THE EU CYBERSECURITY AGENCY

The candidate EUCC certification scheme

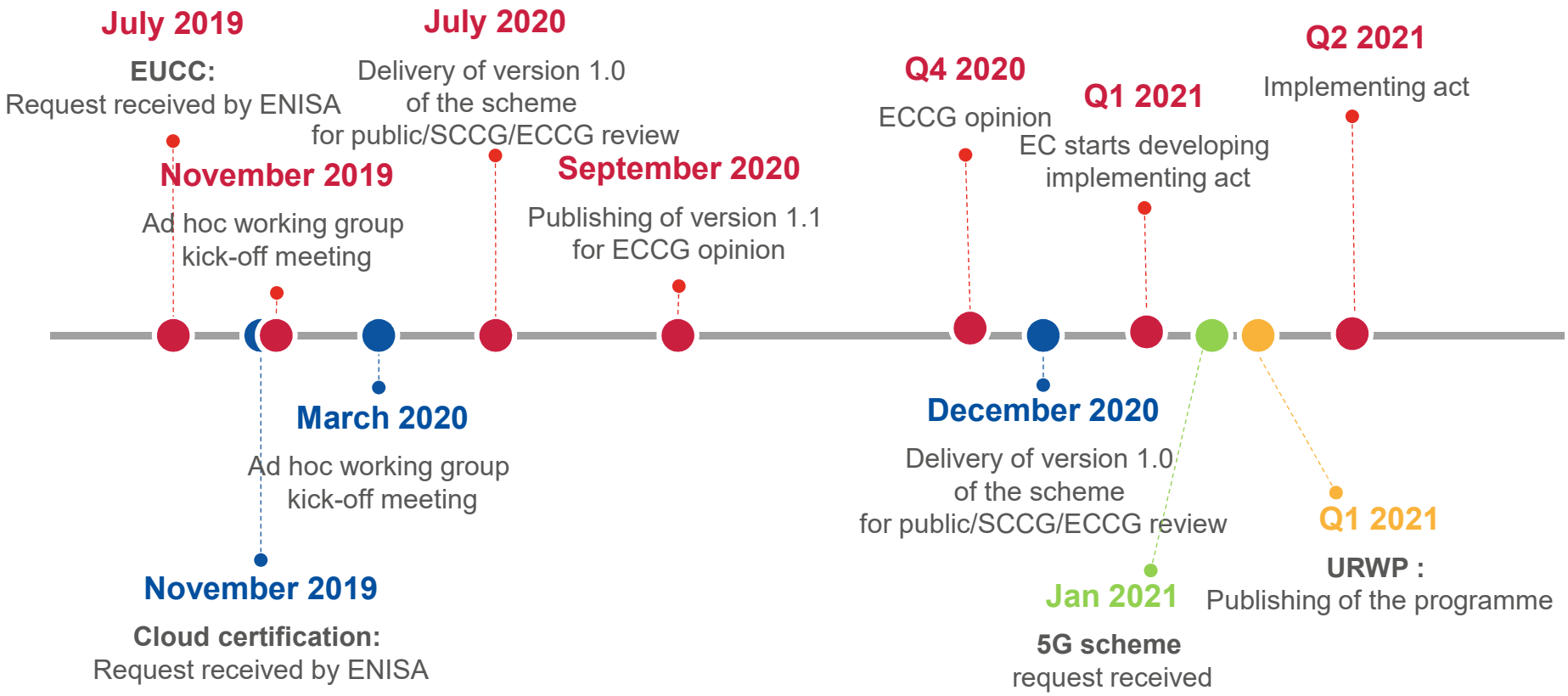
Philippe Blot
Market, Certification & Standardisation Unit

08 | 04 | 2021

Content of the presentation

1. **Overview of current activities on cybersecurity certification according to the CSA**
2. **Where we stand with the candidate EUCC scheme on ICT products**
3. **The candidate EUCC scheme: overview**
4. **The candidate EUCC scheme: some highlights**
5. **Ongoing activities**

Current activities on cybersecurity certification according to the CSA



EUCC: ICT product Cybersecurity Certification scheme based on SOG-IS and CC

URWP: Union Rolling Work Programme

Progress of the candidate EUCC scheme

Upon request of the European Commission (Article 48 (2) of the Cybersecurity Act* (CSA)), ENISA set up an Ad Hoc Working Group to support the preparation of a candidate cybersecurity certification scheme to serve as a successor to the SOG-IS Mutual Recognition Agreement.

