EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CERTIFICATION SCHEMES AND STANDARDIZATION IN CYBERSECURITY

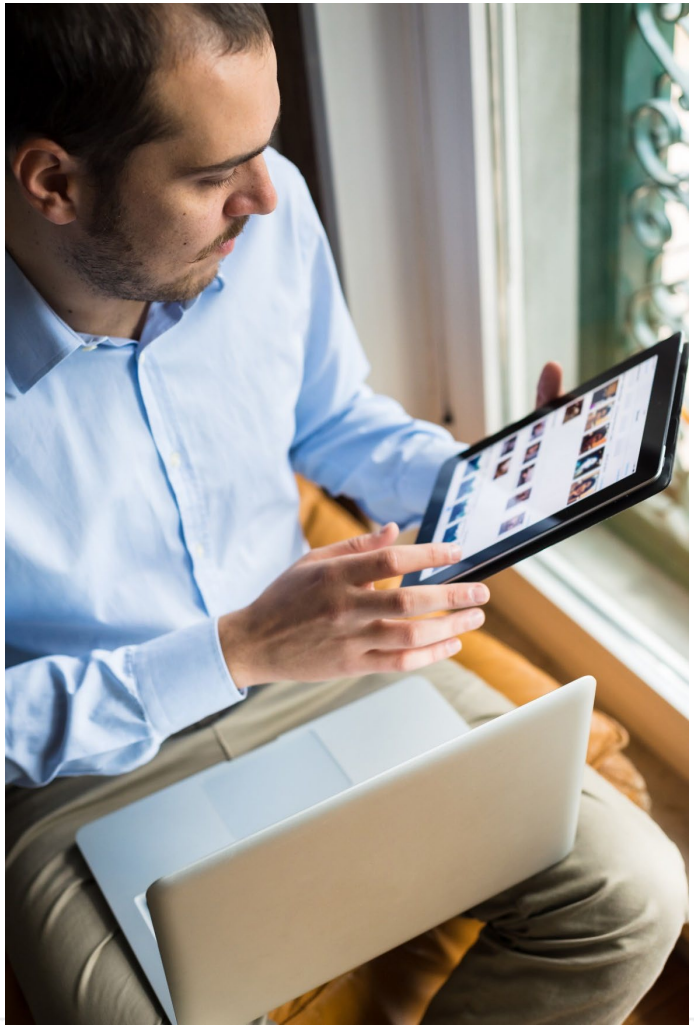
Eric Vetillard, Ph.D.
Lead Certification Expert, MCS, ENISA
Char, EUCS AHWG

17 | 03 | 2023

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.



VISION & MISSION

Vision:

A Trusted and Cyber Secure Europe

Mission:

Achieving a high common level of cybersecurity across the Union in cooperation with the wider community through:

- Acting as a centre of expertise on cybersecurity
- Collecting and providing independent, high quality technical
- Providing advice and assistance to Member States and EU bodies on cybersecurity
- Contributing to developing and implementing the Union's cyber policies

AREAS OF WORK

Cloud and Big Data

COVID19

Critical Infrastructures and Services

CSIRT Services

CSIRTs and communities

CSIRTs in Europe

Cyber Crisis Management

Cyber Exercises

Cybersecurity Education

Data Protection

National Cybersecurity Strategies

NIS Directive

Standards and Certification

Threat and Risk Management

Cyber Crisis Management

IoT and Smart Infrastructures

Trust Services

Trainings for Cybersecurity Specialists

CHAPTER 0

CERTIFICATION 101

WHAT IS CERTIFICATION?

Certification is about third parties making statements about a product, service or process.

certification (from ISO/IEC 17000:2020, 7.6)
- third-party **attestation** related to an object of **conformity assessment**, with the exception of **accreditation**

