

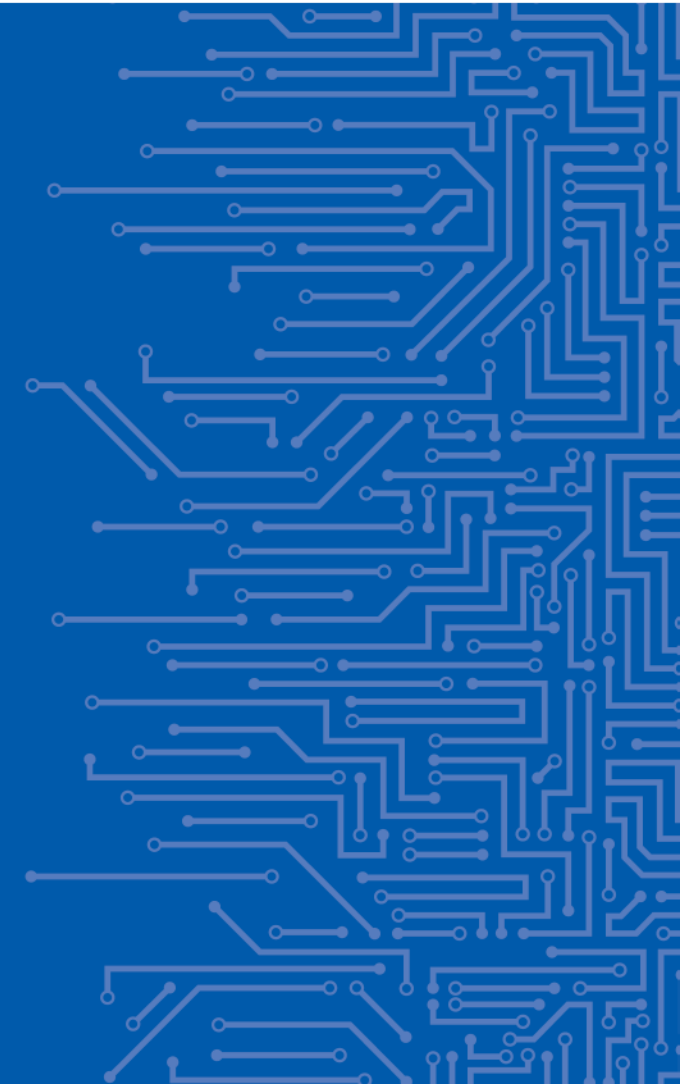


EUROPEAN UNION AGENCY
FOR CYBERSECURITY

AN UPDATE ON SCHEMES DEVELOPMENTS

Philippe Blot / Vassiliki Gogou
Cybersecurity Certification sector
Market, Certification & Standardisation Unit

09 | 11 | 2023



EU REGULATIONS AROUND EU CYBER CERTIFICATION



European Commission

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

European Chips Act

The European Chips Act... In semiconductor... digital and green... technological lead...

The need for EU action

Chips are strategic assets for key industrial value chains. Markets for the chip industry are emerging such as high connectivity, space, defence and supercomputers.

1 trillion microchips were manufactured around world in 2020

Recent global semiconductor shortages forced factory closures in... 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 capabilities.

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



EUROPEAN COMMISSION

Brussels, 21.4.2021
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 ACTS
(SEC(2021) 167 final) - (SWD(2021) 84 final) - (SWD(2021) 85 final)

TITLE III

1. High-risk AI systems shall comply with the requirements established in this Regulation.

2. The intended purpose of the high-risk AI system and the risk management system shall be established, implemented, and updated throughout the lifecycle of the high-risk AI system.

3. A risk management system shall be established, implemented, and updated throughout the lifecycle of the high-risk AI system. It shall consist of a continuous iterative process of:

- identification and analysis of the known and foreseeable risks;
- estimation and evaluation of the risks that may emerge from the high-risk AI system;
- evaluation of other possibly arising risks;
- adoption of suitable risk management measures.

4. The risk management measures referred to in paragraph 3 shall be based on the generally acknowledged state of the art, including the state of the art in the field of artificial intelligence.



