EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EU CYBERSECURITY CERTIFICATION

OUTCOMES AND OPPORTUNITIES

Philippe Blot
Head of Cybersecurity Certification sector
Market, Certification & Standardisation Unit
ENISA, The European Agency for Cybersecurity

25 | 10 | 2022

EU CERTIFICATION: ALL YOU NEED TO KNOW

EU
CYBERSECURITY CERTIFICATION
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
0:04 / 2:11

EU Certification: All you need to know
https://www.youtube.com/watch?v=03zxrb2Fc0A

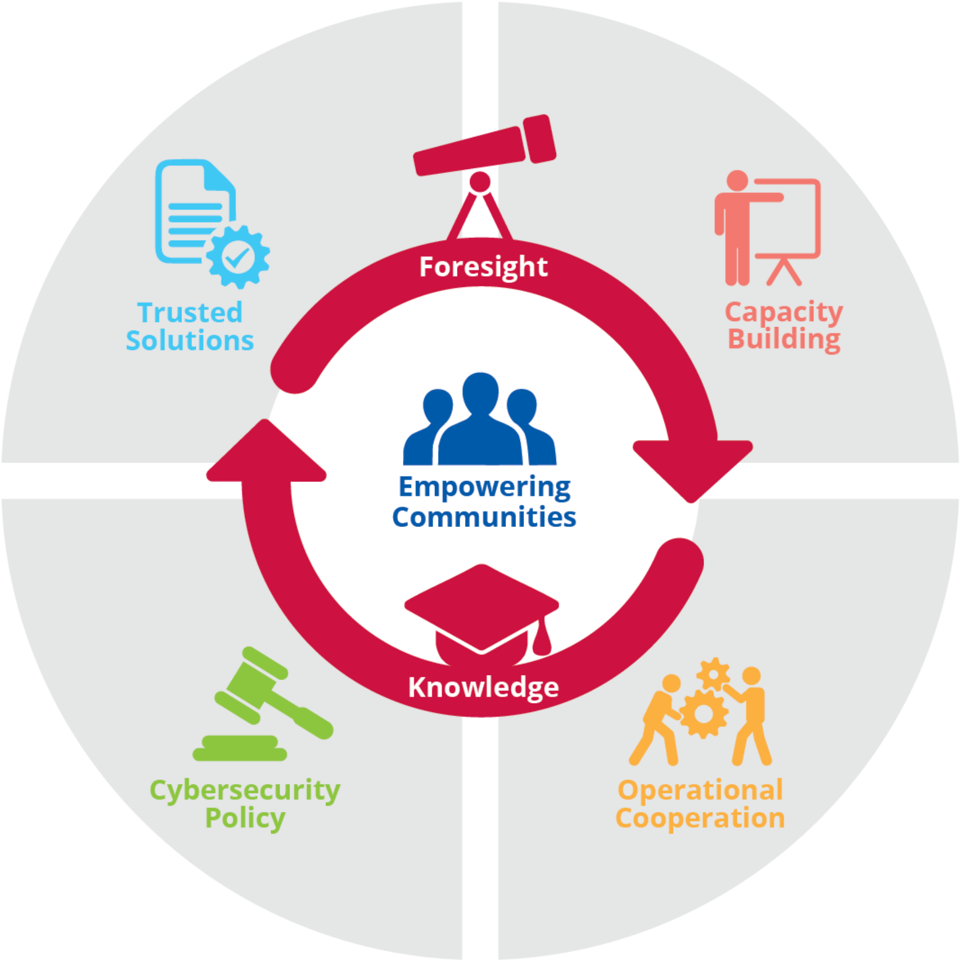
You missed the first episode?
What's in for Conformity Assessment Bodies (CABs)**?**
https://www.youtube.com/watch?v=vabWKHGrjGM