The EUCC AHWG chaired by ENISA is composed of 20 appointed members representing industry** (developers, evaluators)**, as well as around 12 participants from accreditation bodies and Members States.**

* https://eur-lex.europa.eu/eli/reg/2019/881/oj
** https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ahWG01/ahwg01_members

Progress of the candidate EUCC scheme

ENISA with the very efficient support of the AHWG developed v1.0* of the candidate EUCC scheme.

Based upon article 49 (3)** CSA, ENISA offered the SCCG and any other stakeholders the possibility to express their opinion on v1.0 through a **public consultation** which took place **in July**. In parallel, **ENISA consulted the ECCG** (see next slide for some results).

Based on these consultations, ENISA with the support of the AHWG developed **v1.1 of the candidate EUCC scheme**, **submitted to the ECCG for its opinion** according to article 49 (6)*** CSA.

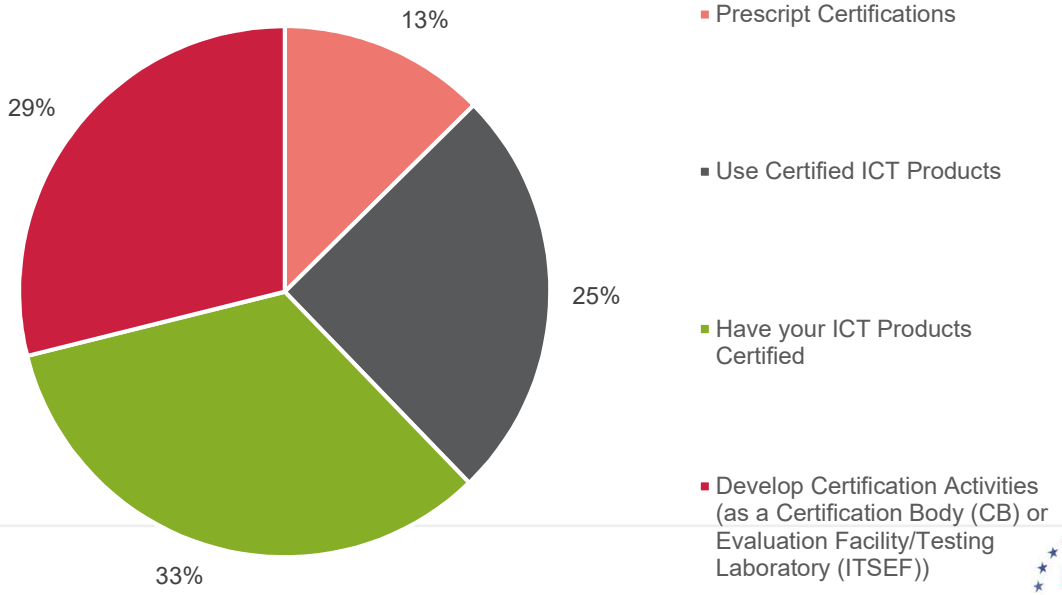
* https://www.enisa.europa.eu/topics/standards/Public-Consultations
** When preparing a candidate scheme, ENISA shall consult all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process
*** ENISA shall take utmost account of the opinion of the ECCG before transmitting the candidate scheme… to the Commission.

Progress of the candidate EUCC scheme

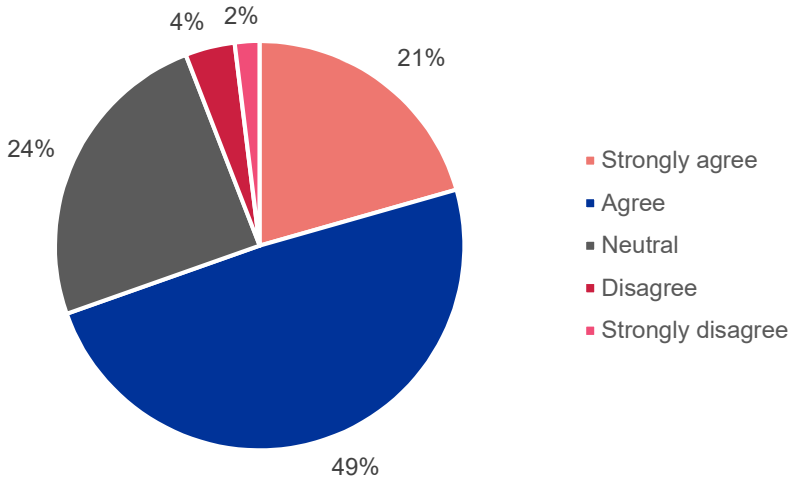
The candidate EUCC scheme version 1.0 published in July received in majority **a positive feedback** from the SCCG, public and ECCG consultations, e.g.:

82% of the participants to the Public/SCCG consultation (61% outside EU/EEA) intend to use it, for the following usages:

All ECCG participants indicated they intend to use the EUCC scheme



Positive impact of improvements brought by the scheme*



The important neutral percentage can well be associated with the ambitious expectation level associated with the improvements, all not developed/experimented yet, and their potential impacts (delays and technical requirements) on the existing certification practices.