Think Tank
European Parliament

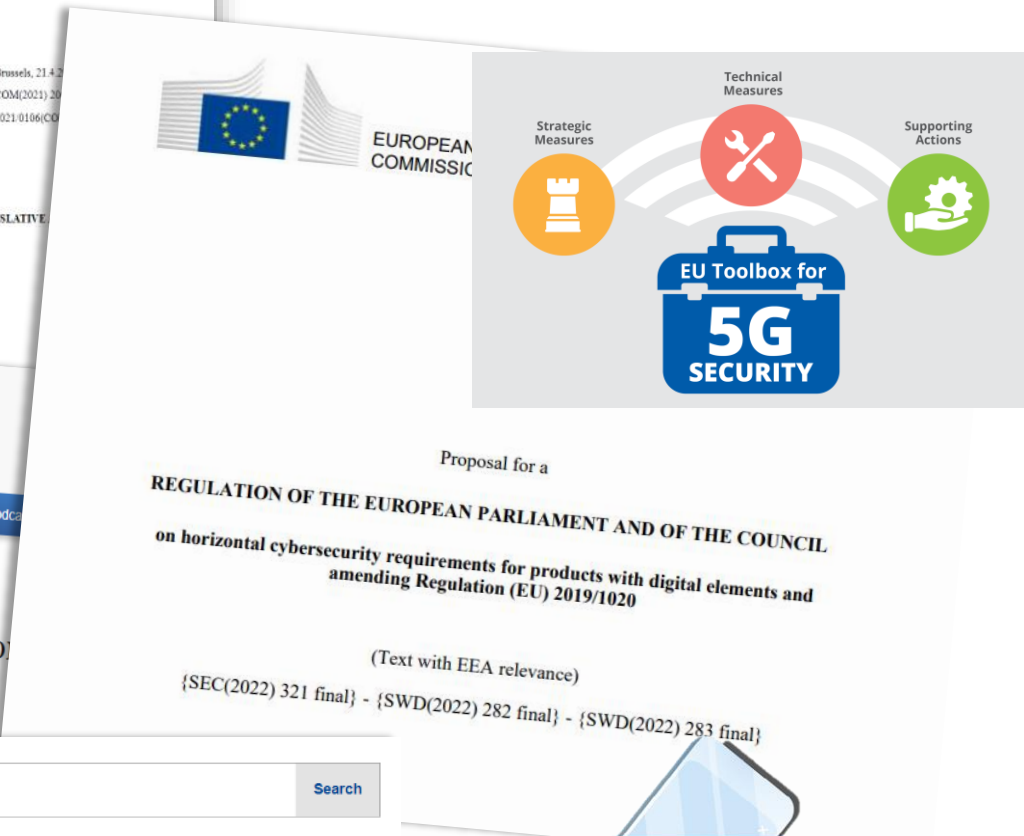
Home Research Events Infographics Sources Partners Audio podcasts

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

The NIS2 Directive: A high common level of cybersecurity in the EU

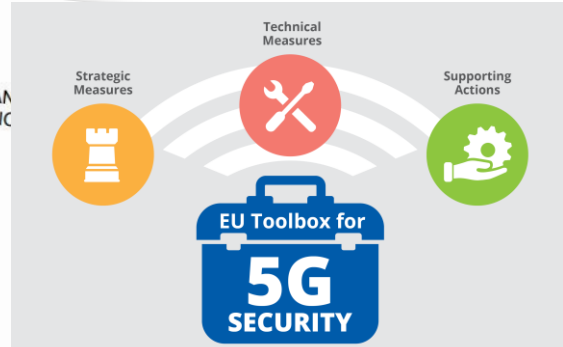
Briefing - 16-06-2022

The Network and Information Security (NIS) Directive...



EUROPEAN COMMISSION

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}



Strategic Measures

Technical Measures

Supporting Actions

EU Toolbox for 5G SECURITY



European Commission

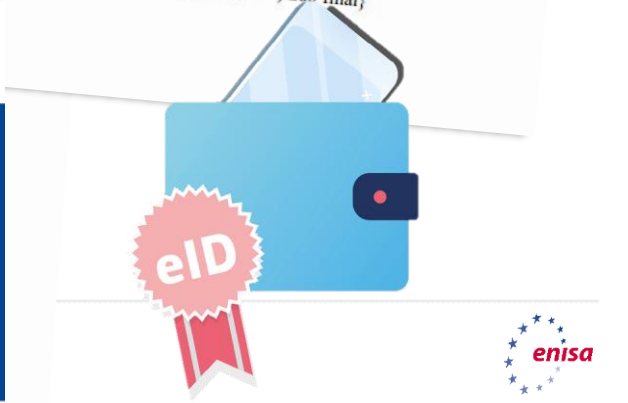
English EN

Home > Press corner > Cyber: towards stronger EU capabilities


Available languages: English

Press release | 18 April 2023 | Strasbourg

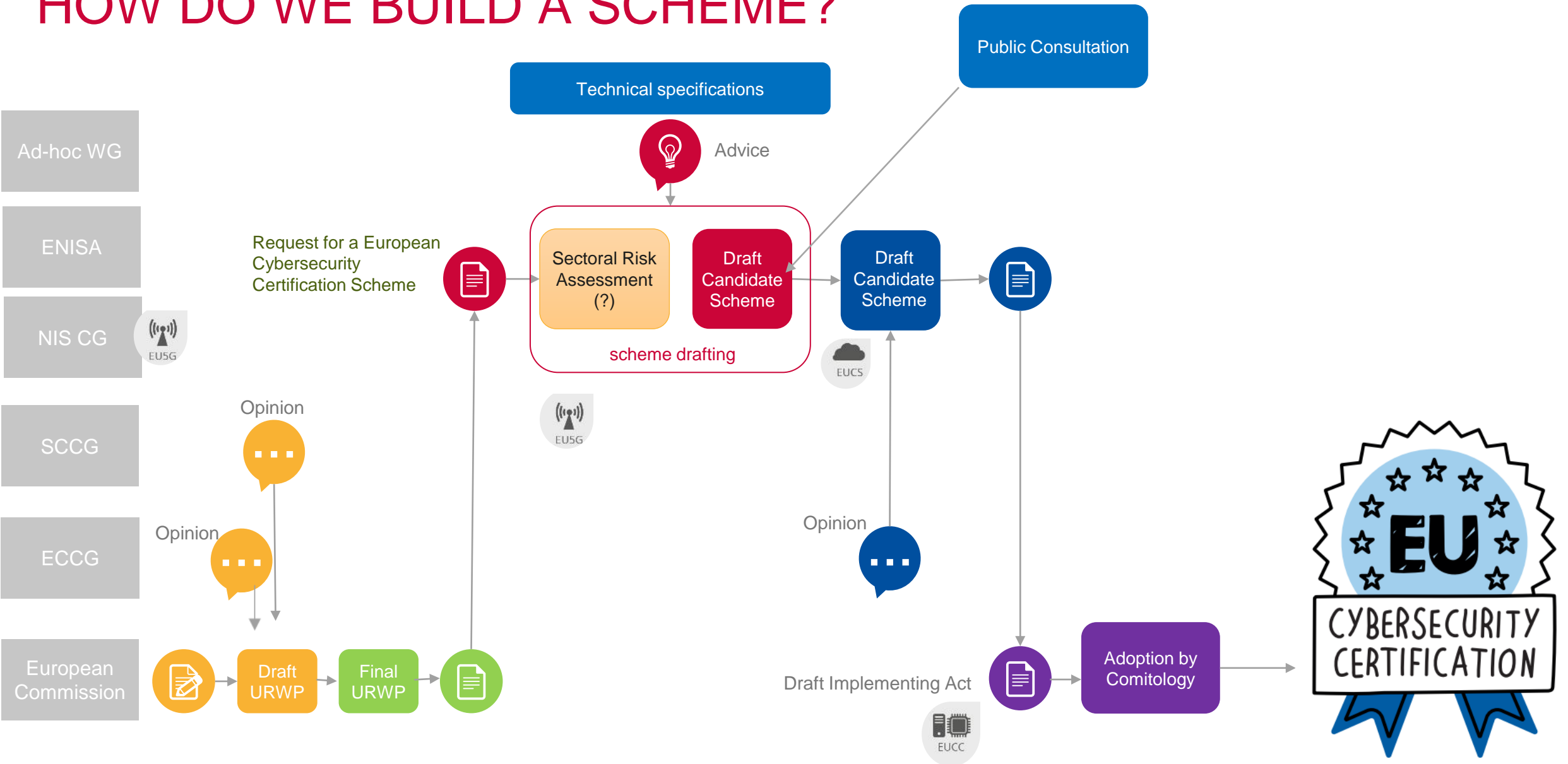
Cyber: towards stronger EU capabilities for effective operational cooperation, solidarity and resilience



eID



HOW DO WE BUILD A SCHEME?



CURRENT ACTIVITIES ON EUCC



- **Implementing Act** (ENISA support to the EC) based on the candidate scheme
- **Maintenance strategy**
- **Reuse of national supporting documents**
- **Cryptography**
- **Certification.enisa.europa.eu** ENISA website dedicated to certification and stakeholders' platform to provide guidance and gather the ecosystem



OTHER ACTIVITIES IN LIAISON WITH EUCC



EUCC

EU5G

for eUICC certification

eIDAS/wallet

may mandate EUCC certification or reuse EUCC certificates as a presumption of conformity

AI feasibility study

will analyse how to reuse EUCC certification and where different evaluation methods would be necessary

Cyber Resilience Act (CRA)

how to use EUCC certificates for presumption of conformity to CRA essential requirements as defined in Annex I

CURRENT ACTIVITIES ON EUCS



- **CEN-CENELEC is making progress on the elements passed by ENISA (security controls) for their transformation and maintenance into Technical Specifications**
- **Candidate scheme under revision for final release**
- **EUCC Implementing Act will have to be considered**
- **Guidance development has been launched**
- **Discussion at ECCG has started**

CURRENT ACTIVITIES ON EU 5G



- **The AHWG supporting ENISA (established Q4 2021) is composed of a rich representation of relevant stakeholders:**
 - eUICC and network products developers
 - CABs
 - MNOs
 - standardisation and specification organisations including ESOs, and GSMA
 - national authorities, both telco and cybersecurity regulators
- **ENISA plans a first draft of the scheme(s) to be available for public review Q1 of 2024**

EU 5G SCHEME VERSION 1



2022- 2023: 7 EU 5G AHWG Thematic Groups
Mid 2023: 3 Thematic Groups & 1 Thematic Group on accreditation

Thematic Group eUICC

eUICC certification to be based on the EUCC scheme with the appropriate Protection Profile(s) to allow also convergence with the eIDAS/wallet

Thematic Group NESAS

Existing GSMA/3GPP schemes and structures on NESAS to be transformed into a relevant EU scheme, reusing lessons learnt from national implementations

Thematic Group SAS

Existing GSMA SAS-UP/SAS-SM processes on SIM provisioning and eUICC secure development to be transformed to the possible extend into a relevant EU scheme, in close relation with the other schemes under development (EUCC and EUCS)

Accreditation requirements

Vulnerability handling rules



ADAPTING THE SCHEMES FOR SPECIFIC SECTORS

- **Both the EUCC and EUCS have been designed to allow to cover sectoral specific needs and EU 5G is being designed in that mindset as well:**
 - **The EUCC scheme allows the development and certification of Protection Profiles and where necessary to extend existing functional and assurance requirements**
 - **The EUCS scheme allows the development of specific extension profiles for different uses**
 - **The EU 5G scheme is still under development**

HOW TO BE INVOLVED AND LEARN THE PROGRESS OF CYBERSECURITY CERTIFICATION

AHWGs and public consultations

Website: <https://certification.enisa.europa.eu/>
CEF platform

Awareness Raising Videos :

3 episodes on Youtube: [ENISAvideos](#)

Tradeshows and Events:

Annual Cybersecurity Certification Conference

Presentations, Talks & Social Media:

Follow [European Union Agency for Cybersecurity \(ENISA\)](#) on LinkedIn
and [@enisa_eu](#) on Twitter

ENISA Certification video
playlist:



THANK YOU FOR YOUR ATTENTION

Philippe Blot, Head of Cybersecurity Certification Sector

Vassiliki Gogou, Cybersecurity Expert

Market, Certification & Standardisation Unit

ENISA, The European Agency for Cybersecurity



Philippe.blot@enisa.europa.eu /
Vassiliki.gogou@enisa.europa.eu