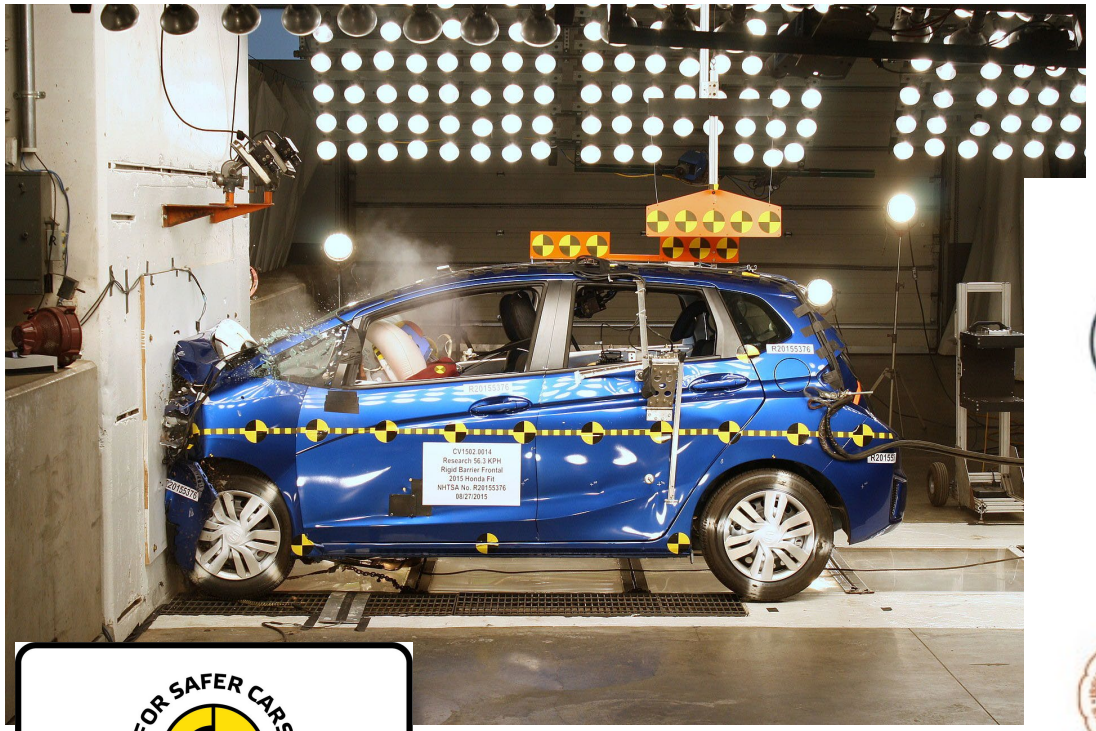
attestation (from ISO/IEC 17000:2020, 5.2)
- issue of a statement, based on a decision, that fulfilment of specified **requirements** has been demonstrated

conformity assessment (from ISO/IEC 17000:2020, 4.1)
- demonstration that specified **requirements** are fulfilled

requirement (from ISO/IEC 27000:2018, 3.56)
- need or expectation that is stated, generally implied or obligatory

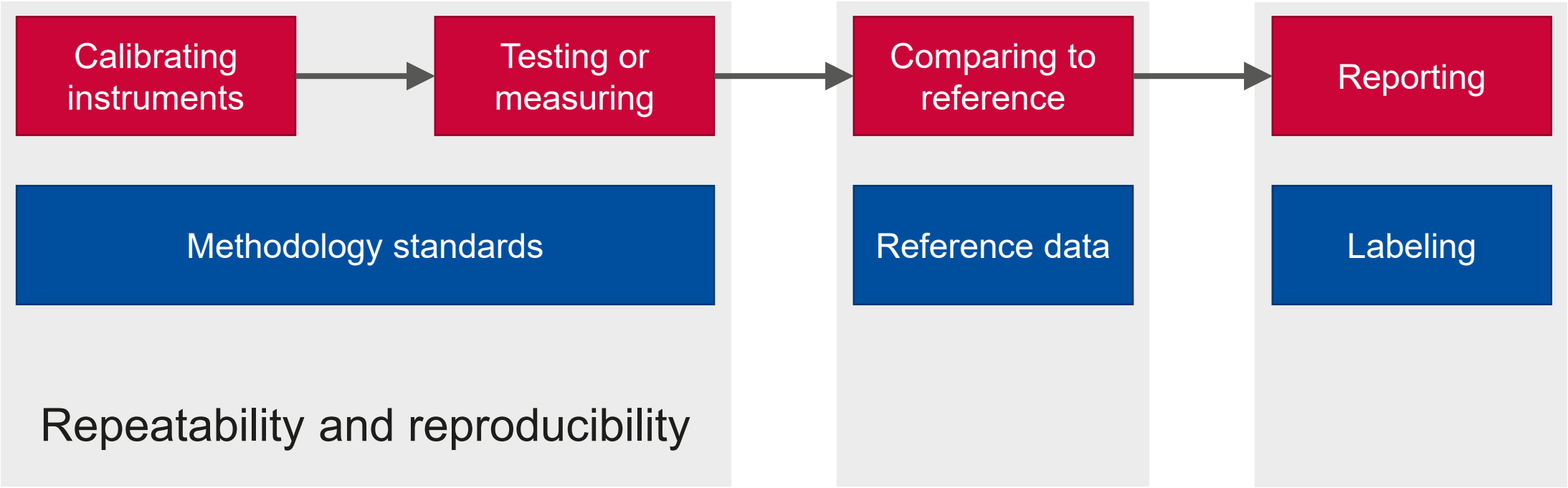
accreditation (from ISO/IEC 17000:2020, 7.7)
- third-party **attestation** related to a **conformity assessment** body, conveying formal demonstration of its competence, impartiality and consistent operation in performing specific **conformity assessment** activities

CERTIFICATION IS EVERYWHERE…



TRADITIONAL CERTIFICATION ACTIVITIES

Traditionally, certification is about measuring and testing, and comparing the actual results to expected results.



