RED ALERT LABS
IoT Security

TrustBoost Training - Day 4:
EUCC, the Common Criteria based European cybersecurity certification scheme

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

12/11/2024

TrustBoost

+ Q&A

The Training Content

From Candidate to Implementing Act

EUCC Implementing Act

Key Concerns Raised

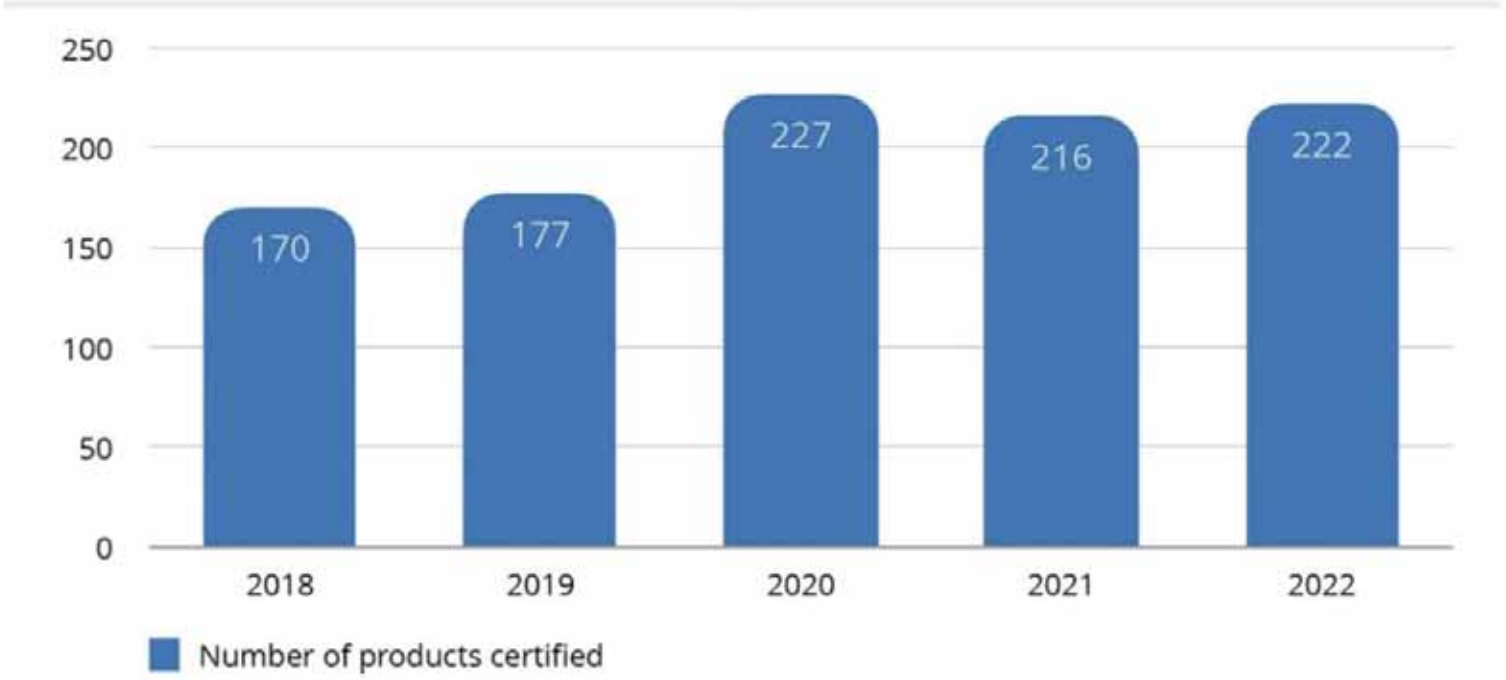
EUCC Vulnerability Management

EUCC & CRA

RED ALERT LABS
IoT Security

ENISA: Market of Cybersecurity Assessments - Jan 31, 2024

Common Criteria certified products in the European Union up to 2022



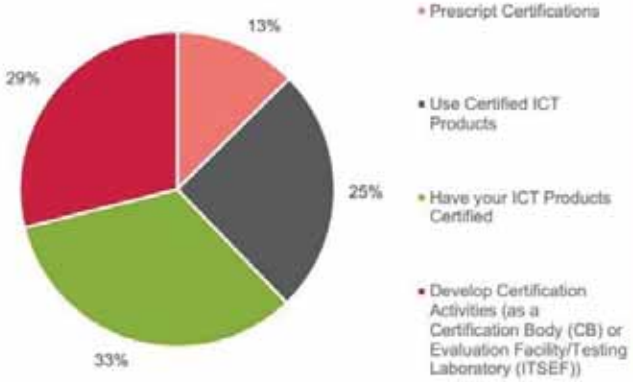
EUCC
A EUROPEAN
Scheme

EUCC SCHEME

What is EUCC?

Intention to use the EUCC scheme

82% of the participants (61% outside EU/EEA), for the following usages (in line with the profile of participants):



All MS participants (100%) indicated they intend to use the EUCC scheme.

RED ALERT LABS
IoT Security

EUCC Highlights

- Allows for composite certification
- Harmonised conditions for vulnerability handling and disclosure;
- Voluntary scheme unless it is mandated by policy or regulation
- **EUCC**
- Clearly defined rules on monitoring and handling non-compliance and non-conformity
- Introduces a new patch management mechanism to support vulnerability handling
- Use of a framework-based label and a QR code to ensure easy access to accurate certification information

RED ALERT LABS
IoT Security

EUCC SCHEME GOALS

EUCC Common Criteria Certification Scheme

Scope: Product Schematic

Any type of IT Product that includes Security Features

Follow the Maintenance Working Group

Organization of the maintenance plan

Transition from SOG-IS

Transition and implementation of new plan

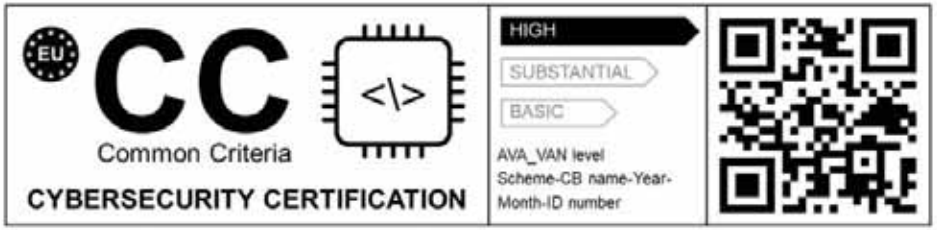
Future Actions

Participation in ENISA work, Accreditation of certification centres, Negotiation and adoption of the Implementing Act

The EUCC Common Criteria Certification Scheme provides a comprehensive framework for the security of IT products, with substantial and high security assurance levels

EUCC SCHEME HIGHLIGHTS

- The necessary information for certification shall include relevant **evidence** for evaluation. It may include previous evaluation results.
- It is foreseen that a **label** is associated with the European Cybersecurity Certification Framework, and specifically implemented for each scheme, including the EUCC scheme.



EUCC SCHEME HIGHLIGHTS

- Retention of records by CAB shall follow the general rules of accreditation standards ISO/IEC 17065 and ISO/IEC 17025.
- Some EU schemes participating to the SOG-IS MRA cover the same type or categories of ICT products but may go beyond the EUCC in terms of national certification or cover partly the EUCC assurance levels.
- A certificate contains the most relevant information for the identification of the product and the assurance level obtained.
- Information associated to a certified ICT product shall be available for a period of at least five years after the expiration date of the certificate.

EUCC SCHEME HIGHLIGHTS

Maximum period of validity of certificates shall be 5 years

ENISA will publish the certificates with appropriate relevant information attached. To manage accurate and up to date dataflows, ENISA will establish conditions and/or guidance for the delivery and publication of information.

The establishment of a mutual recognition agreement (MRA) between the participants shall support mutual recognition with third countries. Preliminary conditions for mutual recognition of certificates and for peer assessment are defined.