WHO WE ARE

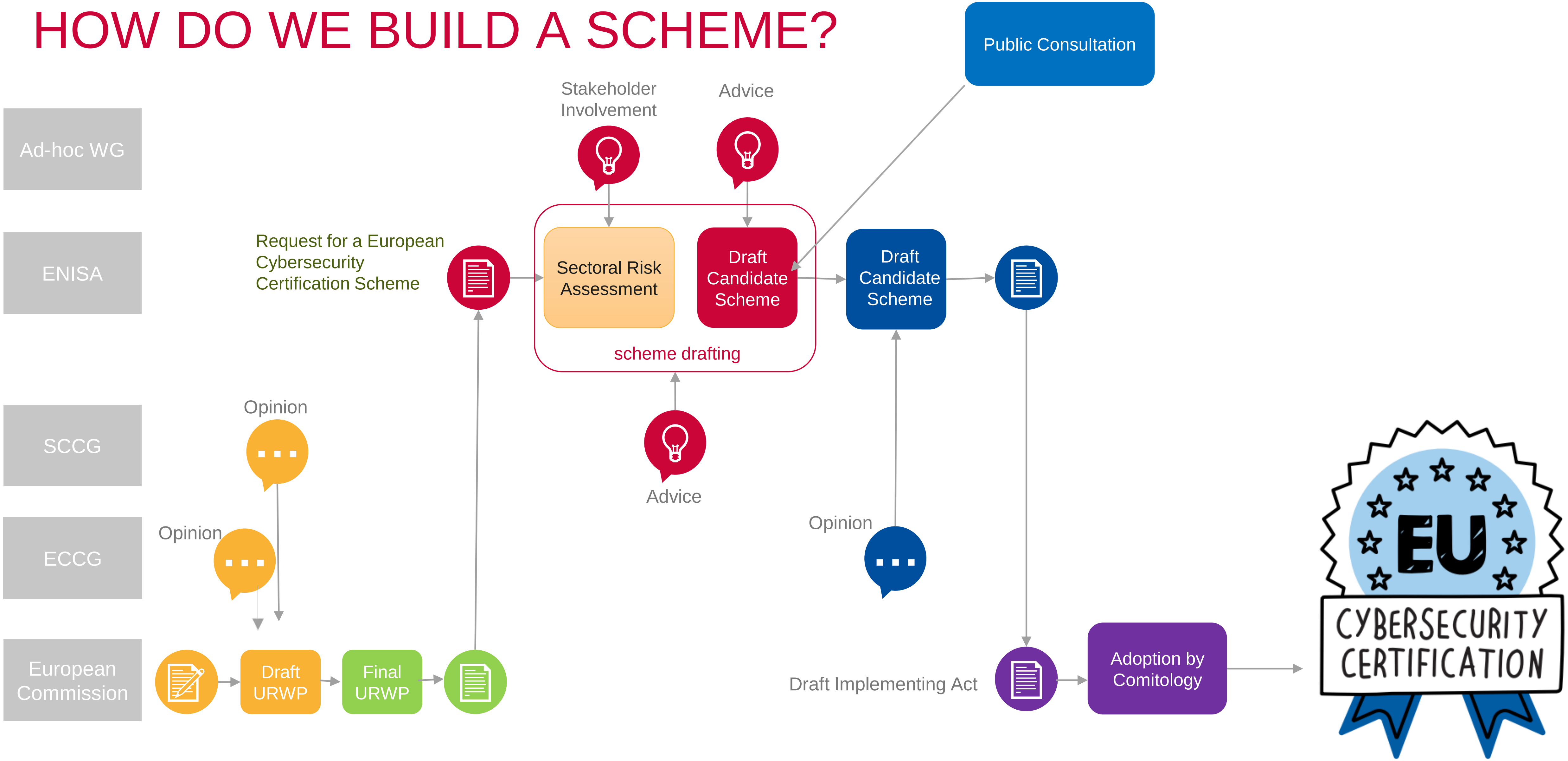
The European Union Agency For Cybersecurity is dedicated to achieving a high common level of cybersecurity across Europe.

- ENISA plays a key role in enabling the Union’s ambition to **reinforce digital trust and security across Europe**, **together** with the Member States and EU bodies.

