The European Cybersecurity Certification Framework

Enhancing cybersecurity in the internal market

Ingrid Lauringson, Legal Officer, DG CONNECT,
Unit H2 Cybersecurity & Digital Privacy Policy,
European Commission

EU Cybersecurity Act

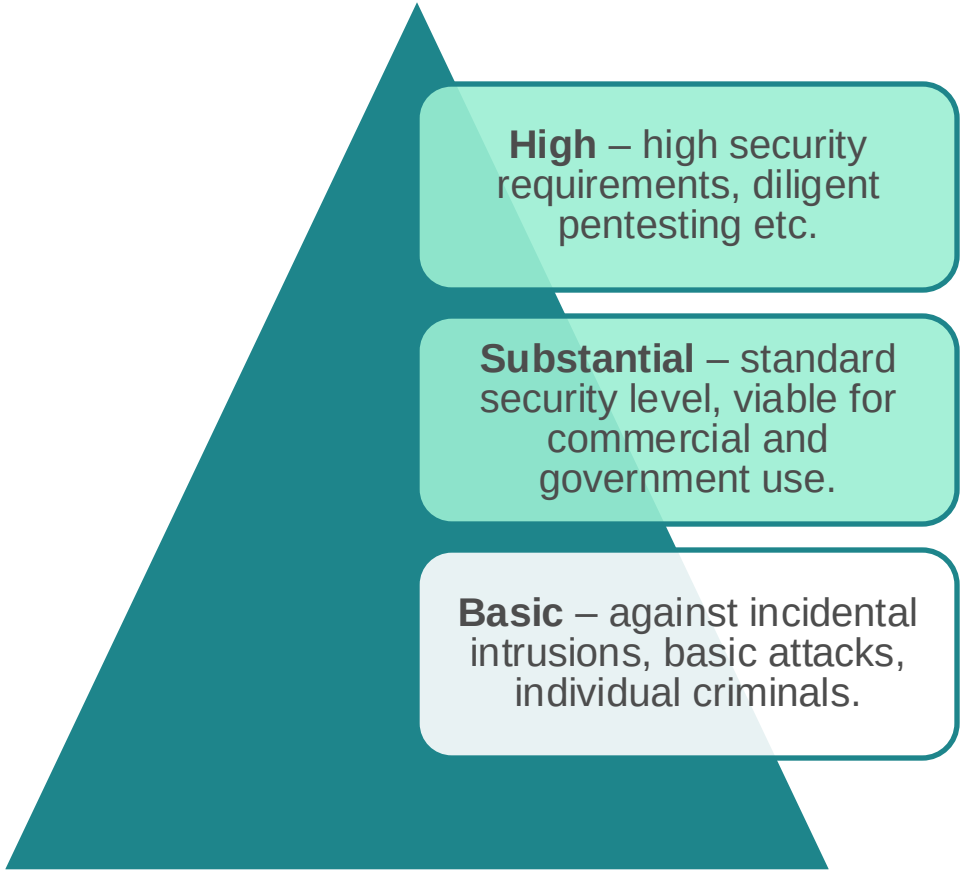
- ✓ Regulation (EU) 2019/881 (**Cybersecurity Act**):
  - ✓ Entered into force in 2019
  - ✓ Reviewed ENISA's mandate
  - ✓ Established a European cybersecurity certification framework (ECCF)
  - ✓ Provided a mechanism to establish European cybersecurity certification schemes

EU Cybersecurity Certification

- ✓ **Certify once**, access the whole EU market (and beyond)
- ✓ Create **trust** by providing clarity and visibility to users
- ✓ Make cybersecurity a competitive advantage and **market opportunity**
- ✓ Boost European technological **leadership**

Tailored, risk-based schemes

- ✓ One cybersecurity certification framework, many schemes
- ✓ Schemes **tailored** to specific ICT products, services or processes
- ✓ A **risk-based approach** with three different levels of assurance



