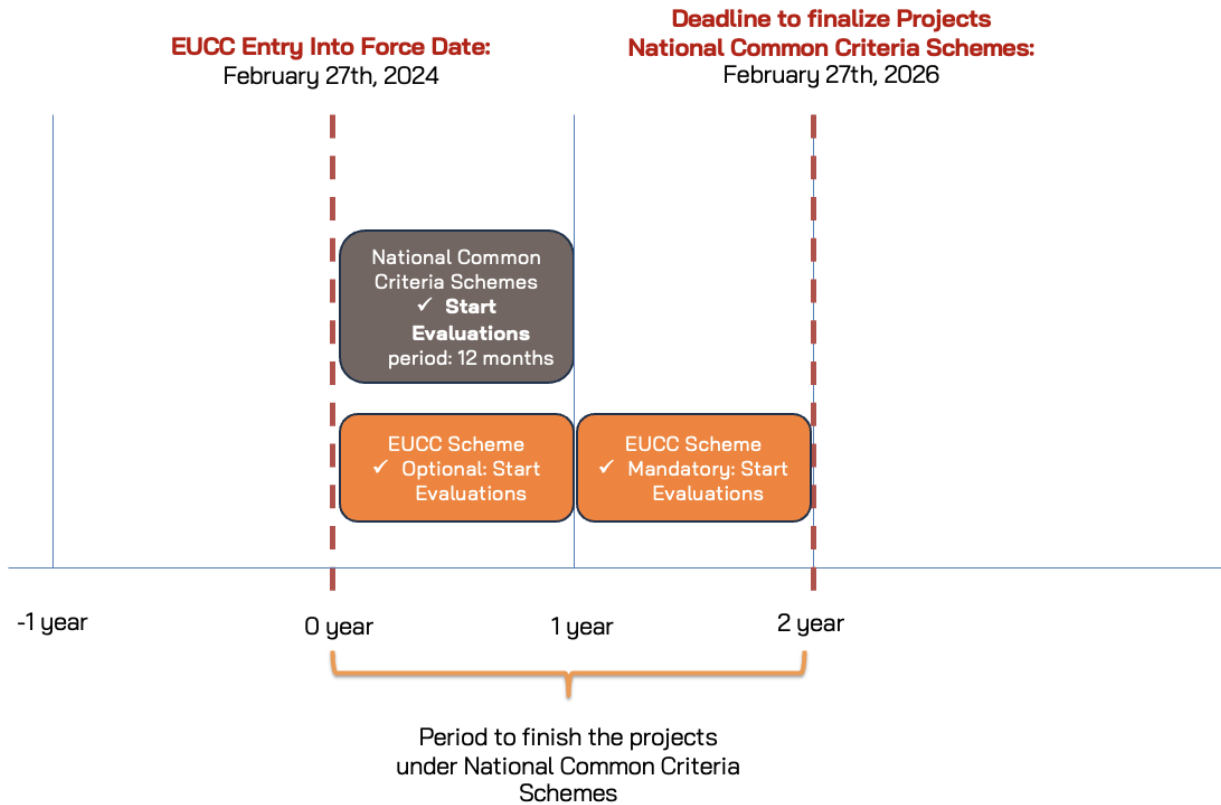
- Conducts authorizations for 'HIGH' assurance.
- Works as supervision and monitoring authority.

- Perform certification activities.



- Performs security evaluations activities.

Important Timelines: EUCC is already a reality.




- The EUCC scheme is now a **voluntary scheme**, meaning that it is up to the manufacturer (or coming from a final client requirement) to pass a security evaluation under CC (now EUCC).
- However, other regulations like **CRA** (Cyber Resilience Act) may mandate the EUCC obligatoriness for some products.
- It is still possible to start evaluations with the National schemes, provided they are finalized before February 2026) but NOT recommended as risk to not finalize on time!
- **CC:2022 mandatory:** 2024/06/30.
- **CC:2022 Protection Profiles mandatory:** 2027/12/31.

Member states → End their participation in the **CCRA**

Two technical Domains listed currently for AVA_VAN.4 and AVA_VAN.5 are:

See Annex I (EUCC Implementing Act).



Smart Cards
and Similar
Devices.



Hardware
Security Boxes

Technical Domain: Reference framework that covers a group of ICT products that have specific and similar security functionality that mitigates attacks where the characteristics are common to a given assurance level.

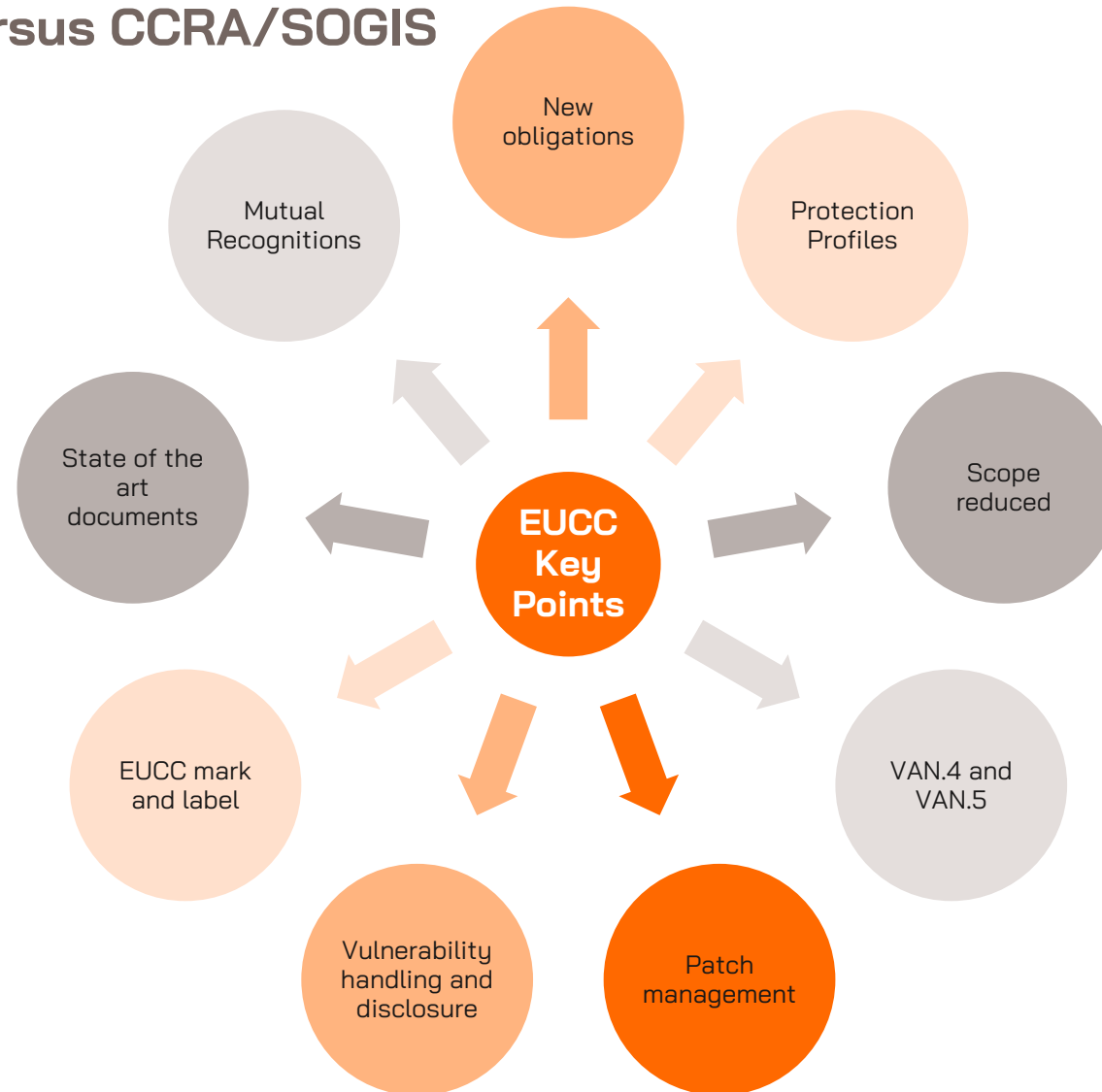
A technical domain describes in state-of-the-art documents the specific security requirements as well as additional evaluation methods, techniques and tools that apply to the certification of ICT products that are covered by this technical domain.

REUSE OF ALL SOGIS DOCUMENTS and INHERITS THE SAME TECHNICAL DOMAINS



Main differences/Key Points

Highlights of EUCC versus CCRA/SOGIS



Applicants **SHOULD** provide ICT product usage documentation

Applicants for EUCC certification provide documentation related to the intended use of the ICT product.

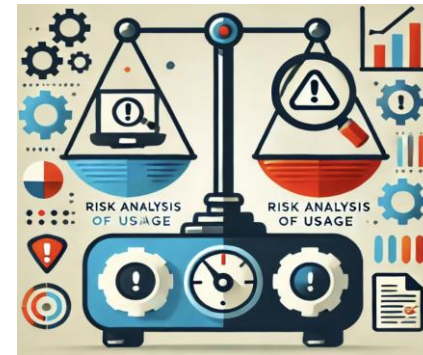
Applicants **SHOULD** provide risk analysis

Applicants also provide analysis analysis of the levels of risks associated with such usage.

CAB → Evaluate the suitability of the assurance level selected.



INTENDED USAGE

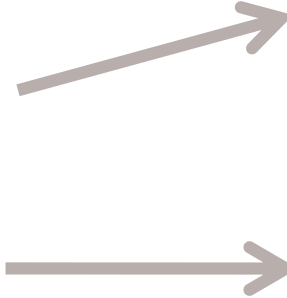


RISK ANALYSIS

Non-compliance of obligations

Article 9(2), 27 and 41

- Commitments/Obligations – Article 9(2)
- Information to be available by the holder of the certificate – Article 41
- Monitoring activities- Article 27



Example of obligations:

- (b) not to promote the ICT product as being certified under the EUCC before the EUCC certificate has been issued;
- (c) to promote the ICT product as being certified only with respect to the scope set out in the EUCC certificate;
- (d) to cease immediately the promotion of the ICT product as being certified in the event of the suspension, withdrawal or expiry of the EUCC certificate;

Non-compliance with CSA

Article 55, CSA

- Supplementary cybersecurity information.

Article 56(8), CSA

- Inform about **detected vulnerabilities or irregularities** concerning the security of the certified ICT product, ICT service or ICT process without undue delay.

Remedial Action period

30 DAYS

Remedial action proposal



If Not proposed



**CERTIFICATE SUSPENDED OR
WITHDRAWN**

Continued or recurring non-compliance will lead to the withdrawal of the certificate



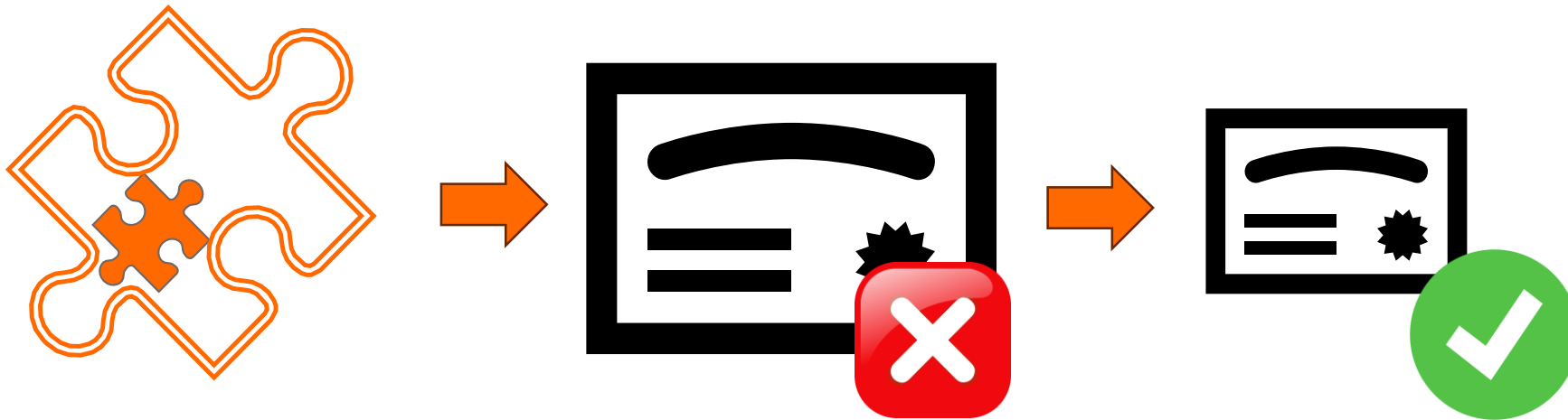
Article 27

Monitoring activities by the holder of the certificate

1. The holder of an EUCC certificate shall perform the following tasks to monitor the conformity of the certified ICT product with its security requirements:
 - (a) monitor vulnerability information regarding the certified ICT product, including known dependencies by its own means but also in consideration of:
 - (1) a publication or a submission regarding vulnerability information by a user or security researcher referred to in Article 55(1), point (c) of Regulation (EU) 2019/881;
 - (2) a submission by any other source;
 - (b) monitor the assurance expressed in the EUCC certificate.
2. The holder of an EUCC certificate shall work in cooperation with the certification body, the ITSEF, and, where applicable, the national cybersecurity certification authority to support their monitoring activities.

Scope Reduction

- Where the **scope of an existing EUCC certificate is reduced**.
 - the certificate shall be withdrawn,
 - a new certificate with the new scope should be issued.



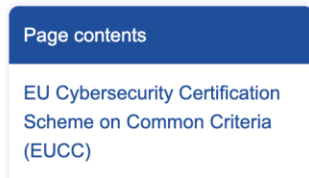
State-of-the-art documents

- Documents to be followed, in particular for **technical domains and protection profiles**. **EUCC Certification Scheme**



- Are **mandatory** **Common Criteria-based Cybersecurity Certification Scheme (EUCC)** EUCC Scheme dedicated to certifying ICT products such as hardware and software products and components is published!

- Currently document



EU Cybersecurity Certification Scheme on Common Criteria (EUCC)

- Will be di

ains

This documentation has been endorsed by the ECCG, the group gathering the EU representatives of the National Cybersecurity Certification Authorities. Some of the following documents are updated versions of the SOG-IS Supporting documents, in this case the document refers to the SOG-IS one.

Guidance Documents

- On the other hand, exist **Guidance Documents**
 - Not mandatory
 - Currently authorization of CABs and Mechanisms.

SoA on Harmonised Accreditation of Conformity Assessment Bodies	+
SoA on Technical Domain Smart Cards & Similar Devices	+
SoA on Technical Domain Hardware Devices with Security Boxes	+

<https://certification.enisa.europa.eu/certification-li>

There is still no mutual recognition...

Mutual recognitions conditions for third party countries are listed in implementing act for 'substantial' and 'high'

*Non-EU countries can recognise EUCC certifications through mutual recognition agreements, provided they meet criteria on **monitoring**, **supervision** and **vulnerability management**.*

- Common Criteria Recognition Agreement (CCRA) includes 31 countries that mutually recognize Common Criteria certificates. Europe is not one of these countries.
 - Private CABs are not considered outside EUCC.
 - Compliance responsibilities and penalties, are not required outside EUCC.
 - ENISA and NIAP committed to work together to harmonize these changes and update the CCRA.
 - Current CCRA proposal might not be acceptable from legal point of view.

CHAPTER VIII of EUCC



“MUTUAL RECOGNITION
AGREEMENTS WITH THIRD
COUNTRIES”

- They should be certified **only by public bodies** and developed as state-of-the-art documents which should be endorsed by the European Cybersecurity Certification Group.
- See **Annex II** → Protection profiles certified at AVA_VAN level 4 or 5.
- See **Annex III** → Recommended PPs (and don't expect to find NIAP PPs, but just SOG-IS PPs)

- Machine readable travel documents
- Secure signature creation devices
- Digital tachographs
- Secure integrated circuits smart cards and related devices
- Points of (payment) interaction and payment terminals
- Hardware devices with security boxes

VAN.4 and VAN.5 assurance levels

- should only be possible under specific conditions and where a specific evaluation methodology is available.
- Only possible in the next scenarios:
 1. where the **ICT product is covered by any technical domain** listed in Annex I, it shall be evaluated in accordance with the applicable state-of-the-art documents of those technical domains,
 2. where the **ICT product falls into a category of ICT products covered by a certified protection profile** that includes AVA_VAN levels 4 or 5 and that has been listed as a state-of-the-art protection profile in Annex II, it shall be evaluated in accordance with the evaluation methodology specified for that protection profile,
- **Exception:** where points a) and b) of this paragraph are not applicable and where the inclusion of a technical domain in Annex I or of a certified protection profile in Annex II is unlikely in the foreseeable future, and only in exceptional and duly justified cases, subject to the some conditions → **NEED APPROVAL NCCA.**

“Certification at AVA_VAN.4 and AVA_VAN.5 reserved for scenarios that ensure high assurance levels due to the critical nature of ICT products”

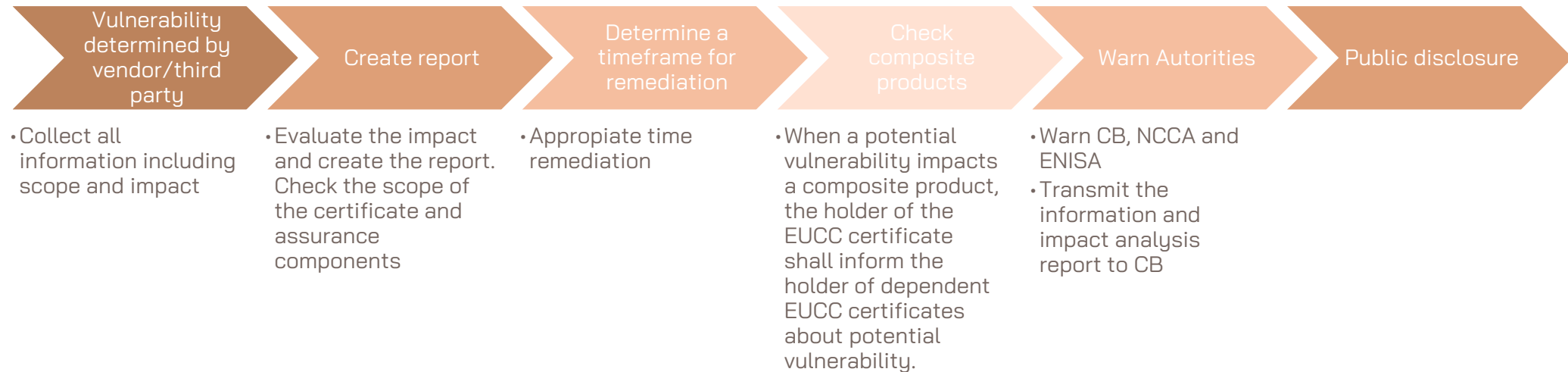
Note VAN.3 is considered ‘high’ too.

Vulnerability Handling Process shall be established for assurance continuity!



SURVEILLANCE WILL BE IN PLACE FOR THE CURRENT SCHEME

Example of flow after a vulnerability is disclosed by the manufacturer/vendor



Where necessary, the standard EN ISO/IEC 29147 should supplement the procedure for the vulnerability disclosure and ISO/IEC 30111 for vulnerability management.

EUCC Guidance for vulnerability management and disclosure is being developed.

What is a patch management composed of?



the **process for the development and release** of the patch for the ICT product



the **technical mechanism and functions** for the adoption of the patch into the ICT product



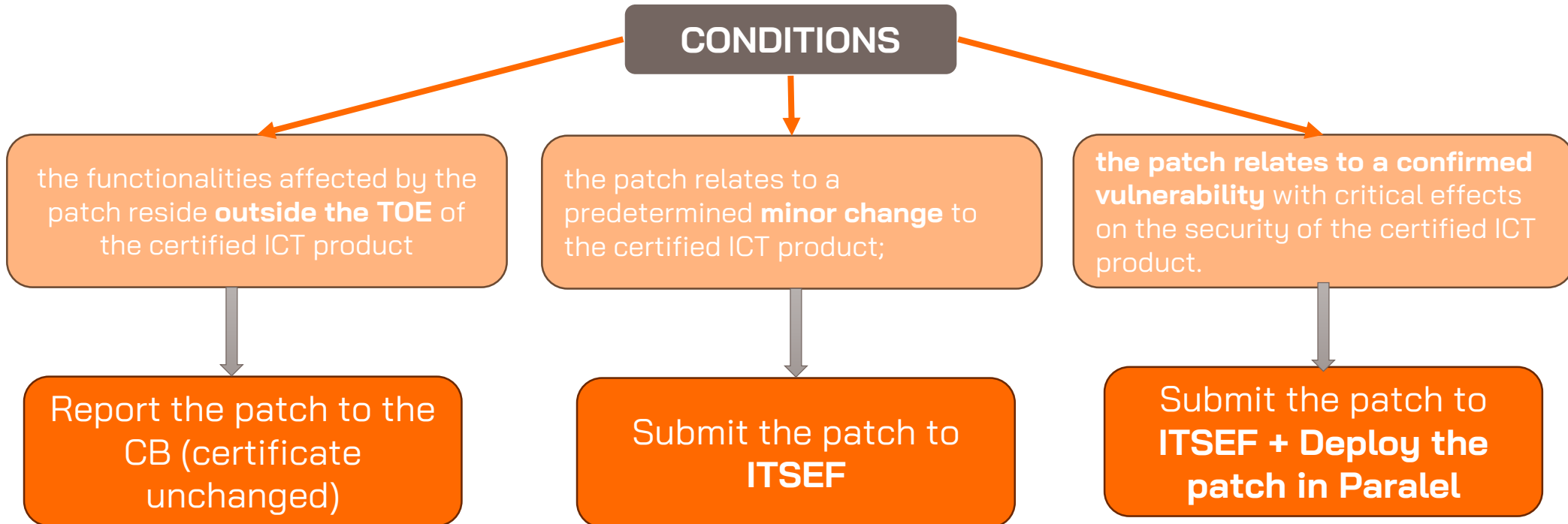
a set of evaluation activities related to the effectiveness and performance of the technical mechanisms

- Several initiatives such as include extended components on ALC

Check ISO/IEC
TS 9569:2023

Patch Management

If the certification included in the scope of certification a patch management procedure and a new patch is released the following conditions apply based on the contents of the patch:

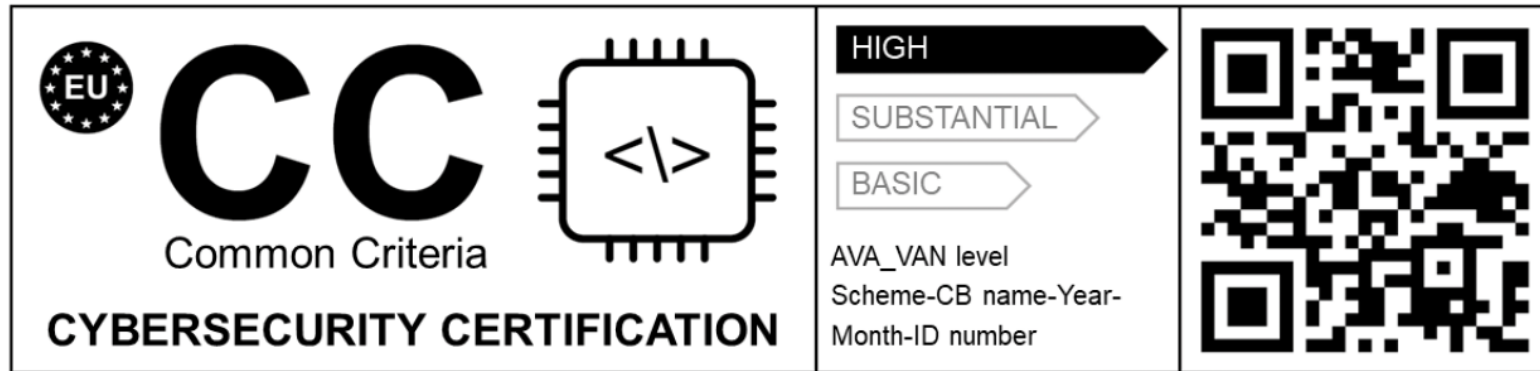


5 working days

I am obligated to include a Mark?

It is voluntary to affix the mark and label in your ICT product

- The EUCC has defined a new label and associated mark, established for the European Cybersecurity Certification Framework, and specifically implemented for this scheme.
- This label is to be used in combination with a **QR code** with a link to a website providing more details.

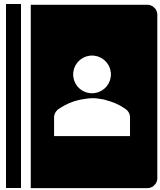


ARTICLE 11 and ANNEX IX.



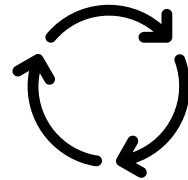
What's NEXT?

What is expected from now on?



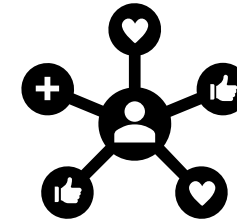
Maintenance of EUCC documents

Maintenance of the documents shall be performed as well as inclusion of new state of the art documents



AVA_VAN.3 and Substantial level

Well-defined for AVA_VAN.4 and 5, but what about AVA_VAN.3 and lower levels, 'Substantial'



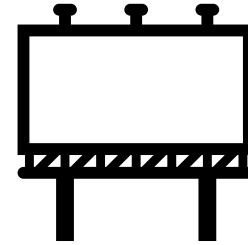
Interplay with other regulations

Interaction with other regulation (CRA, NIS2) and efforts to harmonize globally the efforts



Monitoring Guidance

Monitoring and
surveillance guidance



Sites recognition

How sites will be
recognized? Validity?

Thanks!



Join us on



TESTING AND CERTIFICATION CENTER

www.appluslaboratories.com