- By bringing communities together, the Agency continues to successfully contribute **to strengthening Europe’s preparedness and response capabilities** to cyber incidents.



HOW DO WE BUILD A SCHEME?



EUCC: AN HORIZONTAL ICT PRODUCTS SCHEME

Based on international standards

Common Criteria & CEM

ISO/IEC 17065 & 17025 for the accreditation

Horizontal

Defines the “how to certify”

The “what to certify” is for risk owners to define through Protections Profiles or individual security targets

2 assurance levels

As defined in the European Cybersecurity Act

‘substantial’ (AVA_VAN.1 & 2)

‘high’ (AVA_VAN.3, 4 & 5)

All levels based on an assessment by an accredited third-party

EUCC : CURRENT WORK IN PROGRESS

- **Implementing Act (ENISA support to the EC**) based on the candidate scheme, including relevant annexes
- **Maintenance strategy**
- **Catalogue of national supporting documents** that may become new mandatory requirements
- **ENISA website dedicated to certification,** promoting schemes and certificates
- **Harmonised cryptographic** evaluation procedures

EUCS SCHEME : GENERIC APPROACH TO THE CLOUD

All capabilities

Based on ISO/IEC 22123-1

All cloud capabilities are supported: Infrastructure, Platform, Application

Preferred for clarity to references to IaaS, PaaS, SaaS, XXaaS

No mention of deployment model

Horizontal

Defines a baseline of requirements that are applicable to all services.

Enables the same methodology for all services

Does not assess the security of product-specific security features (Security as a Service)

3 assurance levels

As defined in the European Cybersecurity Act

'basic' → CS-Basic

'substantial' → CS-Substantial

'high' → CS-High

All levels based on an assessment by an accredited third-party

EU5G SCHEME

Phase 1

Ongoing

Until Q3

- **3 Workstreams**: as-is transposition of GSMA NESAS, SAS-SM, SAS-UP and eUICC, plus risk assessment and gap analysis.
- Then **feedback to the ECCG**

Phase 2

To Follow

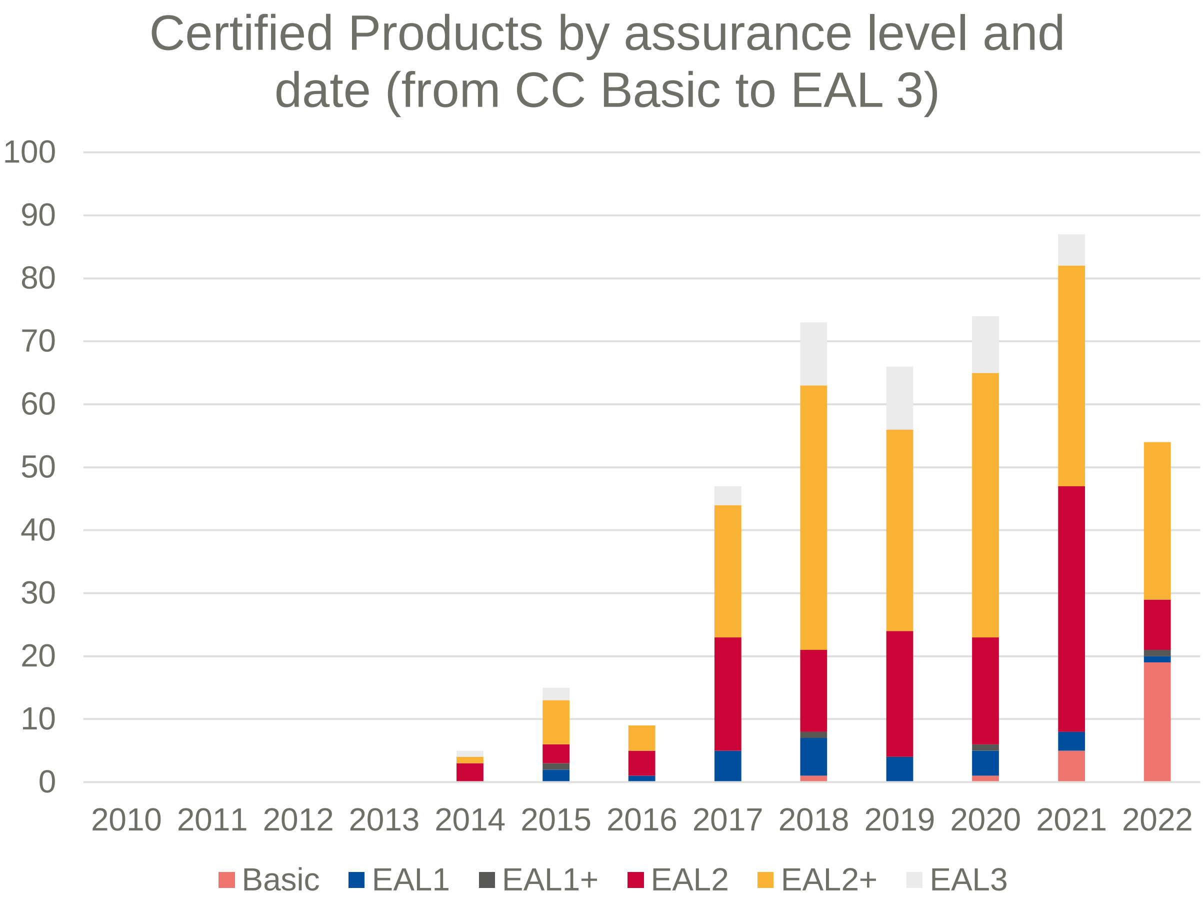
- **Development of the candidate scheme**
- **Permanent coordination with the NIS CG** to reuse their elements for the benefit of the EU5G scheme