*maintenance of the certificates, monitoring and handling of non-compliances, non-conformities and vulnerabilities, patch management),

The candidate EUCC scheme: overview

The **candidate EUCC scheme is a scheme for ICT products, based on the Common Criteria** (ISO/IEC 15408 and 18045). Common examples of certified products according to the CC are integrated circuits and smartcards for electronic signature, identification (passports), banking, tachographs for lorries, and software products (e.g. disk encryption, VPN clients…). **It is more of a horizontal scheme**, reusable by sectorial domains.

It aims to serve as a successor to the existing schemes operating under the SOG-IS MRA*, and therefore **takes advantage of the existing practices of this MRA**, e.g.:

- it addresses **all Common Criteria levels** (and relies therefore on existing material such as Technical Domains for higher levels)
- it is a third party scheme and has **strong requirements for CABs acting at higher levels**, including their peer assessment

* https://www.sogis.eu/

The candidate EUCC scheme: overview

In addition, it provides a number of **improvements associated with the CSA to ensure assurance continuity of the certificates**, covering for example harmonized activities related to:

- the monitoring and handling of non-compliances and non-conformities;
- vulnerability handling and disclosure;

and **introduces a patch management mechanism** that can be part of the certification and will ease maintaining the products and certificates up-to-date.

It includes the possibility to certify Protections Profiles, that allow harmonized definition of the security requirements associated with a category of products.

The candidate EUCC scheme: some highlights

The candidate EUCC scheme is designed to address the requirements of the CSA, in particular:

- Article 51, Security objectives of European cybersecurity certification schemes
- Article 52, Assurance levels of European cybersecurity certification schemes
- Article 54, Elements of European cybersecurity certification schemes

It includes a **core part** addressing all elements requested by Article 54, a section on **additional elements** to the scheme (e.g.: the possibility to certify PPs), plus **recommendations** from the AHWG (both on transition from the SOG-IS and on the future maintenance of the scheme) and a series of **annexes for mandatory application**.

Guidance will be provided in addition, through the ENISA website dedicated to certification.

The candidate EUCC scheme: some highlights

The candidate EUCC scheme covers assurance levels “substantial” and “high” of the CSA, with a mapping associated with AVA_VAN levels*:

- AVA_VAN.1 and AVA_VAN.2 map to the assurance level ‘substantial’ of the CSA;
- AVA_VAN.3 to AVA_VAN.5 map to the assurance level ‘high’ of the CSA.

According to the CSA, **commercial CABs will be in charge of certifying for the substantial level**.

* 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.

The candidate EUCC scheme: some highlights

CABs shall be accredited to perform activities:
- CB shall be accredited according to ISO/IEC 17065;
- ITSEFs shall be accredited according to ISO/IEC 17025.

At the “substantial” level, accreditation will be the main element for their notification.
Specific requirements will apply in addition for their authorization to operate at level “high”.