REPEATABILITY VS. REPRODUCIBILITY

Verifying your own results

Measure of the variability of measurements

- By the same person on the same setup, using the same method

Ensures that results are not “random”

- The tester is able to perform the measurement again with limited differences between setups
- But the quality of the result may depend on the operator skills and setup performance

Obtaining consistent results

Measure of the variability of measurements

- Performed by different persons on different setups, using the same method

Ensures that similar results can be obtained

- The method and calibration allows different testers to obtain consistent results
- The quality of the result is independent from the tester and equipment (provided that they meet the methodology’s requirements).

CAN YOU CERTIFY OTHER THINGS?

Standardized products are “easy” to measure, but you can also certify other things, such as any product, services, processes, or management systems.

Also, a few big categories of certification

- What needs to be verified is fixed and product/service independent (*e.g.* ,toys don’t catch fire)
  - Strict measurement specifications, fixed acceptance criteria
- What needs to be verified is fixed and product/service dependent (*e.g.*, electrical properties)
  - Catalog of requirements, strict measurement specifications
- What needs to be verified is defined by the vendor (e.g., an IT service)
  - Catalog of requirements, product/service description is essential

Certification becomes more challenging when properties and measurement methods cannot be precisely defined.

CERTIFICATION IS DEFINED IN STANDARDS

These are the main standards in the ISO 17000 family.

EN ISO/IEC 17000	**Vocabulary and general principles**
EN ISO/IEC 17011	Requirements for accreditation bodies accrediting conformity assessment bodies
EN ISO/IEC 17020	Requirements for the operation of various types of bodies performing inspection
EN ISO/IEC 17021-1	Requirements for bodies providing audit and certification of management systems
EN ISO/IEC 17024	General requirements for bodies operating certification of persons
EN ISO/IEC 17025	**General requirements for the competence of testing and calibration laboratories**
EN ISO/IEC 17029	General requirements for validation and verification bodies
EN ISO 17034	General requirements for the competence of reference material producers
EN ISO/IEC 17040	General requirements for peer assessment of conformity assessment bodies and accreditation bodies
EN ISO/IEC 17043	General requirements for proficiency testing
EN ISO/IEC 17065	**Requirements for bodies certifying products, processes and services**

THREE ESSENTIAL ASPECTS IN CERTIFICATION

Requirements

The reason for certification

- Better to be specific
- Otherwise, much freedom of interpretation for the CAB

Often defined in standards

- Or in Technical Specifications
- To be listed in an Implementing Act

Assessment

Not specified in EN ISO/IEC 17065 or in 765/2008

- Needs to be properly defined to ensure that objective evidence is sufficient and appropriate
- Defined in many other standards

Monitoring/Governance

Certificate management

- Issuance, duration, *etc*.

Activities after certification

- Surveillance
- Assessment of changes
- Nonconformity handling

Very important for security

CHAPTER 1

BACKGROUND

EU CERTIFICATION SCHEMES?

The EU Cybersecurity Act (EU 2019/881) has defined the idea of a European Cybersecurity Certification Framework.

Certification is seen as a useful tool in the fight for cybersecurity

- An EU-wide framework can promote the use of certification in Europe, reducing market fragmentation
- Harmonization between EU countries is a positive development for vendors, reducing the costs of certifying the same product / service in several schemes and standards
- Certification can be a useful tool for procurement by EU companies and Member States

Certification remains voluntary in principle

- Latest draft regulations mention regulation as a way to be “presumed in conformity” to requirements
- Yet, certification may eventually become mandatory in specific use cases with due justification

THE EU CYBERSECURITY CERTIFICATION FRAMEWORK

Defined in the Cybersecurity Act, together with the role of ENISA.

Strengthens many aspects of certification for cybersecurity

- An improved framework with specific parties and groups
- A requirement for well-defined certification schemes
- Strong requirements on CABs

Contrasts with many other regulations that mention certification

- Many aspects are explicitly mentioned, like monitoring, clear objectives
- There is a notion of level, based on a risk assessment
- But it is not perfect, for instance on the very abstract definition of assurance levels

SOME NOTIONS FROM THE CSA

The Cybersecurity Act is quite recent (2019), so some of its content is quite appropriate.