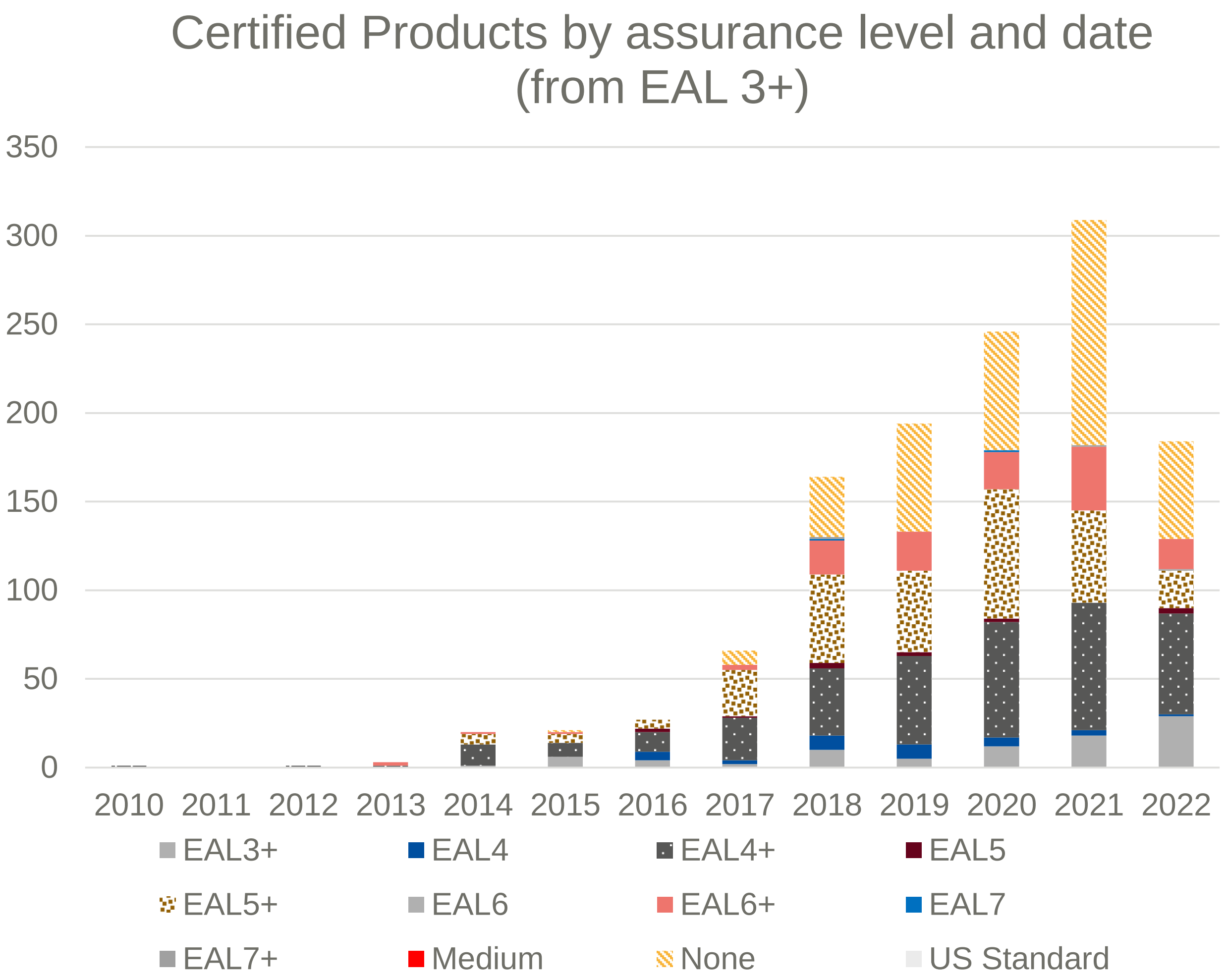
Challenges:

- Estimate the equivalent CSA assurance level of existing GSMA schemes and ensure consistency
- Conduct risk assessments to potentially ensure technical comparability between GSMA/3GPP and EU schemes
- Future maintenance of the scheme

CURRENT CCRA AND SOG-IS MARKETS

Total = 1662

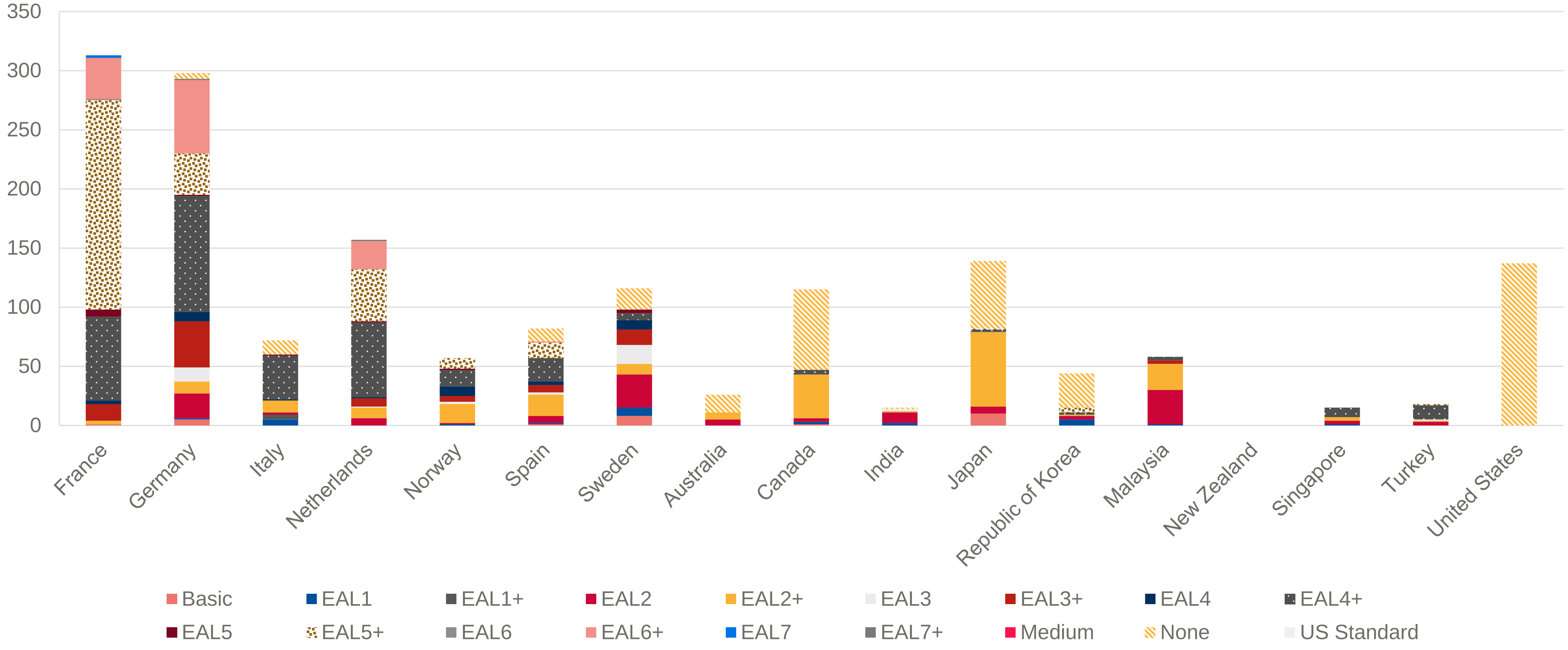




Based on Certified Products List – Statistics : New CC Portal (commoncriteriaportal.org)

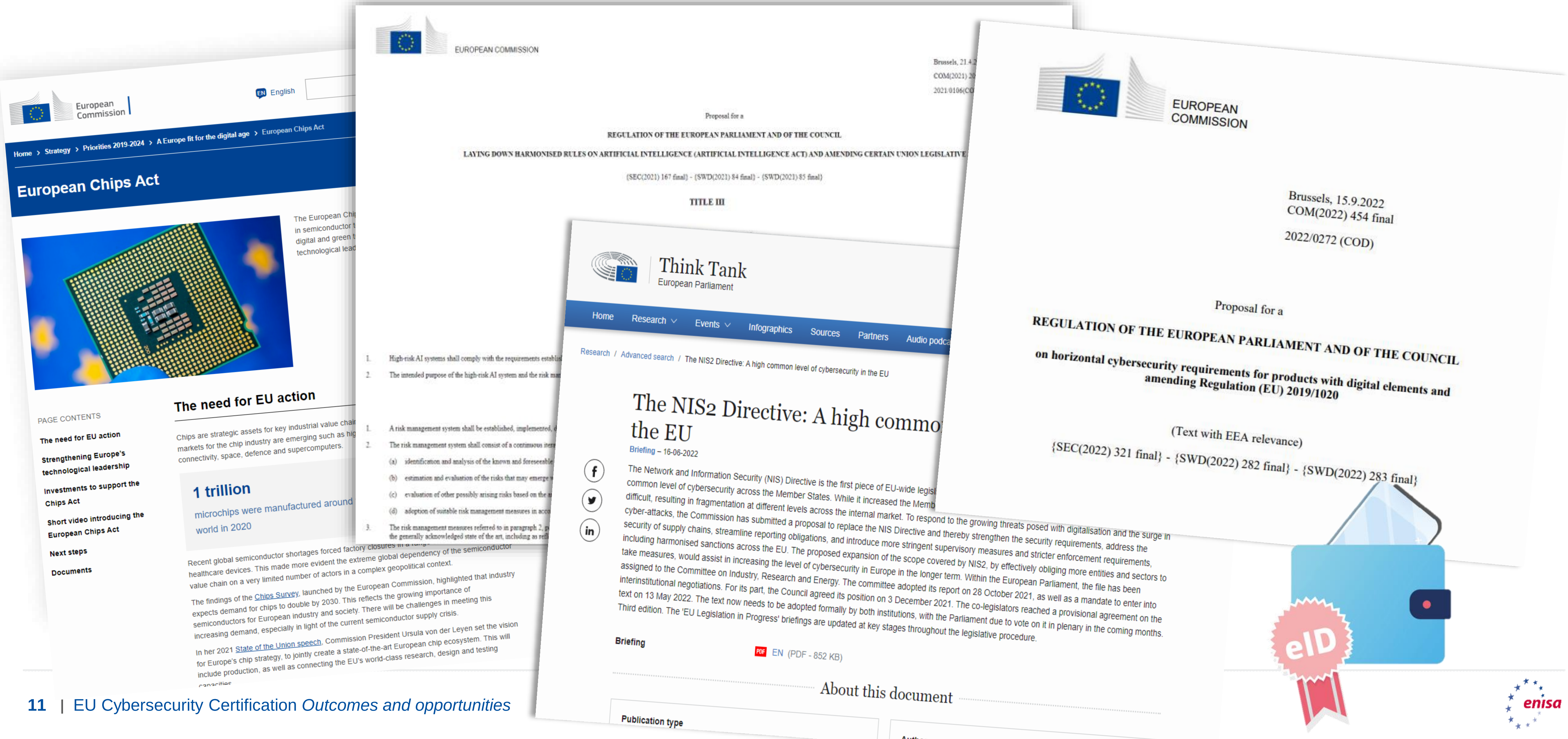
CURRENT CCRA AND SOG-IS MARKETS

Total = 1662



Based on Certified Products List – Statistics : New CC Portal (commoncriteriaportal.org)

REGULATIONS TO COME



European Commission

EN English

Home > Strategy > Priorities 2019-2024 > A Europe fit for the digital age > European Chips Act

European Chips Act

The European Chi
in semiconductor t
digital and green t
technological lead

PAGE CONTENTS

- The need for EU action
- Strengthening Europe's technological leadership
- Investments to support the Chips Act
- Short video introducing the European Chips Act
- Next steps
- Documents

The need for EU action

Chips are strategic assets for key industrial value chai
markets for the chip industry are emerging such as hig
connectivity, space, defence and supercomputers.

1 trillion

microchips were manufactured around
world in 2020

Recent global semiconductor shortages forced factory closures in a range
healthcare devices. This made more evident the extreme global dependency of the semiconductor value chain on a very limited number of actors in a complex geopolitical context.

The findings of the Chips Survey, launched by the European Commission, highlighted that industry expects demand for chips to double by 2030. This reflects the growing importance of semiconductors for European industry and society. There will be challenges in meeting this increasing demand, especially in light of the current semiconductor supply crisis.

In her 2021 State of the Union speech, Commission President Ursula von der Leyen set the vision for Europe's chip strategy, to jointly create a state-of-the-art European chip ecosystem. This will include production, as well as connecting the EU's world-class research, design and testing capacities

EUROPEAN COMMISSION

Brussels, 21.4.2
COM(2021) 20
2021/0106(CO

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

TITLE III

1. High-risk AI systems shall comply with the requirements establis
2. The intended purpose of the high-risk AI system and the risk man

1. A risk management system shall be established, implemented, d
2. The risk management system shall consist of a continuous itera
   (a) identification and analysis of the known and foreseeable
   (b) estimation and evaluation of the risks that may emerge w
   (c) evaluation of other possibly arising risks based on the a
   (d) adoption of suitable risk management measures in acco
3. The risk management measures referred to in paragraph 2, g
the generally acknowledged state of the art, including as refl

Think Tank
European Parliament

Home | Research | Events | Infographics | Sources | Partners | Audio podca

Research / Advanced search / The NIS2 Directive: A high common level of cybersecurity in the EU

The NIS2 Directive: A high commo the EU

Briefing – 16-06-2022

The Network and Information Security (NIS) Directive is the first piece of EU-wide legisl common level of cybersecurity across the Member States. While it increased the Memb difficult, resulting in fragmentation at different levels across the internal market. To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The proposed expansion of the scope covered by NIS2, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term. Within the European Parliament, the file has been assigned to the Committee on Industry, Research and Energy. The committee adopted its report on 28 October 2021, as well as a mandate to enter into interinstitutional negotiations. For its part, the Council agreed its position on 3 December 2021. The co-legislators reached a provisional agreement on the text on 13 May 2022. The text now needs to be adopted formally by both institutions, with the Parliament due to vote on it in plenary in the coming months. Third edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.