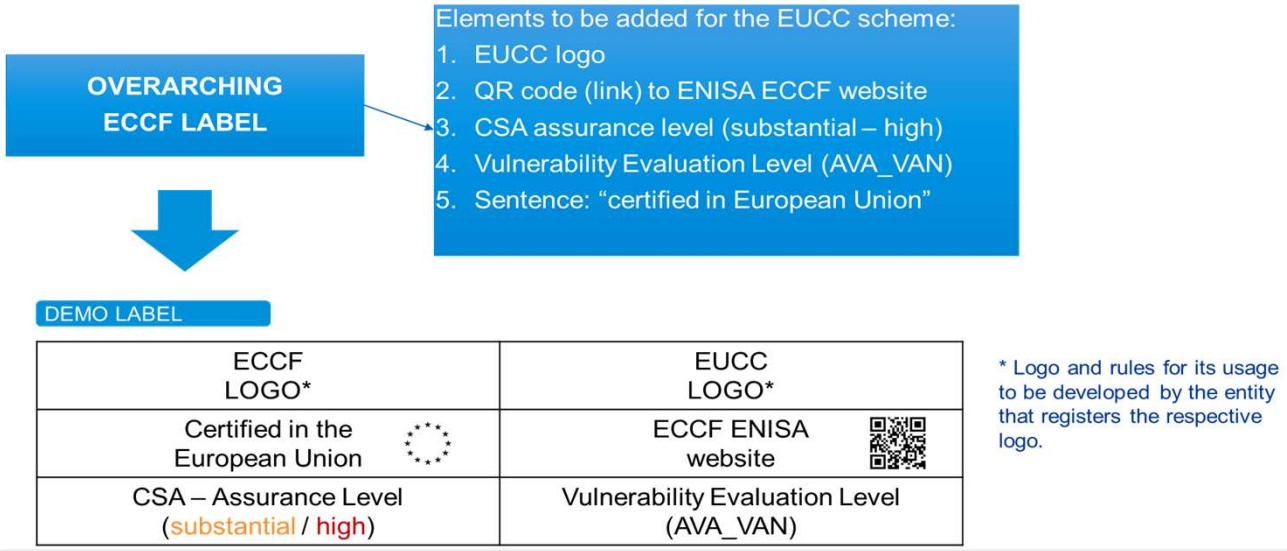
ENISA has engaged with its AHWG and with EA on the development of **harmonized interpretations** of above listed standards for the EUCC scheme.

The candidate EUCC scheme: some highlights

ENISA is developing a **website dedicated to cybersecurity certification** that will disclose:

- The scheme and associated documentation (guidance)
- The certificates and related information on the status of these certificates

The candidate EUCC scheme provisions the establishment of a **label**, which could present the following information:



The candidate EUCC scheme: some highlights

The candidate EUCC scheme introduces **rules for monitoring compliance**, with the goal the detect :

- non-compliance in the application by a manufacturer or provider of the rules and obligations related to a certificate issued on their ICT product;
- non-compliance in the conditions under which the certification takes place and that are not related to the individual ICT product;
- non-conformity of a certified ICT product with its security requirements, which includes and is not limited to a:
  - change in the threat environment after the issuance of the certificate, which has an adverse impact on the security of the certified ICT product;
  - vulnerability identified and related to the certified ICT product, that has an adverse impact on the security of the certified ICT product.

Monitoring consists in **preventive measures** (e.g.: commitments from the developer), **detection activities** (e.g.: market surveillance), and **defined consequences** with associated timelines on CABs and/or certificates.

The candidate EUCC scheme: some highlights

The candidate EUCC scheme introduces **a general process on vulnerability handling and disclosure** based on ISO/IEC 30111and ISO/IEC 29147. It defines timelines, and adds requirements as to assess assurance on whether the developed and deployed remediation does not introduce new vulnerabilities and related tasks and methodology for a third-party assessment body.

A **non-mandatory patch management mechanism is introduced** with a trial use status for 2 years, it may either use Patch management ISO SC27 WG3 Technical Report “Extension for Patch Management for 15408 and 18045* or the ISCI WG1 Proposal for new SAR components and Packages in CC for Patch Management**.
The possible use of the patch management as a fast track approach to handle functional changes to a certified product is also introduced.

*as defined by https://www.jtsec.es/papers/Technical/Report_Patch_Management.pdf
**as defined by https://cclab.com/isci-workgroup .

The candidate EUCC scheme: some highlights

The candidate EUCC scheme defines **conditions for mutual recognition** with 3rd countries, that can serve as a basis for future MRAs.

The responsibility however for establishing a new MRA or to define conditions under which the current MRA can continue is not on ENISA.

Ongoing activities

The candidate EUCC scheme proposes the establishment of the **supporting guidance**, covering for example:

- Harmonized interpretation of ISO/IEC 17025 for the accreditation of ITSEFs
- Guidance on the manufacturer/provider commitments that may be part of an application request, with an indication of the associated gravity
- How to reuse of existing SOG-IS certificates in order to establish EUCC certificates
- Taxonomy of ICT products
- Guidance for the delivery and for the publication in due time of certificates and their updates
- How to ensure the security of information based on the workflows associated with the activities described in the EUCC scheme
- Checklists to support peer assessments

ENISA has engaged with the AHWG and the support of additional external experts into the development of some of these elements.

Additional activities will also be launched soon on specifying an **EU label**, and on **potential pilots** to experiment the new features of the candidate EUCC scheme.

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu