National Certification Structure and Schemes based on Cyber Security Act (CSA)

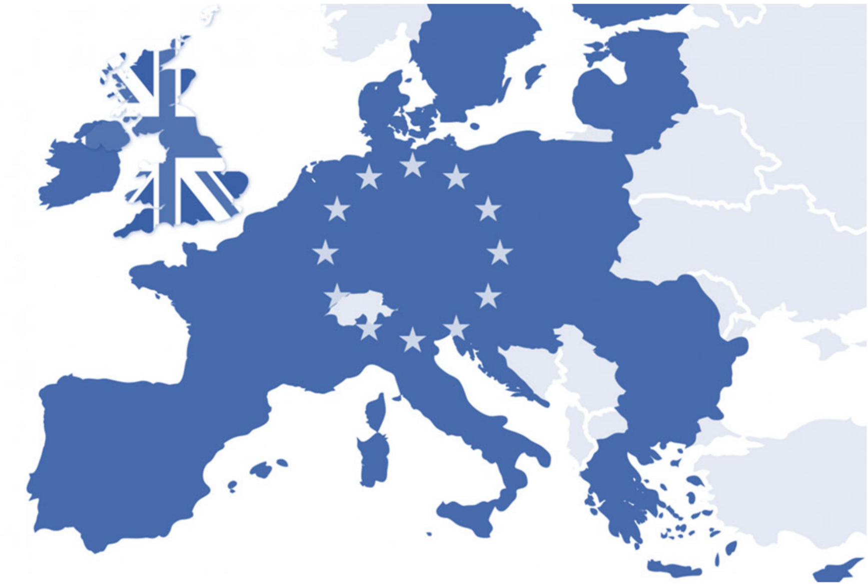
George Hadjichristofi
Team Leader NCCA

ΕΠΙΤΡΟΠΟΣ
ΕΠΙΚΟΙΝΩΝΙΩΝ

Αρχή
Ψηφιακής
Ασφάλειας

Γεώργιος Μιχαηλίδης
Επίτροπος Επικοινωνιών
www.dsa.cy/ | www.csirt.cy/

WHAT IS THE CYBERSECURITY ACT?



- Revamps and strengthens the EU Agency for cybersecurity, ENISA (17)
- Establishes an EU-wide cybersecurity certification framework for digital products, services and processes. (48)
- Certification of ICT products, processes and services are recognised across the European Union. (69)

Definitions

- **‘ICT product’** means an element or a group of elements of a network or information system;
- **‘ICT service’** means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems;
- **‘ICT process’** means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service;
- Common examples are:
  - integrated circuits and smartcards for electronic signature, identification (passports), tachographs for lorries, and software products (e.g. disk encryption, VPN clients…).

Benefits to vendors

Demonstrate that their products or services have been attested to fulfil specific requirements

Provide evidence to the market and to regulators of their commitment to good cybersecurity practices

Benefits to customers

Providing them with the appropriate level of confidence that specific requirements have been fulfilled

Capture and expresses requirements from broad communities of end users

Benefits to Regulators

Demonstrate the presumption of conformity
with advancements in Cybersecurity
(European level or Member state level)

Actors and Roles in Certification

Actors and roles: European Commission

Article 47

- Publish a Union rolling work programme for European cybersecurity certification

- Request ENISA to prepare a candidate scheme
  or review an existing scheme

Actors and roles: SCCG

STAKEHOLDER CYBERSECURITY CERTIFICATION GROUP (SCCG)
Article 22

- Composed of members selected from amongst recognised experts representing the relevant stakeholders
- 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
- Advice the Commission & ECCG on the need for additional certification schemes.

Actors and roles: 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
- Participate in ECCG (EU Cybersecurity Certification Group)

Actors and roles: ECCG

EUROPEAN CYBERSECURITY CERTIFICATION GROUP (ECCG)
Article 62

- Facilitate alignment of European cybersecurity certification schemes with internationally recognised standards
- Facilitate cooperation between NCCAs
- Advise & assist ENISA in EU CSA implementation
- Advise & assist ENISA in preparing candidate schemes. Article 48
- Comprises NCCAs from member countries.

Actors and roles: ENISA

(Article 49)

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

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

Actors and roles: ADHOC Working Group

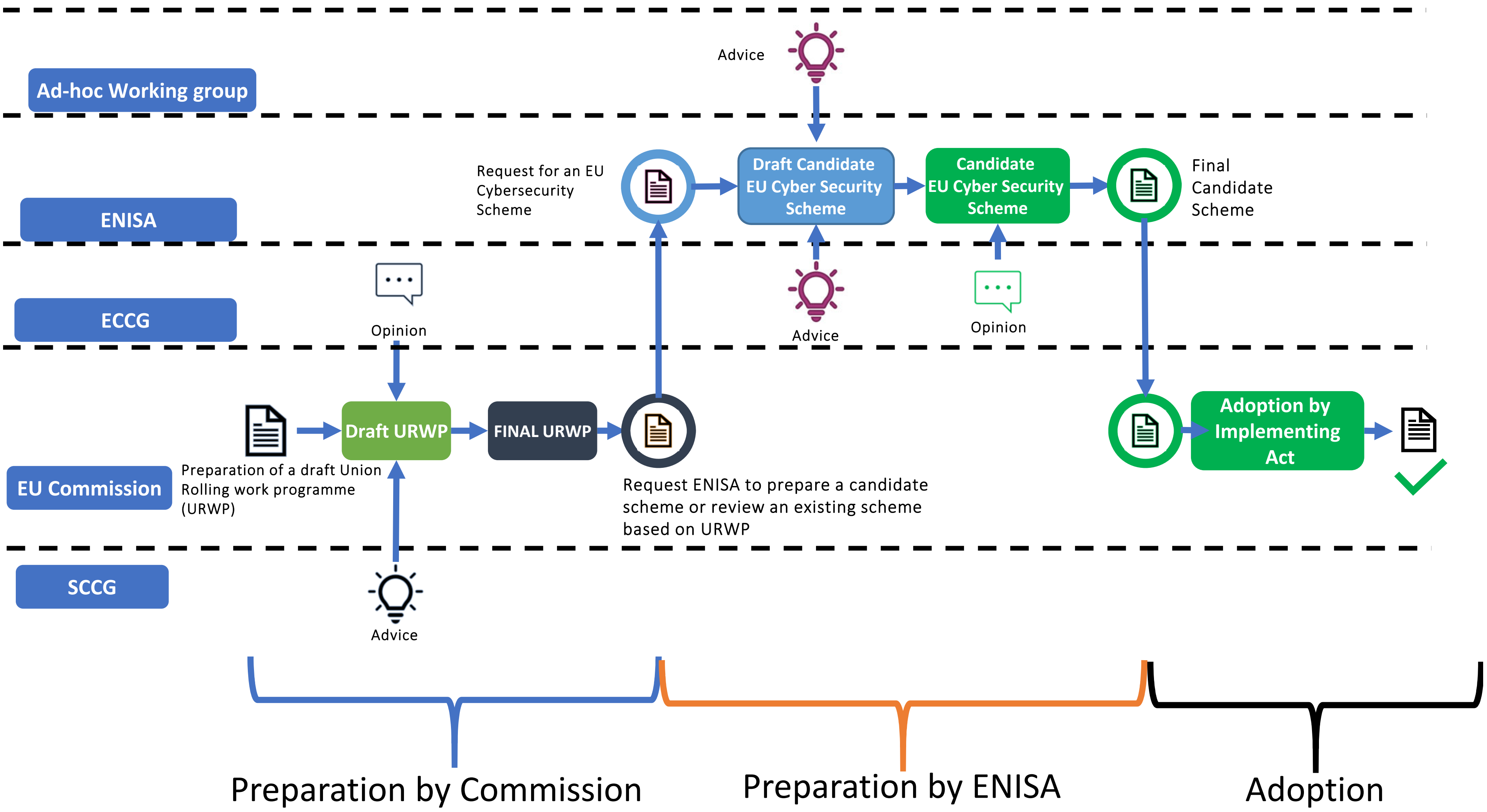
ADHOC WORKING GROUP
(AWG)
Article 20

➡ Tasked with providing to ENISA, specific advice and expertise on a subject matter

- A candidate scheme

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

EU CYBERSECURITY CERTIFICATION FRAMEWORK



Ad-hoc Working group

ENISA

ECCG

EU Commission

SCCG

Preparation of a draft Union Rolling work programme (URWP)

Draft URWP

FINAL URWP

Opinion

Advice

Request ENISA to prepare a candidate scheme or review an existing scheme based on URWP

Request for an EU Cybersecurity Scheme

Advice

Draft Candidate EU Cyber Security Scheme

Advice

Candidate EU Cyber Security Scheme

Opinion

Final Candidate Scheme

Adoption by Implementing Act

Preparation by Commission

Preparation by ENISA

Adoption

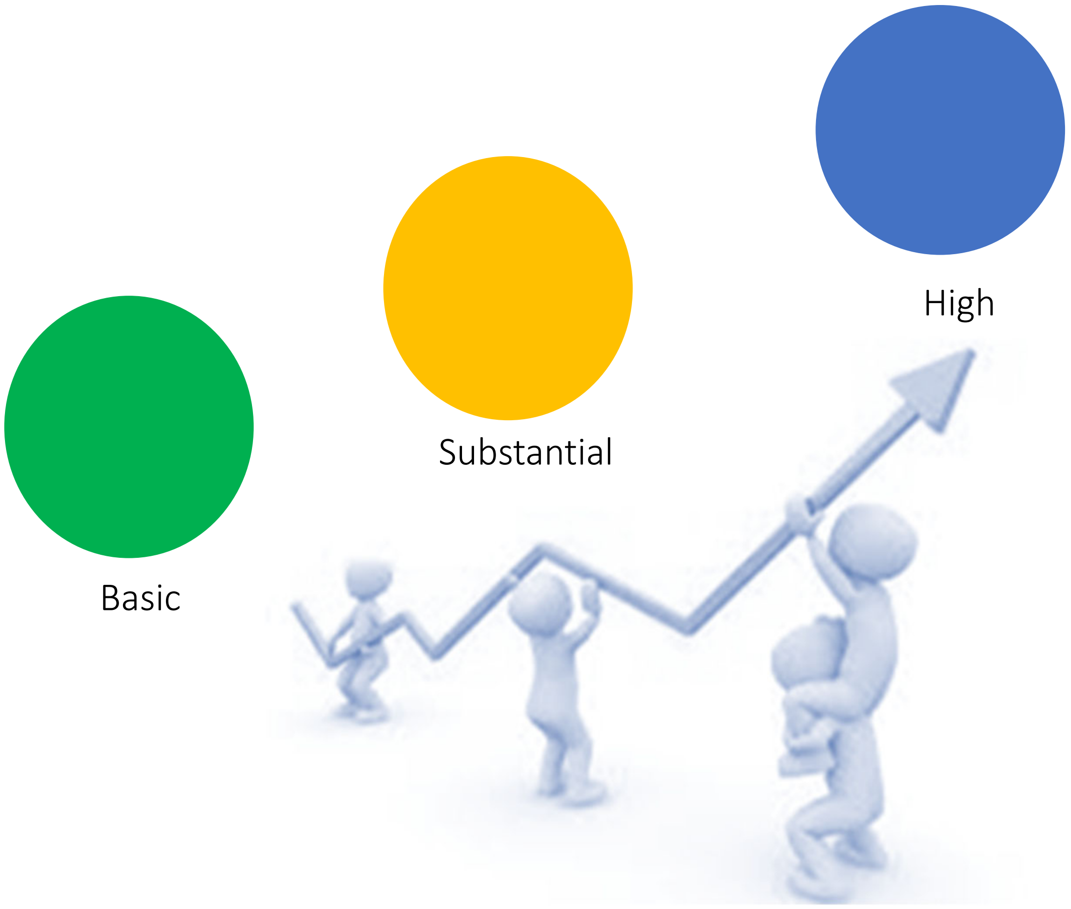
03

CYBERSECURITY CERTIFICATION schemes

R

EU CERTIFICATION SCHEMES: ASSURANCE LEVELS

ARTICLE 52



Basic

Substantial

High

Certification is Voluntary

EU CERTIFICATION SCHEMES: EUCC

Third party assessment (CABs)

- First candidate cybersecurity certification scheme request received by ENISA under CSA - July 2019
- The EUCC scheme covers the certification of ICT products
- It uses the Common Criteria ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security

EUCC Candidate scheme highlights

- It is more of a horizontal scheme, covering different types of generic and sector specific ICT products
  - Users of the scheme may establish Protection Profiles to express their security requirements

- The EUCC scheme covers assurance levels ‘substantial’ and ‘high’ of the CSA

- It addresses the requirements of the CSA:
  - Security objectives (art. 51)
  - Assurance levels (art. 52)
  - Elements of European Cybersecurity Certification Schemes (art.54)

EUCC

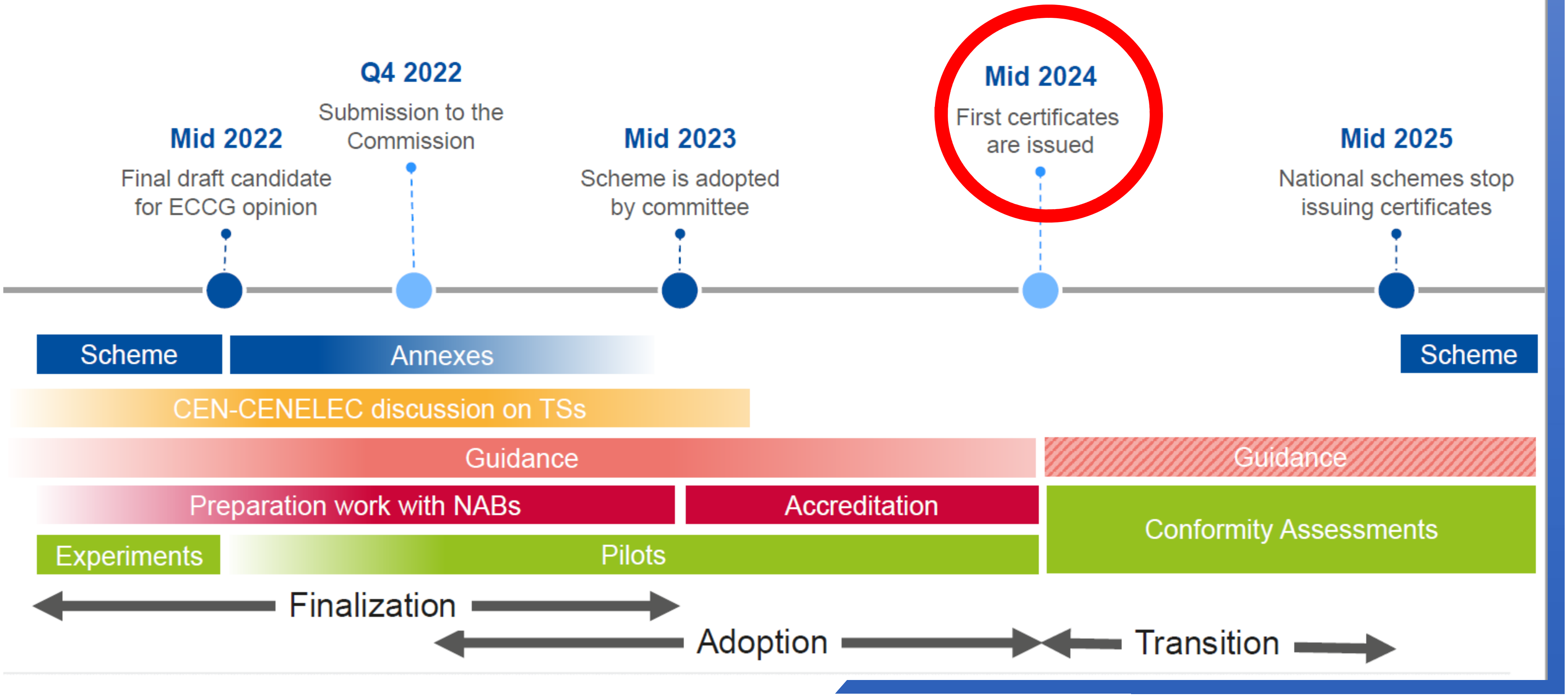
- It ensures **assurance continuity of the certificates**, covering
  - the monitoring and handling of non-compliances and non-conformities;
  - vulnerability handling and disclosure;
  - and introduces **a patch management mechanism** that can be part of the certification and will ease maintaining the products and certificates up-to-date.
- The draft EUCC scheme has been documented and is awaiting the **EU Implementing Act**
    - More info could be provided at 2023 Cybersecurity Certification Conference May 25th, 2023

R

EU CERTIFICATION SCHEMES: EUCS

- Certification of the cybersecurity of **Cloud Services**
- Cloud service providers of any size can use it to **demonstrate** that they have set up a framework for **guaranteeing some security of their customers**
- EUCS supports the three assurance levels in the EUCSA: ‘basic’, ‘substantial’ and ‘high’.
- The ‘substantial’ level may be the level of choice for many applicants and their users
- Ad Hoc Working Group provided the **draft candidate scheme on March 5th 2020**

EUCS SCHEDULE – JUNE 2022



Mid 2022
Final draft candidate
for ECCG opinion

Q4 2022
Submission to the
Commission

Mid 2023
Scheme is adopted
by committee

Mid 2024
First certificates
are issued

Mid 2025
National schemes stop
issuing certificates

Scheme

Annexes

Scheme

CEN-CENELEC discussion on TSs

Guidance

Guidance

Preparation work with NABs

Accreditation

Conformity Assessments

Experiments

Pilots

Finalization

Adoption

Transition

There is a significant amount of work to be done

EU CERTIFICATION SCHEMES: EU5G

- Certification of Cybersecurity in 5G Communication

- Scheme drafting was to start at the beginning of 2023

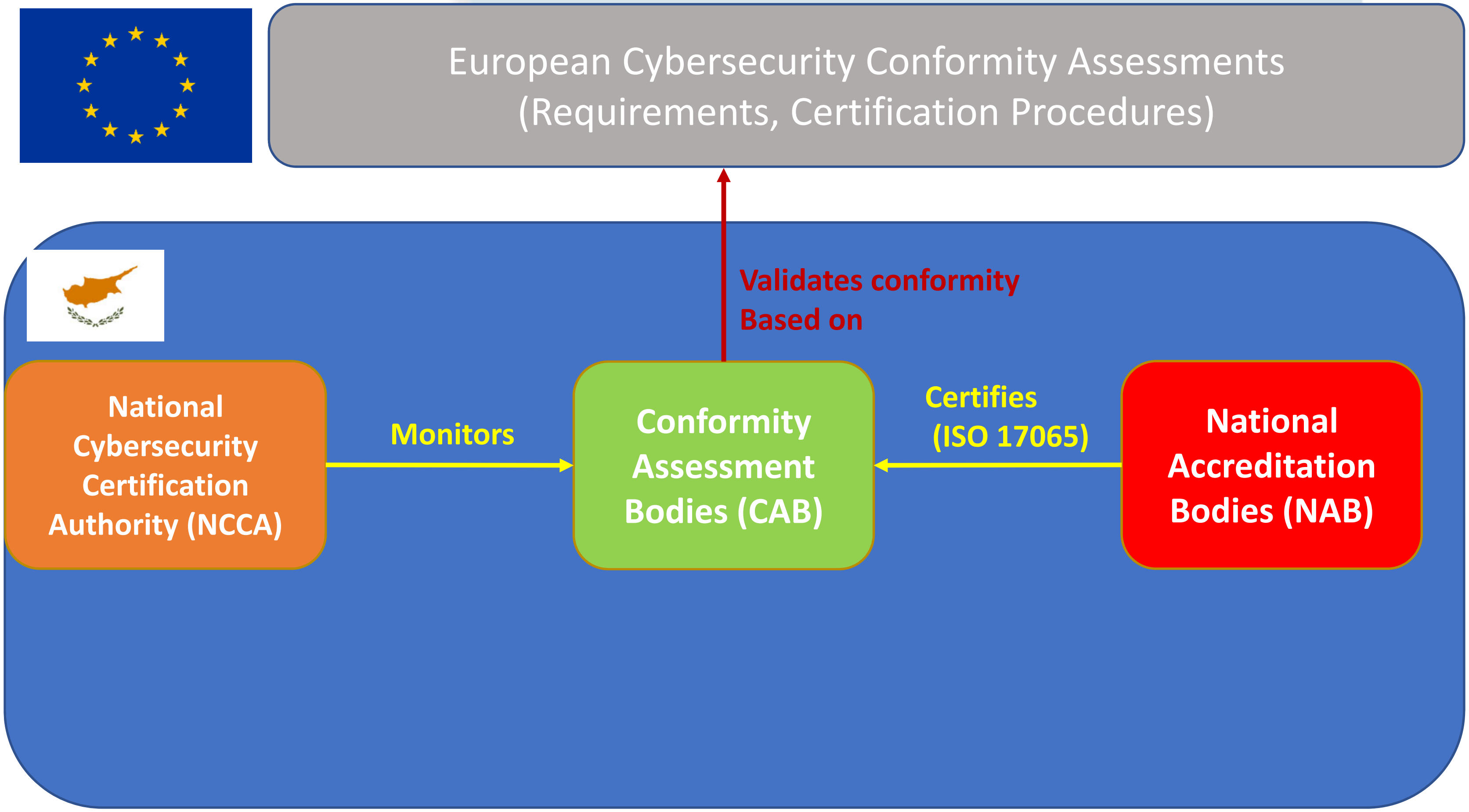
- Version 1 of the candidate scheme could be available at the end of Q2 2023 for a first review

- ENISA works with an AHWG structure (approx. 100 members) and organises specific thematic groups to work on grouped tasks

Certification Entities

- National Certification Authority (NCCA)
- Conformity Assessment Bodies (CAB)
- National Accreditation Bodies
- Testing Labs

Cybersecurity Certification in Cyprus



European Cybersecurity Conformity Assessments
(Requirements, Certification Procedures)

Validates conformity
Based on

National Cybersecurity Certification Authority (NCCA)

Monitors

Conformity Assessment Bodies (CAB)

Certifies
(ISO 17065)

National Accreditation Bodies (NAB)

NCCA DUTIES

National Cybersecurity Certification Authorities (NCCA)
Article 58

- Monitor and enforce the obligations of manufacturers or providers of ICT products, services, processes in relation to the EU statement of conformity
- Monitor relevant developments in cybersecurity certification field
- Handle complaints in relation to CAB-issued or NCCA-issued certificates.
- Share information regarding non-compliance of products processes & services with other NCCAs .
- Assist NABs in monitoring & supervision of CABs
- Issuing certificates, particularly for the “High” assurance level.

EU CERTIFICATION: BECOMING A CAB

- Shall possess the means & tools necessary to perform evaluations
- Shall be technically capable, covering all categories of evaluations which it undertakes.
- Shall be independent & avoid conflict of interests
- Shall be a legal entity under a national law
- Shall demonstrate professional integrity
- Shall take a liability insurance.
- Shall be compliant to relevant standards for accreditation of a CAB.

R

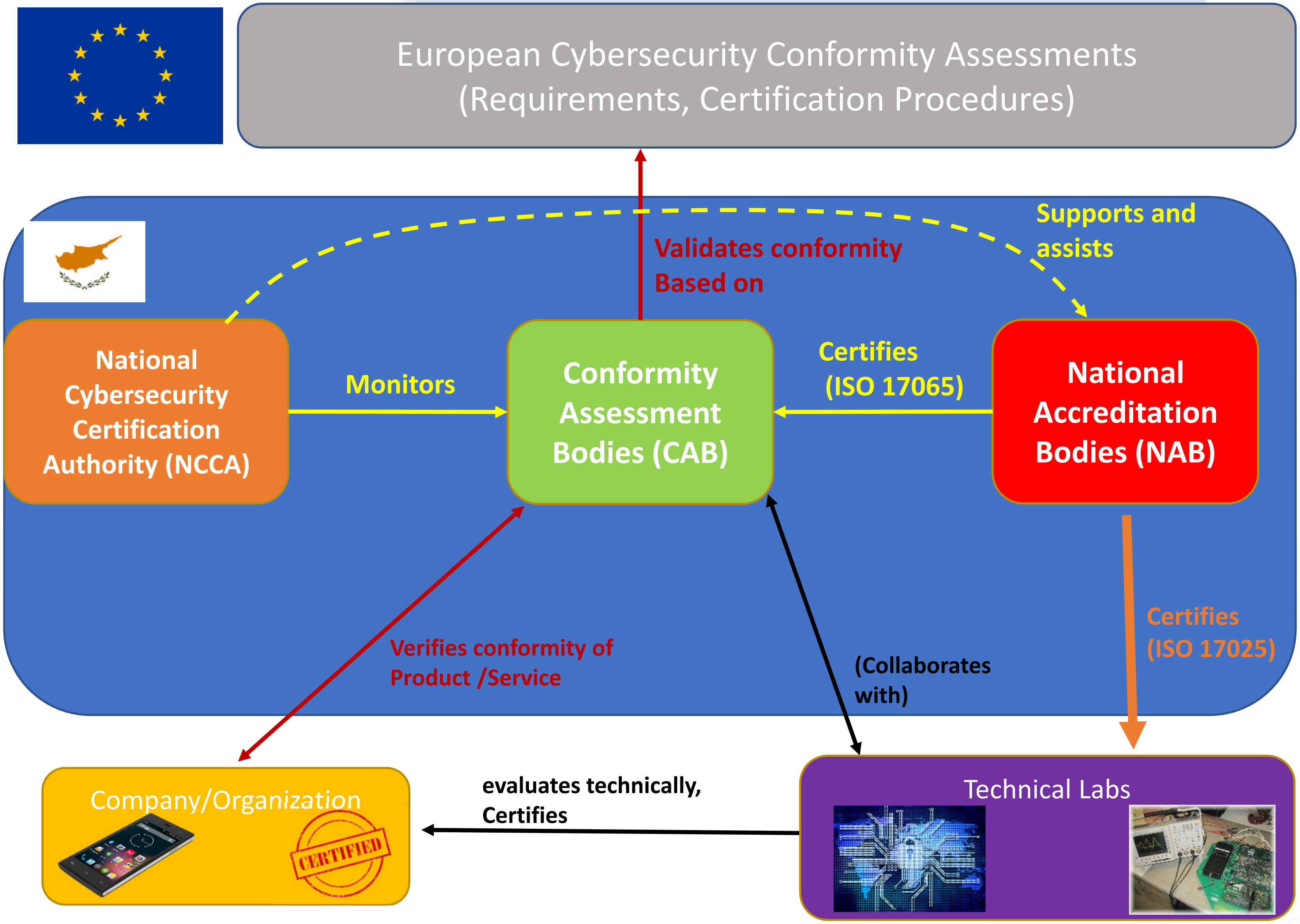
NATIONAL ACCREDITATION BODY

National Accreditation Body (NAB)
Article 60

- National accreditation body (NAB) is **the sole body in a Member State** that performs accreditation with authority derived from the State
- **Restrict, suspend or withdraw CABs accreditation** due to non-compliance to CSA or a Certification Scheme.
- Accrediting CABs (MAX 5yrs validity).

QUALITY CONTROL APPROVED

Cybersecurity Certification in Cyprus



European Cybersecurity Conformity Assessments
(Requirements, Certification Procedures)

Supports and assists

Validates conformity
Based on

National Cybersecurity Certification Authority (NCCA)

Monitors

Conformity Assessment Bodies (CAB)

Certifies
(ISO 17065)

National Accreditation Bodies (NAB)

Certifies
(ISO 17025)

Verifies conformity of
Product /Service

(Collaborates
with)

Company/Organization

CERTIFIED

evaluates technically,
Certifies

Technical Labs

CEF B4C – Building up the Cybersecurity Certification Capabilities of Cyprus

- The project had the following objectives:
  - **to determine the provisions of the Regulation which must be transferred to the DSA law**
    - The Authority needs to have the **appropriate powers and responsibilities**
  - **to develop the internal capabilities of DSA** for the effective undertaking of the control and supervision obligations of cyber security certifications in Cyprus,
  - **to promote the exchange of best practices** and relevant information on certification, with peer support in cybersecurity certification within the EU.
- Duration:18 months (July 2020- December 2021)
- **<u>Budget:</u> €160,000** (of which €40,000 was covered by the DSA)

CEF A4CEF - Advancing Cybersecurity Certification Capabilities with Cross-border exchange and Enhancing (business) Flows

- Cross-border **exchange of best practices** and relevant information related to conformity assessment activities
  - two-way exchange between **Cyprus and Ireland**;
- Building an **integrated reference model** to directly support the full range of Cybersecurity certification activities
  - Interactions and flows
- Strengthening the internal capabilities of all partners through new educational material for the **certification of Cloud Computing Services**
- **Duration: 3 years (**December 2020 – December 2023)

- **Budget**: **€280,000**.

Current Tasks

- Identifying and Extracting ALL requirements of the NCCA based on CSA
- Setting up collaboration framework between NCCA and CAB and NCCA and NAB
- Defining the duties of each party (MOUs preparation)
  - NCCA
  - Conformity Assessment Body (CAB)
  - National Accreditation Body
  - Lab
- Defining the business model

Next step for certification

- Before EUCC is released (May 2023)
  - Training on EUCC, EUCS
  - Gathering of legal aspects (compliance, complaints, penalties)
- After EUCC is released (June – July 2023)
  - Agree on project readiness and setup deadlines once
    - Certification of labs, CAB on 17065, 17025
    - MOU with various parties involved (NAB)
    - Pilot tests
    - Publication of any relevant Secondary Law
  - Define the process of handling HIGH levels of security

BuCfES - BUilding Cybersecurity Certification processes for Enhanced Surveillance

- The project's overall objective is **to improve the capabilities of NCCA and Conformity Assessment bodies (CAB)**
- Foster collaboration and **exchange of information** between NCCAs and CABs of EU member states in **Ireland and Cyprus**
- The workplan includes a series of **trainings in vulnerability handling**
  - **EU Cloud Services and EU Common Criteria schemes**
- The project also includes **pilot projects** involving external participants (SMEs)
- The **development of an AI powered tool** that will support information gathering and exchange between participants (NCCAs, CABS, manufacturers/service providers) in EU schemes
- **Submission date:** February 15th, 2023
- **Duration:** 3years
- **Budget:** € ***517 622***

Ευχαριστούμε!
Thank you!

ΕΠΙΤΡΟΠΟΣ
ΕΠΙΚΟΙΝΩΝΙΩΝ

Αρχή
Ψηφιακής
Ασφάλειας

Γεώργιος Μιχαηλίδης
Επίτροπος Επικοινωνιών
www.dsa.cy/ | www.csirt.cy/