European Commission

Elements of a certification scheme

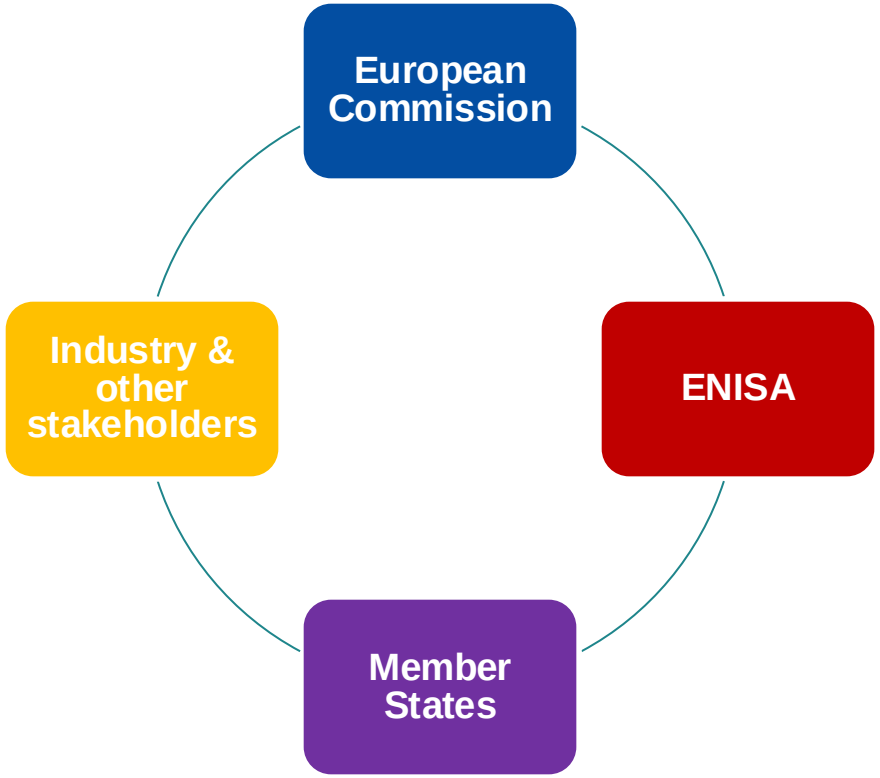
Essential elements (exhaustive list in **Article 54 of the CSA**):

- ✓ A clear description of the subject matter, scope and purpose of the scheme
- ✓ Type or categories of ICT products, ICT services and ICT processes
- ✓ One or more assurance levels
- ✓ References to international, European, or national standards
- ✓ The aspect of conformity self-assessment
- ✓ Specific evaluation criteria and methods to be used

A voluntary tool based on a collective effort

Lifecycle of a scheme:

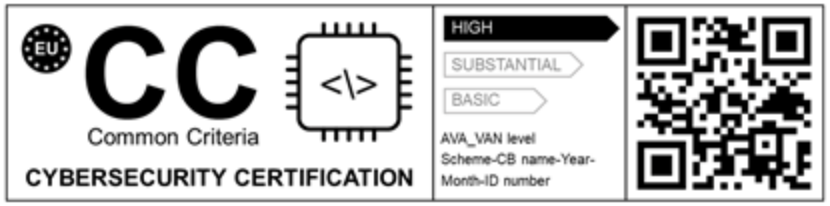
- ✓Planning
- ✓Request
- ✓Preparation
- ✓Implementation
- ✓Review



European Commission

The European Common Criteria-based cybersecurity certification scheme (EUCC)

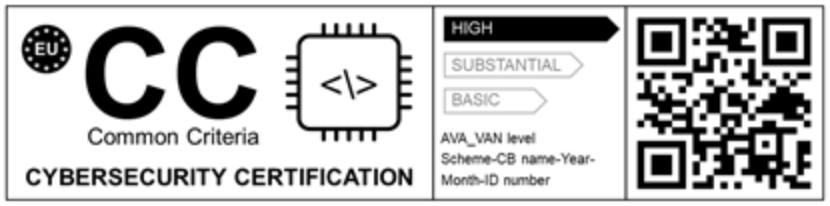
- ✓ **One scheme for the whole Union** – Commission Implementing Regulation (EU) 2024/482 (EUCC)
- ✓ Legal basis **Article 49(7) of the CSA**
- ✓ The EUCC targets **ICT products, including components** that have critical cybersecurity functions (assurance levels substantial and high)



European Commission

The European Common Criteria-based cybersecurity certification scheme (EUCC)

- ✓ Builds on **SOG-IS** and Common Criteria Recognition Arrangement (**CCRA**)
- ✓ Implements a **life-cycle approach** (in line with the CSA)
- ✓ **Private Certification Bodies** can issue certificates at level 'substantial'
- ✓ **Accreditation** of the whole ecosystem (ITSEFs and CBs)



European Commission

Impact of the Cyber Resilience Act

- To enter into force in 2024; full applicability in 2027
- Cybersecurity rules for the placing on the market of **hardware** and **software products**
- Set obligations on **manufacturers**, **distributors** and **importers** (based on New Legislative Framework)
- **Risk-based approach** to conformity assessment (critical and important products)
- European cybersecurity certification schemes as one **way to demonstrate conformity** with the CRA where presumption of conformity exists
- Specific relevance of EUCC for «**critical products**» listed in Annex IV

Some resources

- **All information on EU certification on ENISA's dedicated website** : https://certification.enisa.europa.eu/
- **Union Rolling Work Programme for European cybersecurity certification:** https://digital-strategy.ec.europa.eu/en/library/union-rolling-work-programme-european-cybersecurity-certification
- **Cybersecurity Act**: https://eur-lex.europa.eu/eli/reg/2019/881/oj
- **Implementing Regulation on the European Common criteria-based cybersecurity certification scheme (EUCC):** https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R0482&qid=1707312751025

Thank you!

European Commission