EUCC SCHEME HIGHLIGHTS

- Certificates will provide a link to Supplementary cybersecurity information. Such information may be required for certification activities.
- In addition to the certification of ICT products, the scheme shall as well cover the certification of Protection Profiles.
- Security of information used for and created by certification shall be insured.
- Based on its experience, the AHWG recommends a transition period of two (2) years to adopt the new rules while introducing no market disruption. Any shorter period should be accompanied with temporary derogations to the EUCC rules.
- Groups of experts involving NCCA, CAB and their testing facilities, and manufactures or providers of ICT products should be considered as to further develop harmonised requirements for the scheme.

QUIZ

- **Name one of the key features in the EUCC**
- **EUCC is applicable to ICT products, processes and services certification, TRUE or FALSE**
- **What is the maximum validity of EUCC certificates ?**

EUCC Stakeholders

As defined in Cybersecurity Act

- SCCG
- NCCA
- ECCG
- AHWG
- ENISA

Stakeholders

Stakeholders

THE COORDINATION CENTER

ENISA

EUROPEAN CYBERSECURITY CERTIFICATION GROUP (ECCG) Article 62

Prepare a candidate scheme or to review an existing European cybersecurity certification scheme:

- based on the Union rolling work program.
- which is not included in the Union rolling work program.

Transmits Candidate scheme to the Commission after interacting with ECCG, SCCG, Adhoc working Group and other Industry and standardisation bodies

RED ALERT LABS
IoT Security

Stakeholders

THE POWER CENTER

ECCG

EUROPEAN CYBERSECURITY CERTIFICATION GROUP (ECCG) Article 62

Comprises national cybersecurity certification authorities from member countries.

Advise & assist ENISA in EU CSA implementation.

Advise & assist ENISA in preparing candidate schemes. Article 48

Facilitate cooperation between national cybersecurity certification authorities

Facilitate alignment of European cybersecurity certification schemes with internationally recognised standards

NCCA

NATIONAL CYBERSECURITY CERTIFICATION AUTHORITIES (NCCA) ARTICLE 62.2

Each Member State designates one or more national cybersecurity certification authorities in its territory or with mutual agreement, in the territory of another Member State

Monitor & supervise activities of CABs & Public bodies functioning as CABs

Enforce rules as described in EU certification schemes

RED ALERT LABS
IoT Security

Stakeholders

THE HELP CENTER

SCCG

STAKEHOLDER CYBERSECURITY CERTIFICATION GROUP (SCCG) ARTICLE 22

Composed of members selected from amongst recognised experts representing the relevant stakeholders.

Advice the Commission & ECCG on the need for additional certification schemes.

Advise ENISA on general and strategic matters relating to the market, cybersecurity certification, and standardisation.

Advise the Commission on strategic issues regarding the EU certification framework.

Assist the commission in the preparation of the Union rolling work programme

AHWG

ADHOC WORKING GROUP (AWG) Article 20

Appointed by the Executive Director of ENISA after notifying the management board.

Tasked with providing to ENISA, specific advice and expertise on a subject matter e.g. a candidate scheme.

Committee members must declare any conflict of interest

RED ALERT LABS
IoT Security

Stakeholders

INTERNATIONAL COOPERATION

Third Countries

ARTICLE 12

ENISA shall contribute to the Union's efforts to cooperate with third countries and international organisations as well as within relevant international cooperation frameworks by:

- engaging, where appropriate, as an observer in the organisation of international exercises;

- facilitating, at the request of the Commission, the exchange of best practices;

- providing, at the request of the Commission, its expertise;

- providing recommendations and assistance to the Commission on matters concerning agreements for the mutual recognition

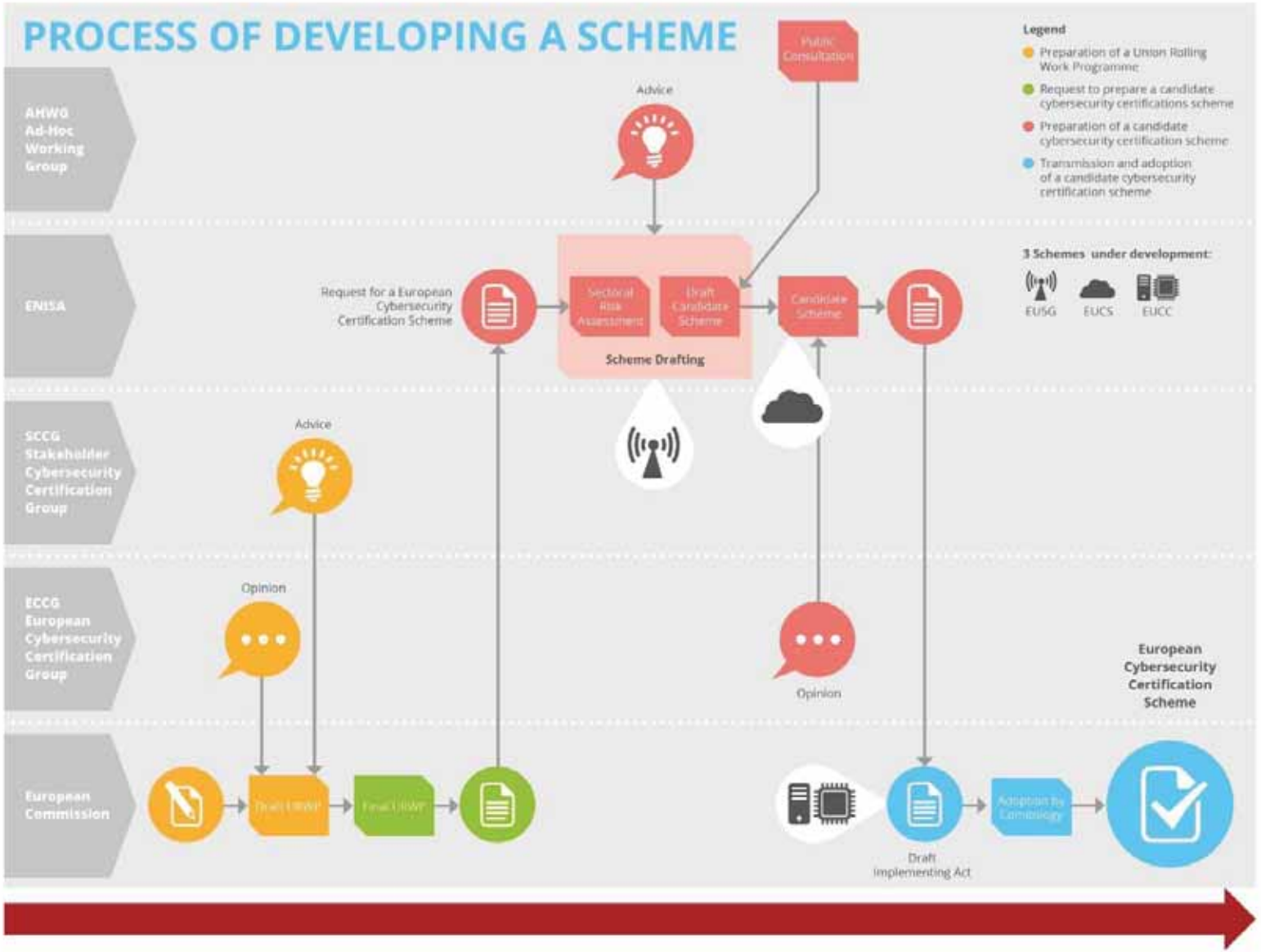
RED ALERT LABS
IoT Security

Highlights...

EUCC Implementing Act

RED ALERT LABS
IoT Security

From Condidate to Scheme



The EUCC to Adoption Timeline

RED ALERT LABS
IoT Security

EUCC implementing act

General Provisions (**6 articles**)	Certification of ICT products (**8 articles**)	Certification of Protection Profiles (**6 articles**)	Conformity Assessment Bodies (**4 articles**)
Monitoring, non-conformity and non-compliance (**7 articles**)	Vulnerability management and disclosure (**8 articles**)	Retention, disclosure and protection of information (**4 articles**)	Mutual recognition agreements with third countries (**1 article**)
Peer assessment of certification bodies (**3 articles**)	Maintenance of the scheme (**1 article**)	Final provisions (**2 articles**)	
State of the art documents (Annex I – III)	Assurance continuity (Annex IV)	Sundry requirements (Annexes V – IX)	

RED ALERT LABS
IoT Security

What didn't change (with regards to the Candidate Scheme)...

EUCC mapping with AVA_VAN levels

EUCC assurance levels will be mapped to AVA_VAN assurance levels

Authorization of CABs

Conformity assessment bodies (CABs) will require authorization on top of accreditation to issue EUCCs

Mutual recognition conditions

Conditions will be defined for mutual recognition of EUCCs issued in different member states

The EUCC scheme will define key provisions for assurance levels, CAB authorization, certificate duration, and mutual recognition to enable a harmonized certification framework.

Some New Provisions...

SOTA docs

with dynamic updates

Transition period

12 months, except for CABs notifications, ...

CCRA participation

Member States should end their participation in the CCRA in the areas covered by this Regulation

RED ALERT LABS
IoT Security

Guidelines for Certificate Validity Duration

- ## Certification bodies should determine certificate validity

  Certification bodies should decide on the duration of the validity of certificates based on the life cycle and version management policies of the ICT product. The validity should not exceed five years and should align with practices in other Member States.

- ## Validity duration recommendations

  The maximum duration is five years. Align with practices in other Member States for the same ICT product.

- ## Key factors in determining validity duration

  Life cycle and version management policies of the ICT product should inform the duration.

RED ALERT LABS
IoT Security

ECCG & MG

The European Cybersecurity Certification Group plays an important role in the scheme

Through cooperation with the private sector, the creation of specialised subgroups and relevant preparatory work

The Maintenance Group assists the Commission

With maintenance of the scheme and any assistance requested

The European Cybersecurity Certification Group maintains the scheme through cooperation, preparatory work, and assistance to the Commission.

EUCC Implementing Act

Selected Provisions

RED ALERT LABS
IoT Security

General Provisions (1-2)

Scope of EUCC

EUCC applies to all ICT products submitted for certification and the protection profiles used in the certification process.

Common Criteria

Refers to the ISO/IEC 15408 standard, which sets the evaluation criteria for IT security.

Common Evaluation Methodology

Refers to the ISO/IEC 18045 standard, detailing the methods used in security evaluations.

Target of Evaluation

Defines the ICT product or protection profile that is the subject of the security evaluation.

Security Target

Specifies the security requirements, security functions, and security assurance measures for the Target of Evaluation.

Intended Use & Risk Analysis

- **Applicants SHOULD provide usage documentation**
  Applicants for EUCC certification provide documentation on intended product usage.

- **Applicants SHOULD provide risk analysis**
  Applicants also provide analysis of risk levels associated with the intended usage.

RED ALERT LABS
IoT Security

General Provisions (3-6)

Evaluation Standards

Evaluations under EUCC must adhere to CC and CEM.

Objectivity and Independence

Certification requires independent third-party evaluations, not self-assessment.

The EUCC establishes a robust framework for cybersecurity certification, promoting trust and security in ICT products across the EU through the implementation of these comprehensive provisions.

Certification at AVA_VAN Level 4 or 5 (7)

Rigorous Security Evaluation

Certification at AVA_VAN level 4 or 5 is reserved for scenarios that ensure high assurance levels due to the critical nature of the ICT products.

(scenario a) Technical Domains in Annex I

If an ICT product falls under any technical domain listed in Annex I, it must be evaluated using the relevant state-of-the-art documents and methodologies specific to that domain, ensuring the security measures meet AVA_VAN level 4 or 5 standards.

Example: Smart Card Devices

A smart card device, such as a secure payment card, falls under this category

The certification at AVA_VAN level 4 or 5 ensures that critical ICT products undergo a rigorous security evaluation process, with specific requirements based on the technical domains listed in Annex I.

Certification at AVA_VAN Level 4 or 5 (7)

Certified Protection Profile (Scenario b)

If an ICT product belongs to a category covered by a certified protection profile that includes AVA_VAN levels 4 or 5, it must be evaluated according to the methodologies specified in that protection profile.

Exceptional and Duly Justified Cases (Scenario c)

If neither Scenario (a) nor (b) is applicable, and it is unlikely that the technical domain or PP will be included in the foreseeable future, certification can be sought in exceptional and duly justified cases.

Example (scenario b)

A HSM used in financial transactions falls under a certified PP for such devices listed in Annex II and would be evaluated based on the security requirements and evaluation methodologies specified in the PP.

Example (scenario c)

A new type of biometric authentication device that does not yet fall under any existing technical domain or protection profile could be considered for certification. The CAB must notify the NCCA with a detailed justification and proposed evaluation methodology for approval.

RED ALERT LABS
IoT Security

Article 8 - Info Necessary for Certification

- **Provide all information to CB & ITSEF**
  Relevant evidence & details on product & code
- **Can provide prior cert evidence**
  From EUCC, other EU schemes, national schemes
- **ITSEF reuses evaluation results**
  If evidence conforms & authenticity confirmed
- **Provide composite elements**
  If composite certification allowed
- **Provide other information**
  Vulnerability management/disclosure, Cybersecurity information for certified products
- **Retain information for 5 years after the expiry of the certificate**
  The retention concerns the certification body, the ITSEF and the applicant

RED ALERT LABS
IoT Security

CONTENT AND FORMAT OF CERTIFICATES (Article 10 + ANNEX VII)

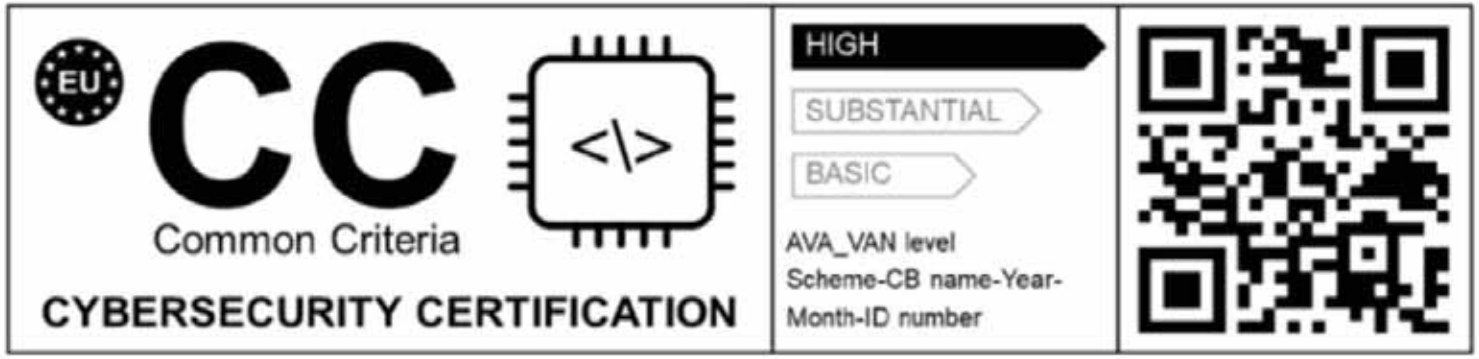
- CABs will have to adopt the new **content** and **format** of the EUCC **certificate**, that, amongst other requirements includes:
  - A unique identifier established by the certification body issuing the certificate;
  - Information related to the certified ICT product or protection profile and the holder of the certificate (name and type of the product, version, link to the website, ...),
  - Information related to the evaluation and certification of the ICT product or protection profile (name and addressed of CB, ref to certification report, period of validity, ...)
  - The mark and label associated with the certificate in accordance with Article 11.

Am I required to put a Mark or a Label on my Certified Product ?

RED ALERT LABS
IoT Security

MARKS AND LABELS (Article 11 + ANNEX IX)

- 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** provided by ENISA once a certificate is issued.
- The label needs to entail obligated information as defined under the EUCC.



***Note*: The use of new EUCC mark and label on the certified product is voluntary**

What are the rules regarding the validity period of an EUCC certificate and under what conditions can it be extended?

RED ALERT LABS
IoT Security

Period of validity of EUCC certificate (12)

- **Certification bodies shall determine certificate validity**

  The certification body shall set a period of validity for each EUCC certificate issued taking into account the characteristics of the certified ICT product.

- **Validity duration < 5 years**

  The maximum duration is five years. Align with practices in other Member States for the same ICT product.

- **Key factors in determining validity duration**

  Life cycle and version management policies of the ICT product should inform the duration.

- **Exceptional cases > 5 years**

  subject to the prior approval of the NCCA. The NCCA shall notify the ECCG of the granted approval without undue delay.

RED ALERT LABS
IoT Security

POST-ACQUISITION OBLIGATIONS OF EUCC CERTIFICATE HOLDERS

Regularly monitor vulnerability intelligence (article 27)

Monitor emerging vulnerabilities in the certified product throughout the certificate's duration

Provide assistance in rectifying non-compliances (article 29)

Assist in addressing any non-compliances identified during audits

Have a process to handle newly discovered vulnerabilities per EUCC guidelines

Certificate holders must uphold key responsibilities during the certificate's duration to maintain compliance

How are PPs evaluated, and under what circumstances can they be certified ?

RED ALERT LABS
IoT Security

Article 15 - Certification of PPs

- **Applicable elements of standards**
  the applicable elements of the standards referred to in Article 3 (CC, CEM)

- **Applicable state-of-the-art document**
  document related to the harmonised accreditation of conformity assessment bodies: 'Accreditation of ITSEFs for the EUCC', initially approved by ECCG on 20 October 2023.

- **Level of risk**
  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

RED ALERT LABS
IoT Security

PPs

Protection Profiles should be certified by approved bodies

PPs should only be certified by public or private certification bodies approved by the national cybersecurity authority

PPs should be published as state-of-the-art docs

PPs should be published as SOTA docs for that ICT product category

PPs have key role for high assurance certification

Due to their key role, PPs should be developed as state-of-the-art and endorsed by the EC Cybersecurity Cert Group

Certified PPs should be monitored by authorities

Certified PPs should be monitored by national cybersecurity authorities for compliance

Certified Protection Profiles play a critical role in ensuring high assurance cybersecurity certification of ICT products.

How does the NCCA conduct its monitoring activities, and what is the annual sampling requirement for EUCC certificates?

RED ALERT LABS
IoT Security

Compliance Monitoring by NCCAs (25)

Annual sampling of EUCC certificates

The NCCA hall sample at least 4% of the EUCC certificates annually based on a risk assessment.

Cooperation with market surveillance authorities

The NCCA shall cooperate with other market surveillance authorities for the sampling of EUCC certificates.

Monitoring compliance

CBs and, if necessary, ITSEF shall assist the national cybersecurity certification authority in monitoring compliance with the EUCC requirements.

monitor the compliance of: (a) the CB and the ITSEF (b) the holders of an EUCC certificate (c) the certified ICT products; (d) the assurance expressed in the EUCC certificate addressing the evolving threat landscape.

What are the monitoring responsibilities of the CB regarding certificate holders, certified ICT products, and PPs?

RED ALERT LABS
IoT Security

Compliance Monitoring by the CB (26)

Monitor certificate holder compliance

The CB shall monitor the compliance of the holders of a certificate with their obligations under this Regulation and Regulation (EU) 2019/881 towards the EUCC certificate that was issued by the certification body.

Monitor certified product security

The CB shall monitor the compliance of the ICT products it has certified with their respective security requirements.

Monitor certified protection profiles

The CB shall monitor the assurance expressed in the certified protection profiles.

The certification body has a critical role in ensuring the integrity and compliance of the EUCC certification process, monitoring certificate holders, certified products, and protection profiles.

What responsibilities does the holder of an EUCC certificate have in monitoring the conformity ?

RED ALERT LABS
IoT Security

Monitoring Vulnerability by the Certificate Holder (27)

Known Dependencies

Understand and track the software and hardware components that the certified ICT product relies on.

User and Security Researcher Reports

Review and address vulnerability reports received directly from users and security researchers.

External Sources

Monitor other channels for vulnerability information, such as industry reports and security advisories.

Proactively monitor and address vulnerability information from various sources to ensure the security of the certified ICT product.

Example of Vulnerability Monitoring (27)

RED ALERT LABS
IoT Security

Vulnerability Management Procedures (33)

Establishing Vulnerability Management Procedures	Receiving Vulnerability Information	Vulnerability Impact Analysis	Composite Products	Information Transmission
set up and maintain necessary procedures for managing vulnerabilities, supplemented by EN ISO/IEC 30111 procedures.	must maintain and publish methods to receive information on vulnerabilities	carry out a vulnerability impact analysis.	must inform the holders of dependent EUCC certificates.	transmit all relevant information about potential vulnerabilities to that certification body.

RED ALERT LABS
IoT Security

Vulnerability Impact Analysis (34)

Target of Evaluation and Assurance Statements

Vulnerability impact analysis must reference the specific target of evaluation and the assurance statements in the EUCC certificate.

Timeframe for Analysis

The analysis should be carried out in a timeframe that reflects the exploitability and criticality of the potential vulnerability.

Attack Potential Calculation

If applicable, an attack potential calculation must be performed following the relevant methodology in the standards mentioned in Article 3 and the state-of-the-art documents listed in Annex I. The AVA_VAN level (assurance vulnerability analysis level) of the EUCC certificate must be considered in the calculation.

The vulnerability impact analysis is a crucial part of the EUCC certification process, ensuring that the analysis is thorough, timely, and considers the specific target and assurance statements, as well as the attack potential calculation.

Step by Step...

RED ALERT LABS
IoT Security

Publication of the vulnerability (39)

Continuously monitor the ICT product and identify any vulnerabilities as part of the certification process.

Keep detailed records of all identified vulnerabilities, including their nature, potential impact, and remediation actions taken.

Once the certificate is withdrawn, ensure that all known and remediated vulnerabilities are disclosed to the public.

Use the European vulnerability database established under Directive (EU) 2022/2555 to register the identified vulnerabilities, providing detailed information about them and how they were addressed.

If necessary, vulnerabilities can also be registered in other designated online repositories as per Regulation (EU) 2019/881.

Maintain comprehensive records of all disclosed vulnerabilities and the corresponding remediation efforts, keeping them securely and making them available for verification when required.

RED ALERT LABS
IoT Security

Under what conditions can a CB suspend an EUCC certificate, and what steps must the certificate holder take upon receiving notification of suspension?

RED ALERT LABS
IoT Security

Consequences of non-conformity (28)

EUCC Certificate Suspended

The certification body may suspend, without undue delay, the EUCC certificate in accordance with Article 30 in case of emergency, or where the holder of the EUCC certificate does not duly cooperate with the certification body

Remedial Action Timeline

Upon receipt of the information referred to in paragraph 1, the holder of the EUCC certificate shall within the time period set by the certification body, which shall not exceed **30 days**, propose to the certification body the remedial action necessary to address the non-conformity.

RED ALERT LABS
IoT Security

What are the consequences for a certificate holder failing to meet their obligations?

RED ALERT LABS
IoT Security

Consequences of non-compliance by the holder of certificate (29)

Non-compliance with Commitments and Obligations

Non-compliance with commitments and obligations as outlined in Articles 9(2), 17(2), 27, and 41.

Non-compliance with Regulation (EU) 2019/881

Non-compliance with Article 56(8) of Regulation (EU) 2019/881 or Chapter VI of this Regulation.

Remedial Action Period

A time period of no more than **30 days** is set for the certificate holder to take remedial action.

Actions in Case of Non-Compliance

If appropriate remedial action is not proposed within the specified period, the certificate will be suspended or withdrawn. Continued or recurring non-compliance will lead to the withdrawal of the EUCC certificate.

RED ALERT LABS
IoT Security

Example 1

EUCC Certificate Holder

A company holds an EUCC certificate for a security software product.

Routine Audit

During a routine audit, the certification body finds that the company failed to apply necessary security patches.

Violation of Article 27

The failure to apply security patches violates Article 27 of the EUCC requirements.

Notification and Grace Period

The certification body notifies the company and sets a 30-day period to implement the required security patches.

Consequences of Non-Compliance

If the company fails to comply within the 30-day period, the certificate is suspended. Continued non-compliance will lead to the withdrawal of the certificate.

RED ALERT LABS
IoT Security

Example 2

Vulnerability Discovery

ICT product certified under EUCC found a vulnerability.

Notification Requirement

The certificate holder is required to inform the relevant authorities per Article 56(8).

Certification Body

Upon discovery, the certification body sets a 30-day period for the company to disclose the vulnerability and provide a remediation plan.

Company Inaction

Failure to disclose the vulnerability and provide a remediation plan within 30 days.

Certification Suspension

The certification body suspends the certificate due to the company's failure to act.

Potential Certificate Withdrawal

The certification body may withdraw the certificate if the company continues to not disclose the vulnerability and provide a remediation plan.

RED ALERT LABS
IoT Security

Will national cybersecurity certification schemes cease to exist ?

RED ALERT LABS
IoT Security

ANNEX I: Technical domains and state-of-the-art documents

Annexes, SOTA docs and Guidance

State-of-the-art documents

State-of-the-art documents could be technical domains dependent like MSSR

Some guidance were initialized under the ENISA AHWG

Guidance will have to be updated and potentially added at later stage.

Technical Domains

common technical framework related to a particular technology for the harmonized certification with a set of characteristic security requirements;

Different types of documents being created as part of the EUCC IA.

ANNEX I: State Of The Art

State-of-the-art documents

Documents that specify evaluation methods, techniques and tools to certify ICT products or security requirements

Harmonize evaluation

Applies to generic ICT product categories to harmonise evaluation in technical domains or of protection profiles

State-of-the-art documents standardize the evaluation of ICT products across organizations.

ANNEX I/II/III: List of SOTA Documents

- Dynamic documents from ECCG

The act refers to dynamic docs initiated by ECCG

- Annex I lists SOTA docs

Legal updates complex by referencing annex docs

- PP list not up-to-date

List of Protection Profiles (Annex II ANNEX III) seems outdated

Future PPs will need new delegated acts

What are the steps and conditions for applying patches under the EUCC certification scheme?

RED ALERT LABS
IoT Security

Patch Management (Annex IV section 4)

- **Patch management provides structured process for updating certified products**

  Patch management procedure allows for updating certified ICT products in a structured way. The procedure and mechanism can be used after certification under the CAB's responsibility.

- **Conditions for including patch mechanism in certification**

  The applicant may include a patch mechanism in the certification if: the patch is outside the TOE, it is a predetermined minor change, or relates to a critical vulnerability.

- **Patch management option does not apply to addressing non-critical vulnerabilities, which should be handled in accordance with Article 13 of the EUCC Regulation.**

RED ALERT LABS
IoT Security

Steps for Patch Application (Annex IV section 4)

- **The holder of the certificate may apply the certified patch**

  Within 5 working days, the holder of the certificate may apply the patch produced according to the certified patch management procedure to the concerned certified ICT product.

- **Report the patch in case 2(a)**

  In case **the patch is outside the TOE**, report the patch to the certification body. The certification body will not change the EUCC certificate.

- **Submit the patch for review in case 2(b)**

  In case **it is a predetermined minor change**, submit the patch to the ITSEF for review. The ITSEF informs the certification body and appropriate action is taken on the EUCC certificate.

- **Submit the patch for re-evaluation in case 2(c)**

  In case **it relates to a confirmed critical vulnerability**, submit the patch to the ITSEF for re-evaluation. The patch can be deployed in parallel. The ITSEF informs the certification body to start certification activities.

RED ALERT LABS
IoT Security

Article 33 - Vulnerability management procedures

- **Implement vulnerability management procedures**
  Holder of EUCC certificate should implement necessary vulnerability management procedures and ensure procedures are embedded in their organisation
- **Perform vulnerability impact analysis**
  When becoming aware of a potential vulnerability, the holder should perform a vulnerability impact analysis
- **Transmit assessment report**
  Where analysis confirms exploitability, the holder of an EUCC certificate shall transmit all relevant information about potential vulnerabilities to the certification body

Follow ISO 29147 for vulnerability disclosure procedures

EUCC vs CC

EVALUATION STANDARDS

Evaluations shall be based on the following standards:

The EUCC scheme is based on the CC and the CEM, with an additional set of supporting elements, further defined

- Common Criteria for Information Technology Security Evaluation, under their applicable ISO/IEC 15408 version or under their applicable version published on CC website and composed of:
  CC Part 1: Introduction and general model;
  CC Part 2: Security functional components;
  CC Part 3: Security assurance components;

- Common Methodology for Information Technology Security Evaluation, under its applicable ISO/IEC 18045 version or under its applicable version published on CC website, simply referred to as the CEM into this candidate scheme.

Certificates issued shall indicate which version/release of the CC and CEM have been used for the evaluation and certification. In addition, the following standards shall apply for the accreditation of the conformity assessment bodies that perform the evaluation and certification activities:

- ISO 17065: for the conformity assessment body or national authority in charge of the activities of certification, hereinafter designated as certification body (CB).

- ISO 17025: for the part of a third-party conformity assessment body or national authority, or the subcontractor of a CAB or national authority, that oversees the activities of evaluation, hereinafter designated as testing laboratory (ITSEF).

ASSURANCE LEVELS

The EUCC scheme covers assurance levels 'substantial' and 'high' of the CSA.

Certification under this scheme shall cover the assurance levels 'substantial' and 'high' of the CSA. The assignment to the assurance levels of the CSA shall be based on the use of the assurance components for vulnerability assessment defined in CC Part 3 as follows:

ASSURANCE LEVELS

The EUCC scheme covers assurance levels 'substantial' and 'high' of the CSA.

All dependencies, as defined in the CC Part 3, that apply to the selected AVA_VAN level shall be applied and included into the applicable Security Assurance Requirements for the evaluation. Preferably, all assurance components of the evaluation assurance level (EAL) defined by the CC Part 3 that is associated to the selected AVA_VAN level shall be applied, in accordance with the associated table.

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
Guidance documents	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
Security Target evaluation	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

Table 1: Evaluation assurance level summary (excerpt from CC Part 3)

ASSESSMENT TYPE

The scheme does not permit conformity self-assessments

Third-party Assessments

Self assessments

REQUIREMENTS APPLICABLE TO A CAB

CAB, including their testing laboratories, are subject to specific requirements in addition to their accreditation for the 'high' assurance level of certification

In accordance with Annex.19 of the CSA, a certification body (CB) shall be accredited with the relevant standard, ISO/IEC 17065. It shall in addition be authorised by its NCCA to produce certificates at the assurance level 'high' of the CSA.

For the assurance level 'substantial', this technical competence shall be assessed through the accreditation of the testing laboratory according to ISO/IEC 17025.

In addition, the EUCC scheme provides for the following specific requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements:

- specific requirements shall concern technical competences related to specific testing activities and shall apply only as regards certificates issued at assurance level 'high'.
- requirements shall apply both to internal testing laboratories of conformity assessment bodies and to the external ones in cases where testing is performed by a subcontractor.

EUCC compatibility

SECURITY FUNCTIONAL REQUIREMENTS (SFRS) AND SECURITY ASSURANCE REQUIREMENTS (SARS)

The new EUCC certification can be implemented on top of both the older and newer versions of the Common Criteria standard. From that point of view, there is no change for SFRs and SARs based on CC Part 2 and CC Part 3, as the EUCC scheme builds upon the core elements of CC and introduces supplementary criteria alongside the established CC and Common Methodology for Information Technology Security Evaluation (CEM) protocols.

Of course, between the older (CC V3.1) and the newer (CC:2022) versions of the Common Criteria, there are differences in terms of the SFRs and SARs, which developers and laboratories need to consider.

QUIZ

- **Which body is ISO 17025 applicable for ?**
- **Conformity self assessments are used in EUCC. True or False?**
- **What standards are EUCC evaluations based on?**
- **EUCC is a horizontal scheme. True or false?**

ANY IMPACTS ON THE EUCC CANDIDATE SCHEME ?

CC:2022 impact on EUCC

Evaluation Approach & Impacts on EUCC

Impacts on EUCC

- "Attack-based approach" does not affect the candidate EUCC scheme version 1.1
- The "specification-based approach", is anticipated to have the following impacts in case it is used to deliver EUCC certificates:
  - where adherence to the assurance level high of the CSA is needed, the "attack-based approach" is required
  - "specification-based approach", on the contrary, may be a useful addition for evaluations at the substantial level
  - as the "specification-based" approach uses exact conformance PPs
  - evolutions in the state-of-the-art is considered by updating the PPs or the supporting documents describing the requirements and the evaluation methodology;

Modularity & Impacts on EUCC

- **Modularity**
  - New version of the standards supports new modularity capabilities, which relate to:
    - the modularity of the evaluation process, through new composition mechanisms.
    - the modularity of requirements within a single TOE, through the following mechanisms:
      - o functional and assurance packages (notably EALs).
      - o modular PPs,
      - o multi-assurance evaluation paradigm
      - o requirement bundling

Modularity & Impacts on EUCC

- **Composition : Impact on EUCC**
  - At this stage, the use of the Network or bi-directional or the Embedded composition models within the EUCC scheme seems premature. The EUCC community should first search to establish and promote harmonised specific mechanisms for these composition models, and where this has priority, it should be taken into consideration into the activities to be further supported by the maintenance organisation put in place for the scheme.
  - The Layered approach, on the other hand, can now benefit to a broader variety of products than the “traditional” ICs/platforms/smart cards, as today covered by Annex 6, COMPOSITE PRODUCT EVALUATION FOR SMARTCARDS AND SIMILAR DEVICES of the candidate EUCC scheme v1.1.1.

Modularity & Impacts on EUCC

- **Packages**
  - Packages are sets of security (either assurance or functional) components or requirements. New assurance packages have been introduced in the new version of ISO/IEC 15408-5:
    - COMP
    - PPA
    - STA
- **Packages : Impact on EUCC**
  - New packages introduced ***do not require any change into the candidate EUCC scheme*** and have potential immediate applicability.

Modularity & Impacts on EUCC

- **Modular PPs**
  - Allow addressing TOE's possible functional variations, and are mostly intended to describe TOEs built out of modules, including modules that are sourced from different developers and/or are evaluated separately, e.g.:
    - alternative architecture choices ;
    - optional features or modules
  - PP-Modules rely on one or more base PPs and may introduce changes to their TOE types. PP-Modules may use other PP-Modules as a base. They may carry a specific set of assurance components for the module
  - The evaluation of PP-Modules is enforced through the evaluation of the configurations they belong to, thus ensuring their consistency. The ACE assurance class, which complements APE, covers the evaluation of PP-Configurations and their PP-Modules. The evaluation of PPs, PP-Modules and PP-Configurations can be reused as usual in the evaluation of STs.
- **Modular PPs : Impact on EUCC**
  - No impact

Modularity & Impacts on EUCC

- **Multi-Assurance evaluations**
  - Defines a flexible framework using predefined EALs from ISO/IEC 15408-5 or assurance components from ISO/IEC 15408-3
  - Allows addressing heterogeneous products and evaluating modular TOEs that require different assurance for different parts of their functionality.
- **Multi-Assurance evaluations : Impact on EUCC**
  - Do not raise any applicability issue, and the conditions associated with the different sub-TSFs evaluations will continue to depend on the individual AVA_VAN level they intend to achieve.

Modularity & Impacts on EUCC

- **Others**
  - ADV_SPM has been redefined
  - The evaluation method of the standards now covers evaluations using formal methods, where this was before left to national schemes. Moreover, the formal model coverage has been clarified, as to avoid misleading STs.
- **Others : Impact on EUCC**
  - This improvement is ***not considered to have any impact on the candidate EUCC scheme v1.1***.

Towards a State of the Art Document

EUCC
Vulnerability Management

Chapter VI of the EUCC Regulation

RED ALERT LABS
IoT Security

Article 33: Vulnerability management procedure

- **Establishment and maintenance of vulnerability management procedures**

  The holder of an EUCC certificate must establish and maintain necessary vulnerability management procedures following ISO/IEC 30111 and relevant documents in Annex I.

- **Following ISO/IEC 30111 general steps**

  Preparation, receipt, verification, remediation development, release, post release, unless there are justified reasons to deviate. Justifications must be reported to the CB and NCCA.

- **Application rules for the EUCC scheme**

  Follow specific application rules for the EUCC scheme for vulnerability management, unless there are justified reasons to deviate.

RED ALERT LABS
IoT Security

1- Preparation

- **Develop and maintain methods for receiving vulnerability information (article 33)**
  These methods shall be made public for holders of EUCC certificates as per Article 55.1.c of the CSA.
- **Contact information**
  Include electronic contact information for receiving vulnerability information.
- **Encryption method**
  Specify the encryption method to be used by external parties, such as PGP with a minimum 3072 bit RSA or Diffie-Hellman key.
- **Communication channel**
  Provide information on how to send the encrypted vulnerability information, such as an email address.

RED ALERT LABS
IoT Security

2- Receipt

Certificate holders must notify CB of vulnerabilities

Holders must notify the issuing CB within **3 days** of discovering any vulnerabilities or irregularities in a certified ICT product.

CB must notify certificate holders

If a CB becomes aware of a vulnerability in an ICT product it certified, it must inform the certificate holder within **3 days.**

Assess and report vulnerabilities

Holders must assess if a potential vulnerability affects security and compliance of the ICT product. They must report such vulnerabilities to the CB in a timely manner.

Certificate holders and CBs have notification requirements for vulnerabilities under the CSA regulation.

3- Verification

Certificate suspension (article 28)

Certificates can be suspended for up to **42 days** by the certification body, who must notify the holder and national authority.

Vulnerability analysis (article 33 / 34)

Certificate holders must conduct a vulnerability analysis within **90 days** of identifying a potential vulnerability.

Attack potential calculation (article 34)

In cases of exploitable vulnerabilities, an attack potential calculation is performed to determine exploitability.

Certificate suspension, vulnerability analysis, and attack potential calculation help ensure security standards are upheld.

Article 35: Impact Analysis Report

1 | Vulnerability Analysis Report Contents

The report must assess the impact of vulnerabilities on the certified ICT product, potential attack risks, and remediation possibilities, including details on exploit methods while maintaining confidentiality.

2 | Certification Body Review

The certification body reviews the vulnerability analysis report, seeking ITSEF input if necessary, and can approve, disapprove, or request clarifications. Non-compliance may lead to suspension or withdrawal of the certificate.

3 | Reporting and Documentation

The report must be sent to the certification body, and if it indicates an unremediable vulnerability, the certificate will be withdrawn. All analysis documentation should be retained for five years.

RED ALERT LABS
IoT Security

Article 36: Remediation Development

1 | ## Proposal Submission

Certificate holders must submit a remedial action proposal to the certification body for any vulnerabilities identified in their ICT product.

2 | ## Assessment and Suspension

The certification body assesses the proposed remedial action, suspending the EUCC certificate during this period, and may involve ITSEF for product review.

3 | ## Outcome and Certification

Following the assessment, if the remedial action is approved and implemented, a new EUCC certificate is issued. If disapproved, the existing certificate may be withdrawn.

RED ALERT LABS
IoT Security

Vulnerability Disclosure

30-day embargo on vulnerability disclosure

Certificate holders can impose a 30-day embargo on vulnerability disclosure, extendable with NCCA approval, to limit disclosure to certain parties.

Notify and share vulnerability details (article 38)

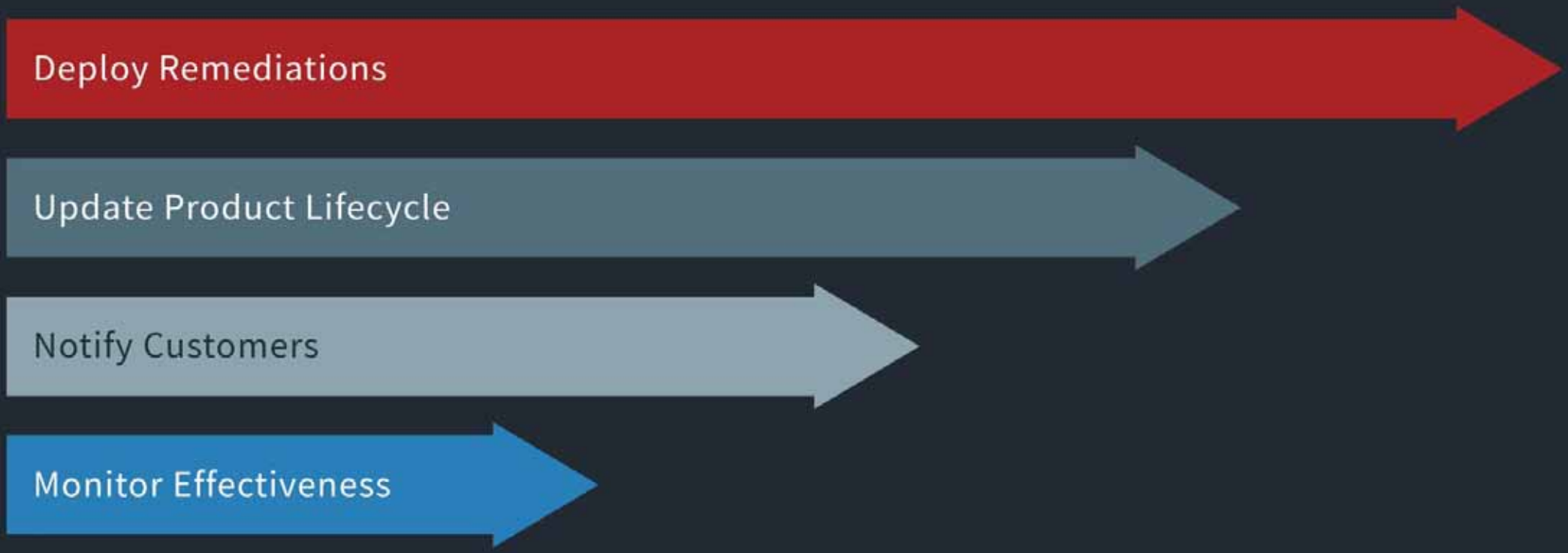
Certification bodies must notify NCCAs of confirmed vulnerabilities, which are then shared with other NCCAs and ENISA, maintaining confidentiality of exploitation details.

Public disclosure guidelines (article 39)

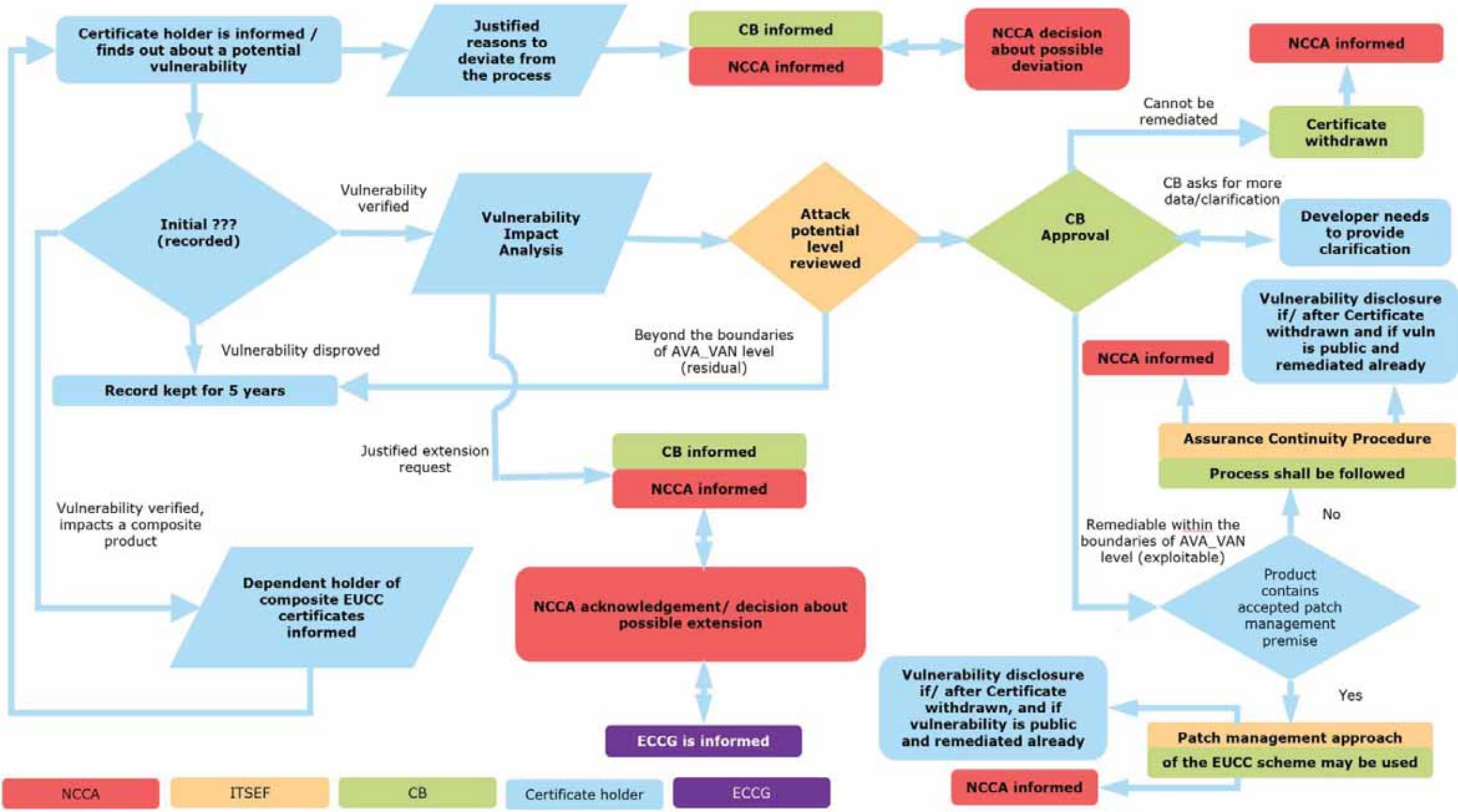
Once a vulnerability is confirmed and the certificate withdrawn, holders must publicly disclose it per ISO/IEC 29147, with NCCA support.

Embargo, notification, and public disclosure guidelines for vulnerabilities found in certified products.