Briefing PDF EN (PDF - 852 KB)

About this document

Publication type

EUROPEAN COMMISSION

Brussels, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

(Text with EEA relevance)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

EUCC REQUIREMENTS REGARDING THE VENDORS

Not so many requirements on the what to certify (the scheme is more on the how to certify), still some (1/2):

On the Security Target:

- mandatory inclusion of SARs AVA_VAN (with all related dependencies), ATE_IND & ALC_FLR
- consider the level of risk associated with the intended use of the product and include the security functions contained in the product that support the security objectives defined in Article 51 of the Regulation (EU) No 2019/881 relevant to that ICT product

Existing SOG-IS technical domains and related requirements (MSSR, …) are kept (specific PPs foreseen to address specific cases

Applicants for certification shall provide the CB and ITSEF with:

- the link to their website containing the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) No 2019/881 with a view to having all necessary information included in the EUCC certificate;
- a description of the vulnerability handling and vulnerability disclosure procedures, and
- if within the scope of certification, a description of the patch management mechanism

EUCC REQUIREMENTS REGARDING THE VENDORS

Not so many requirements on the what to certify (the scheme is more on the how to certify), still some (2/2):

The applicant for certification shall undertake commitments:

- to provide the certification body and the ITSEF with reliable information;
- not to promote an ICT product as certified under the EUCC before the EUCC certificate has been issued;
- to promote an ICT product as certified only with respect to the scope set out in the EUCC certificate;
- to cease immediately the advertisement of the certification of the ICT product or Protection Profile in the event of a suspension, withdrawal or expiry of the EUCC certificate;
- to ensure that the ICT products sold in connection with the EUCC certificate are strictly identical to the ICT product subject to the certification;
- to respect the rules of use of the mark and label established for the EUCC certificate

EUCC CERTIFICATES

- **Maximum period of validity:** five years for products certificates, no limit for PPs
- **NCCAs will monitor certificates** based on sampling, and on non-conformity/compliance of certified products and CBs/ITSEFs
- **CBs and ITSEFs will also have monitoring activities**
- **Vendors will have to monitor vulnerability information,** and to handle non compliances and vulnerabilities
- **A label is foreseen** to promote the certificates
- **Mutual recognition** with third countries is foreseen

EUCC REQUIREMENTS REGARDING THE CABS

Notification of CABs based on:

- **Substantial level:** accreditation of CBs according to ISO/IEC 17065 and of related ITSEFs according to ISO/IEC 17025
- **High level:** accreditation of CBs according to ISO/IEC 17065 and of related ITSEFs according to ISO/IEC 17025, plus their authorisation by a NCCA

CB and ITSEF: appropriate competence management system for the personnel based on ISO/IEC 19896-1.

Specific for ITSEFs:

- ISO/IEC 17025 complemented by ISO/IEC 23532-1 (lab) and ISO/IEC 19896-3 (evaluators)

Foreseen promotion of notified CABs: ENISA Certification website + mark & label

EUCC REQUIREMENTS REGARDING THE CABS

Difference between accreditation and authorization: review* by the NCCA of the CB (resp. ITSEF):

- Competences and expertise to certify (resp. evaluate)
- Capability to protect confidential and sensitive information

*Based on structured interviews and a review of two pilot certifications (resp. evaluations) performed by the certification body (resp. ITSEF)

Specific for ITSEFs:

- Requirements defined for Technical Domains evaluations defined in SOG-IS documentation
- For AVA_VAN.3 evaluations: ENISA guidance available

Authorisation duration: 3 years

Peer assessment of CBs (including associated ITSEFs)

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Ethnikis Antistaseos 72 & Agamemnonos 14, Chalandri 15231
Attiki, Greece

☎ +30 28 14 40 9711

✉ certification@enisa.europa.eu

🌐 www.enisa.europa.eu