5- Release and Post Release



RED ALERT LABS
IoT Security


Certificate holder is informed / finds out about a potential vulnerability
Justified reasons to deviate from the process
CB informed
NCCA informed
NCCA decision about possible deviation
NCCA informed
Cannot be remediated
Certificate withdrawn
Initial ??? (recorded)
Vulnerability verified
Vulnerability Impact Analysis
Attack potential level reviewed
CB Approval
CB asks for more data/clarification
Developer needs to provide clarification
Vulnerability disproved
Record kept for 5 years
Beyond the boundaries of AVA_VAN level (residual)
Vulnerability disclosure if/ after Certificate withdrawn and if vuln is public and remediated already
NCCA informed
Assurance Continuity Procedure
Process shall be followed
Justified extension request
CB informed
NCCA informed
No
Vulnerability verified, impacts a composite product
Remediable within the boundaries of AVA_VAN level (exploitable)
Product contains accepted patch management premise
Dependent holder of composite EUCC certificates informed
NCCA acknowledgement/ decision about possible extension
Yes
Vulnerability disclosure if/ after Certificate withdrawn, and if vulnerability is public and remediated already
Patch management approach
of the EUCC scheme may be used
ECCG is informed
NCCA informed
NCCA
ITSEF
CB
Certificate holder
ECCG

Key points, Clarifications, Recommendations

Some Additional Questions

RED ALERT LABS
IoT Security

ECCG Role - article 48

ECCG's role in scheme maintenance ?

ECCG maintains and provides guidance on cybersecurity certification schemes

Public-private cooperation ?

How would ECCG enables cooperation between public authorities and private sector through technical working groups

Will there be specialized subgroups ?

ECCG can create specialized subgroups focused on specific cybersecurity topics or sectors

ECCG plays a crucial role in cybersecurity certification by bridging public and private sectors and providing specialized guidance.

Evaluation Criteria & Methods - Article 5 / 7

Limitations on using Protection Profiles

Relying on EUCC certified protection profiles limits flexibility; Only in exceptional justified cases, a CAB may not use them subject to specific conditions, in particular the approval by the NCCA.

Substantial & AVA_VAN.3

How about Substantial level ? and AVA_VAN.3 (non-technical domain)

A balanced approach is used to ensures solid ICT security evaluation while providing flexibility in criteria.

Handling New Technical Domains

Uncertainty about new domains

Lack of knowledge about managing products in unfamiliar technical areas

Establish domain process

Create a standardized process for evaluating new technical domains and categorizing products

Decide categorizations

Make informed decisions on product categories based on the domain process

By establishing a formal process for new domains, we can reduce uncertainty and consistently categorize products.

Various issues raised...

Monitoring of Protection Profiles (article 26)

CBs' responsibilities in monitoring is unclear.

Impact of New Vulnerabilities

Lack of clarity on how new vulnerabilities affect existing certificates after certification.

Recommend harmonizing responsibilities, clarifying impact of vulnerabilities, and standardizing archival periods across articles.

Scope & Vulnerability Management

Scope of EUCC vs national schemes

Discuss how the scope of the EUCC compares to national certification schemes.

Vulnerability management and disclosure

Discuss lessons learned from the AHWG pilots on vulnerability disclosure and how they can inform the EUCC process.

key points for discussion include the scope of the EUCC and applying lessons learned from vulnerability pilots.

Potential Next Steps ?

Maintenance

Creation of the EUCC Maintenance Group under the ECCG

Reuse of national supporting docs

Leverage existing national supporting documents to include these to the SOTA rather than recreate from scratch

Cryptography

Creation of CM certification criteria to complement the EUCC and other schemes.

Interplay with other regulations

Consider how various regulations interact with EUCC (e.g. CRA, NIS2, ...)

RED ALERT LABS
IoT Security

QUIZ

- **Who maintains and provides guidance on EUCC certification scheme ?**
- **Does the ENISA get notified in case of a confirmed vulnerabilities?**
- **what are the POST-ACQUISITION obligation of EUCC certificate holders?**

PRESUMPTION OF CONFORMITY

EUCC & CRA

EUCC and CRA Notification

EUCC can be used for presumption of conformity with CRA

EUCC provides a route to demonstrate presumption of conformity with CRA requirements for clinical investigations

EUCC alone does not meet CRA notification requirements

EUCC does not involve CRA notification so additional steps are needed to meet CRA notified body requirements

EUCC provides presumption of CRA conformity but does not meet CRA notification requirements on its own

How to Achieve EUCC Certification Presumption of Conformity

CRA Risk Analysis

Reflect required CRA risk analysis for selected ESRs in EUCC certification process.

Technical Elements for Certification

Identify technical elements to certify for full CRA presumption of conformity.

CAB Requirements

Ensure CABs meet Notified Body requirements under CRA Article 29.

RED ALERT LABS
IoT Security

All the product boundary must be included (TOE+)

All digital elements

This includes any software, apps, or digital components that are part of the product.

Remote data processing

Any data processing done on remote servers or in the cloud that is part of the product's functionality.

Full product scope

The conformance evaluation must cover the complete product, including all digital elements and remote processing.

To fully conform with CRA, the scope must be comprehensive and evaluate all aspects of the product that include digital elements or remote data processing.

Technical Assessment of ESRs

Technical assessment of ESRs

All ESRs in CRA Annex I.1 can be technically assessed through SFRs and SARs existing in CC2022 or by defining extended ones

Extended SFRs/SARs needed

Some ESRs listed in CRA Annex I.1 required the definition of extended SFRs or SARs

The technical assessment of ESRs in CRA Annex I.1 relies on existing and extended SFRs/SARs in CC2022

Vulnerability Handling

The ESRs in Annex I.2 of CRA related to vulnerability handling can largely be assessed against technical elements in the EUCC Components in the ALC_FLR family.

The technical patch management requirements in EUCC also address many of the CRA Annex I.2 requirements for security patch distribution.

RED ALERT LABS
IoT Security

Technical Documentation

- **CRA Annex V**
  Describes technical documentation for processes
- **EUCC CABs**
  Could cover assessment through SARs in EUCC evaluation
- **CRA Annex II**
  Describes information for users of product with digital elements
- **EUCC evaluations**
  Can address through AGD_OPE and AGD_PRE assessment
- **EUCC Patch Management**
  Guidance for patch installation
- **ALC_DEC**
  Instructions for secure decommissioning of the TOE

RED ALERT LABS
IoT Security

SFRs & SARs can cover CRA ESRs

EUCC presumption of conformity

EUCC SFRs can cover CRA Annex I requirements on security functionality and manufacturer processes.

EUCC SARs cover CRA Annex I.1

EUCC SARs can assess vulnerability handling processes equivalent to CRA Annex I.1.

EUCC SARs cover CRA Annex I.2

EUCC SARs can assess product design, development and delivery processes like CRA Annex I.2.

EUCC SARs cover Annex V

EUCC SARs assess product design, VA handling, risk assessment like CRA Annex V.

EUCC SFRs and SARs can cover CRA requirements for security functionality, processes and documentation.

Potential solutions

- **standalone security targets**
  create new STs for CRA presumption of conformity. Flexible but high effort for manufacturers
- **create protection profile**
  generic PP for any product. Supports harmonization but challenging to make generic
- **base PP with configurations**
  base PP with modular options. Balance of harmonization and flexibility
- **security packages without PP**
  SFR and SAR packages without PP for flexibility and harmonization
- **security packages with PP**
  use packages in PP context for flexibility and harmonization

RED ALERT LABS
IoT Security

Multiple Scenarios are possible

Full product certification

Vendor accepts to certify the full product including remote data processing using a multilevel security target based on CC2022

Partial product certification

Vendor certifies parts of the product and complements CRA compliance with other NLF activities

Certified component

Vendor uses a certified component like a secure element and shows partial compliance, complementing with other NLF activities

Multiple scenarios for complying with CRA using EUCC certification

Conclusions

- **CRA Annex I ESRs can be achieved with EUCC**
  Existing and extended SFRs/SARs in EUCC can help achieve compliance
- **Manufacturer obligations supported**
  Technical documentation and user instructions requirements can be handled via EUCC SARs
- **EUCC supports CRA risk assessment**
  For selection of applicable ESRs
- **EUCC supports full CRA presumption**
  By including full product with digital elements in scope
- **CRA conformity assessment defined**
  Requirements for bodies seeking notification are in CSA Annex
- **Some challenges remain**
  Full conformance hard with smaller EUCC scope, CRA SFRs/SARs not easy to integrate

RED ALERT LABS
IoT Security

THANK YOU