Article 51 defines security objectives to be covered

- Beyond CIA, mentions logging, vulnerability/incident management, security by default and by design, updates

Article 52 defines assurance levels

- Levels ‘basic’, ‘substantial’ and ‘high’ are defined in very abstract terms
- At least documentation for ‘basic’, functional testing for ‘substantial, penetration testing for ‘high’

Article 55 lists information that shall be made publicly available

- Includes security documentation, support period, contact for vulns, links to vuln repositories

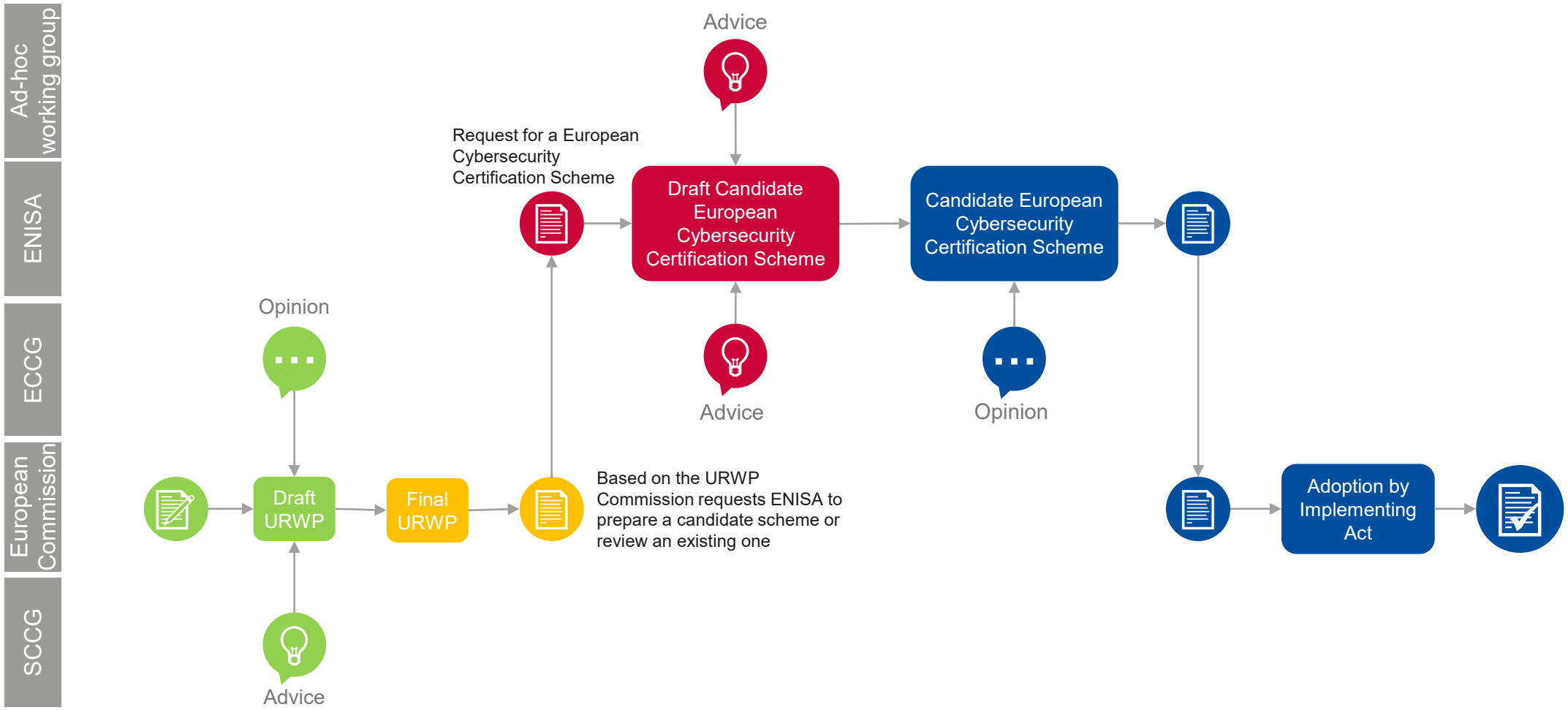
Article 56 defines how certificates can be issued

- ‘basic’ and ‘substantial’ certificates in private sector, ‘high’ only by National Authorities
- Possibilities to delegate certificate issuance for level ‘high’

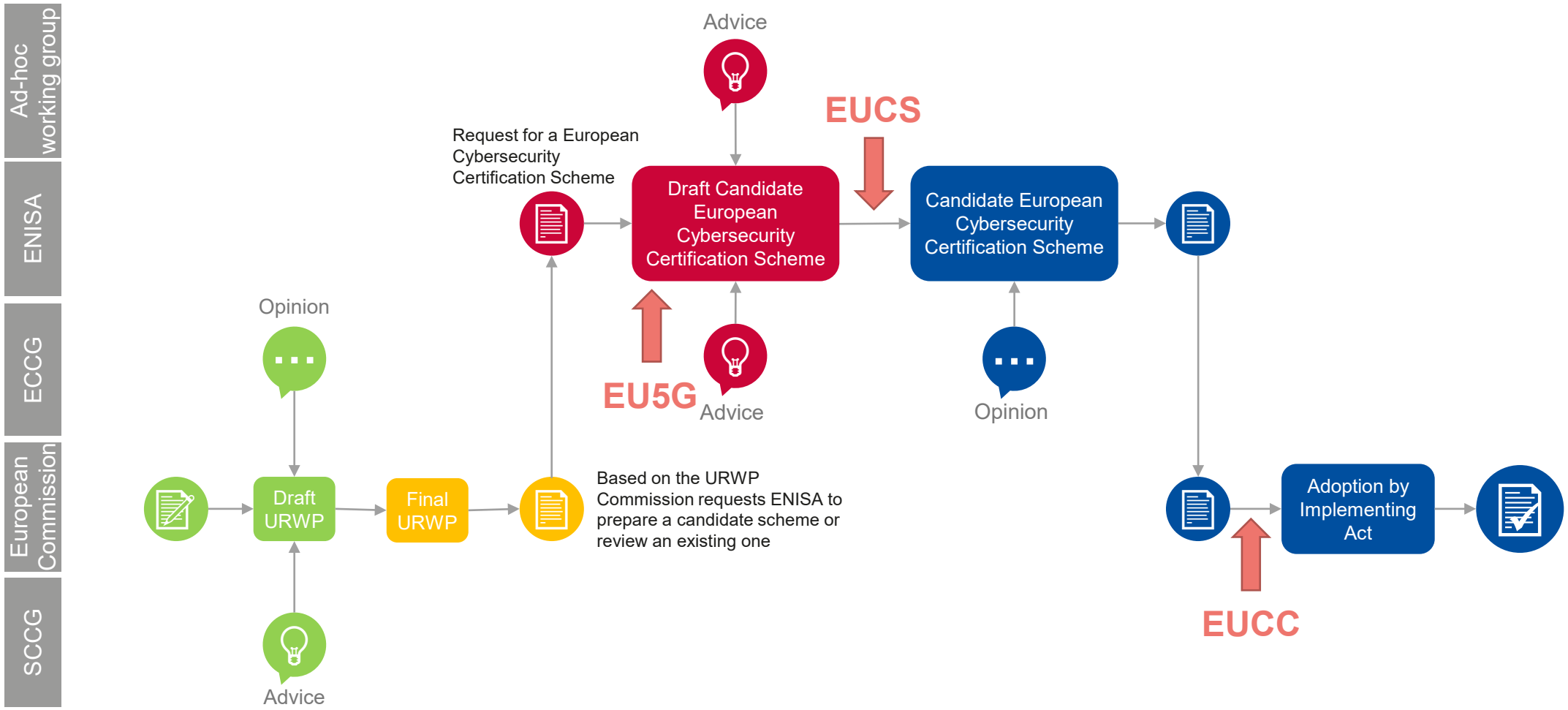
WHAT IS IN A CYBERSECURITY SCHEME?

a) Subject matter and scope
b) Clear description of the purpose of the scheme and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme
c) References to the international, European or national standards applied in the evaluation, and if not available to technical specifications
d) One or more assurance levels
e) An indication whether conformity self-assessment is authorized
f) Specific requirements for the CABs
g) Specific evaluation criteria and methods to be used
h) The information necessary for the evaluation or otherwise to be made available by the applicant
i) If applicable, conditions of use of marks and labels
j) Rules for monitoring compliance of certified and self-assessed products
k) Conditions for issuing, maintaining, continuing certificates, and for extending/reducing scope
l) Rules concerning the consequences for products that have been certified or self-assessed and do not comply
m) Rules concerning how previously undetected vulnerabilities should be reported and handled
n) Rules concerning the retention of records by CABs
o) Identification of national and international schemes with the same scope
p) Content and format of the certificates and EU statements of conformity
q) The period of the availability of EU statements of conformity and related documentation
r) Maximum period of validity of certificates
s) Disclosure policy for certificate issuance, withdrawal, amendment
t) Conditions for mutual recognition with third countries
u) Where applicable, rules for peer assessment
v) Formats and procedures to be followed by suppliers to provide supplementary cybersecurity information

EUCS SCHEME PREPARATION PROCESS



EUCS SCHEME PREPARATION STATUS



CHAPTER 2

THE EUCC FOR PRODUCTS

WHAT IS COMMON CRITERIA?

The ISO/IEC 15408 series of standards defines Evaluation Criteria for IT Security, known as Common Criteria.

This set of standards is widely used for the certification of sensitive IT products

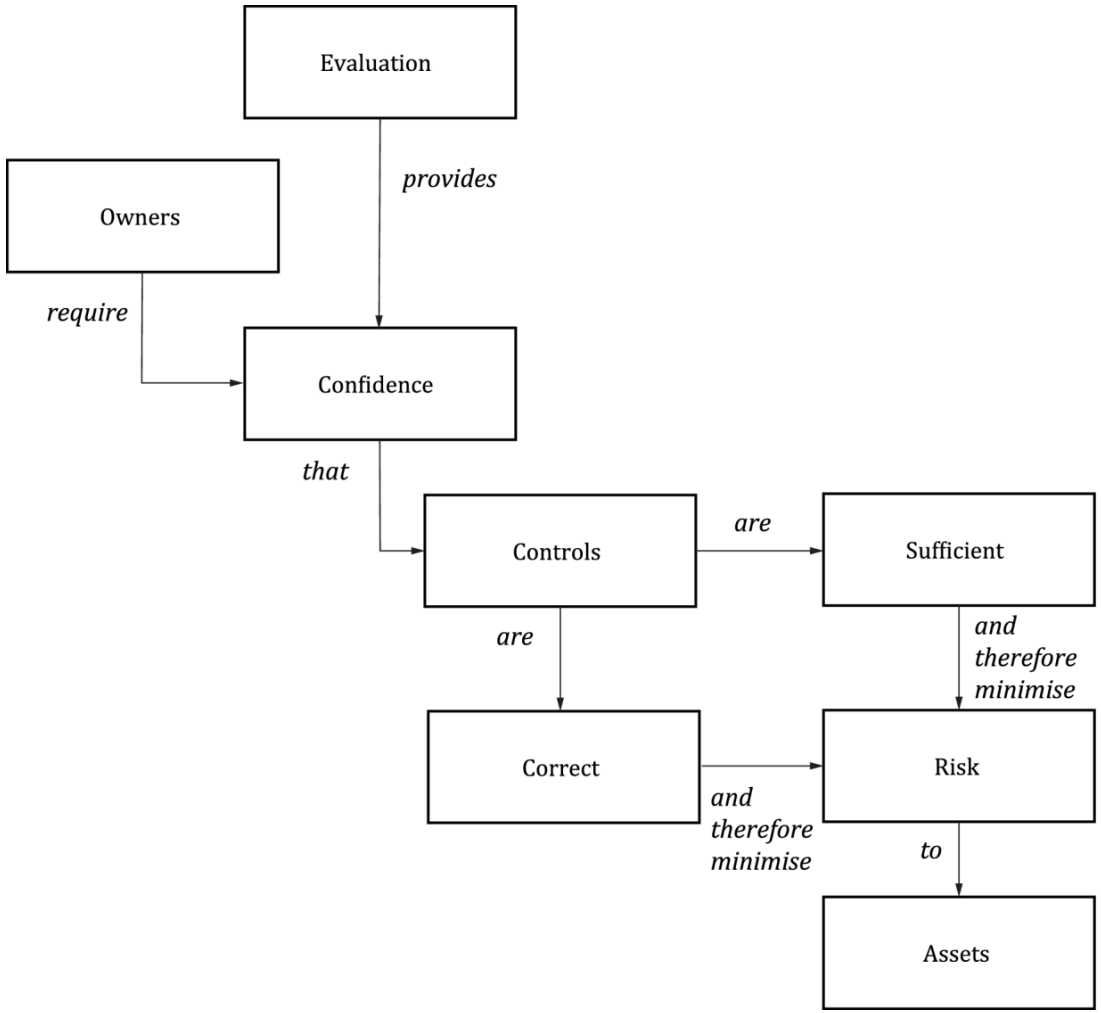
- Very widely used for smart cards and secure elements, and also for HSMs and other crypto boxes
- Also used for smart meters, digital tachographs, network equipment

Together with ISO18045, these standards define a full framework

- A general model for the security of products
- Two sets of security requirements (functional and assurance)
- A methodology for verifying that a product meets requirements
- A framework for certifying complex products (composition, profiles)

Also, these standards are publicly available: https://www.commoncriteriaportal.org/cc/

EVALUATION CONCEPTS AND RELATIONSHIPS IN CC



From CC:2022 Part 1: Introduction and general model, CCMB-2022-11-001

Common Criteria focuses on evaluation activities, not on certification

The EUCC scheme defines how to get and maintain certification based on CC principles

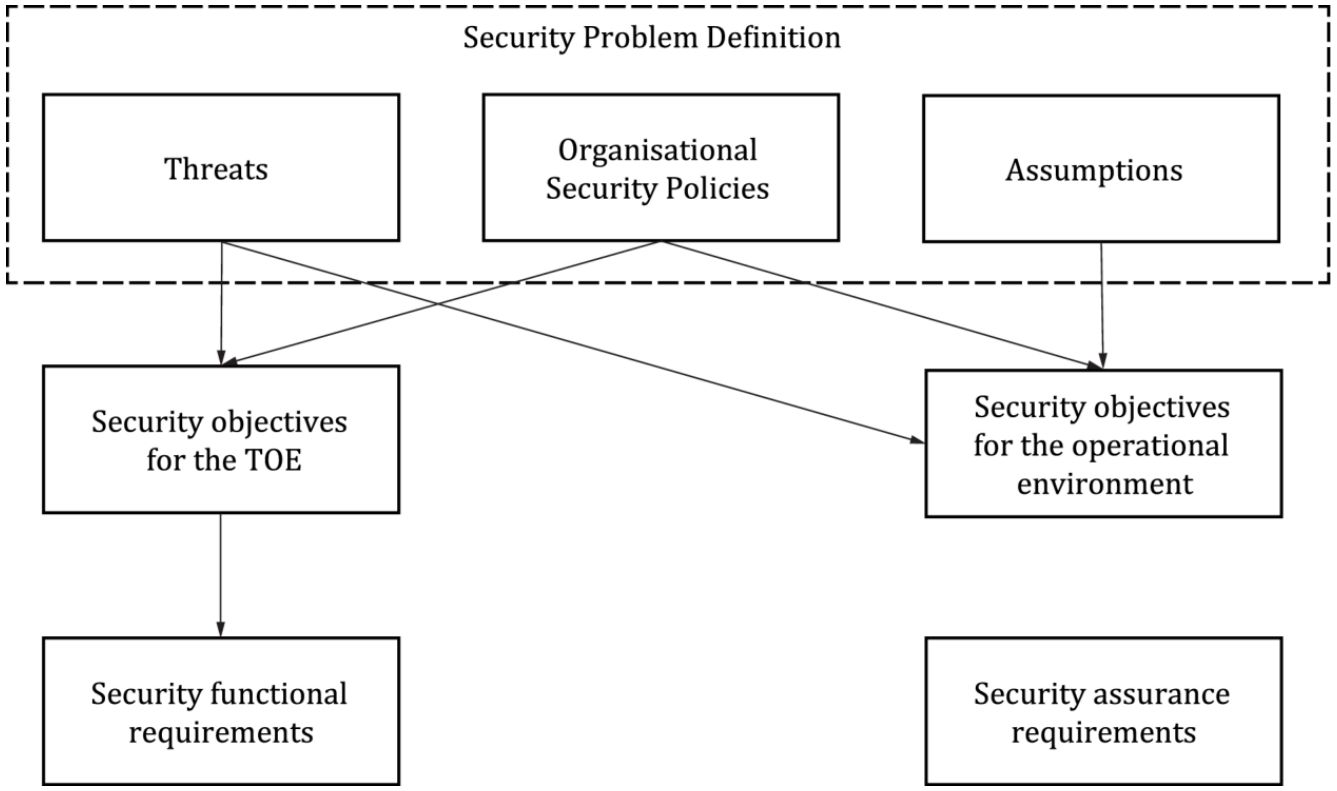
There are two distinct roles in EUCC

- Certification bodies (CBs), which issue certificates
- Evaluation labs (ITSEFs), which apply the evaluation principles on the products

CBs authorize ITSEFs and monitor their work on a daily basis

- Historically, CBs have been government bodies
- In EUCC, they may be private bodies at assurance level ‘substantial’

TARGET OF EVALUATION AND SECURITY TARGET



The security characteristics of a product are defined in a ST

A ST corresponds to a security problem

- It defines a Target of Evaluation (ToE)
- Not necessarily an interesting problem

From the security problem, the vendor derives in the Security Target

- A set of SFRs that satisfy the objectives
- A set of security functions satisfying the SFRs
- Rationales to link all the components
- A list of security assurance requirements

EUCC: AN HORIZONTAL ICT PRODUCTS SCHEME

Based on international standards

Common Criteria & CEM:
ISO/IEC 15408 & 18045

Accreditation standards:
ISO/IEC 17065 & 17025

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 REQUIREMENTS FOR VENDORS

EUCC adds practical details to CC, continuing on the existing SOG-IS scheme, and introducing aspects of the Cybersecurity Act.

Some requirements apply to the product's Security Target

- Ensuring that the security objectives from Article 51 are all met (including the less usual ones)
- Including specific assurance requirements from AVA_VAN (pen testing), ATE_IND (functional testing) and ALC_FLR (flaw remediation, for updates)

Provide specific information, as required by Article 55

- 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 FOR VENDORS

Some of the requirements are commitments for cybersecurity, to be endorsed by top management.

The applicant for certification shall undertake commitments

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

EUCC CERTIFICATES

EUCC certificates have a lifecycle, and many events may happen after issuance.

The maximum validity for EUCC certificates is 5 years (but it may be less).

There are many monitoring activities on issued certificates:

- NCCAs will review in detail a sample of certificates every year
- NCCAs will also monitor CABs to ensure that they do their job properly
- All stakeholders will monitor vulnerabilities and threat landscape, and keep each other updated

Many things may happen to a certificate

- It may be suspended for a while when a vulnerability is identified and needs to be fixed
- It may be revoked if the vendor violates one of their commitments or if the product's security is compromised
- It may also be renewed if the vendor demonstrates continued compliance (through another evaluation)
- By default, it will simply expire at some point

WORK IN PROGRESS

The EUCC scheme is about ready, and it inherits from another scheme, SOG-IS, which has been active for many years in Europe.

The scheme still needs to become an adopted Implementing Act

- There is a draft available at the Commission, which first needs to go through Inter-Service Consultation
- Then, Member States need to adopt it in a Committee with a qualified majority
  - 50% supporting (*i.e.*, at least 14 MS), representing at least 2/3 of EU population

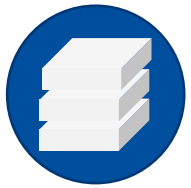
In parallel, everything needs to be ready for the scheme to function

- Catalogue of national supporting documents that could become mandatory
- Harmonised evaluation procedures for cryptography
- Development of ENISA's certification Web site
- Development of a maintenance strategy and organisation

CHAPTER 3

THE EUCS FOR CLOUD SERVICES

EUROPEAN CLOUD SERVICES SCHEME (EUCS): A GENERIC SCHEME



All capabilities

Also based on ISO/IEC 22123-1

All cloud capabilities are supported: Infrastructure, Platform, Application

Covers the full stack

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 evaluation levels

Mapped to assurance levels as defined in the European Cybersecurity Act

‘basic’

‘substantial’

‘high’

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

EUCS TECHNICAL CHALLENGES

Which requirements?

There is no clear standard, so we need to define a list of controls, drawing from existing schemes, and adding the notion of assurance levels

Which assessment?

Several assessment methods, mostly based on ISO270xx and on ISAE standards, and an ability to combine with both assessments

Which assurance levels?

Assurance levels must bring added value and be simple enough to understand in order to bring a clear message

How to make results matter for customers?

A key objective of the scheme is to allow customers to make informed choices, and this is about available documentation

CHAPTER 3

STANDARDIZATION FOR THE EUCS

SCHEME DETAILS

REQUIREMENTS

One of the essential parts of a certification is the set of requirements to which certified cloud services need to conform to: The “what”

This work started in the EUCS ad hoc working group, and it has been turned over to CEN-CENELEC’s JTC13 WG2 for standardisation

A FIXED SET OF REQUIREMENTS

Ongoing work in JTC13 WG2

The requirements on controls are defined for every evaluation level, with increasing details and constraints.

For **CS-Basic**, requirements are defined by removing constraints from the requirements of higher levels

- Focus is mainly on the policies and procedures

For **CS-Substantial**, requirements are comparable to typical frameworks

- Mostly inspired from C5 (Germany), itself drawing from ISO 270xx, and more
- All requirements are considered applicable, but may be conditional
- No Security Target, the requirements are a baseline

For **CS-High**, requirements are more demanding than for usual frameworks

- Some requirements inspired from SecNumCloud, especially for more specific/detailed requirements
- Many requirements about automated monitoring, an important theme for CS-High
- Also, much stronger requirements on penetration testing

SCHEME DETAILS

ASSESSMENT

The second essential part of a certification scheme is the assessment method that it used to determine whether or not a cloud service conforms to the scheme requirements: The “how”

This part has also partly been handed over to CEN-CENELEC’s JTC13 WG3, in the form of requirements for accreditation of CABs

TWO ASSESSMENT METHODS

Ongoing work in JTC13 WG3

Limited assurance

For the Basic level only, as initially proposed by CSP-CERT:

- Mostly a review of evidence provided by the CSP
- In fact, a self-assessment reviewed by a 3rd party
- Fully integrated in the main scheme, certificate lifecycle, maintenance, *etc*.
- Mostly for vendors with no certification

Reasonable assurance

For the Substantial and High levels:

- "Normal" audit of a cloud service
- Focus on the ISMS and processes, but some interest in the "product" underlying the service
- Following a specific methodology, fully defined in the scheme
  - Compatible with both ISO17021 and ISAE3402
- Vendors can keep their certification strategy

ACCREDITATION IN EU SCHEMES

Certificated are by definition issued by third parties. These third-parties need to be accredited before to be allowed to operate (and also authorized and notified).

Accreditation is a classical process, performed by National Accreditation Bodies

- Typically specific to a particular type of certification
- Verifying competencies, processes, organization (including independence), IT systems, *etc*.

In the EU Cybersecurity Act, there are specific conditions

- The CABs are subject to a specific set of requirements, very strong on independence
- The CABs may be subject to authorization by the NCCA to validate some competencies
- Each NCCA needs to notify the CABs operating in the country to the Commission

CHAPTER 4

EU5G FOR 5G EQUIPMENT

5G EQUIPMENT

This is the first vertical scheme, as certification is one of the tools defined in the European 5G Toolbox for Cybersecurity.

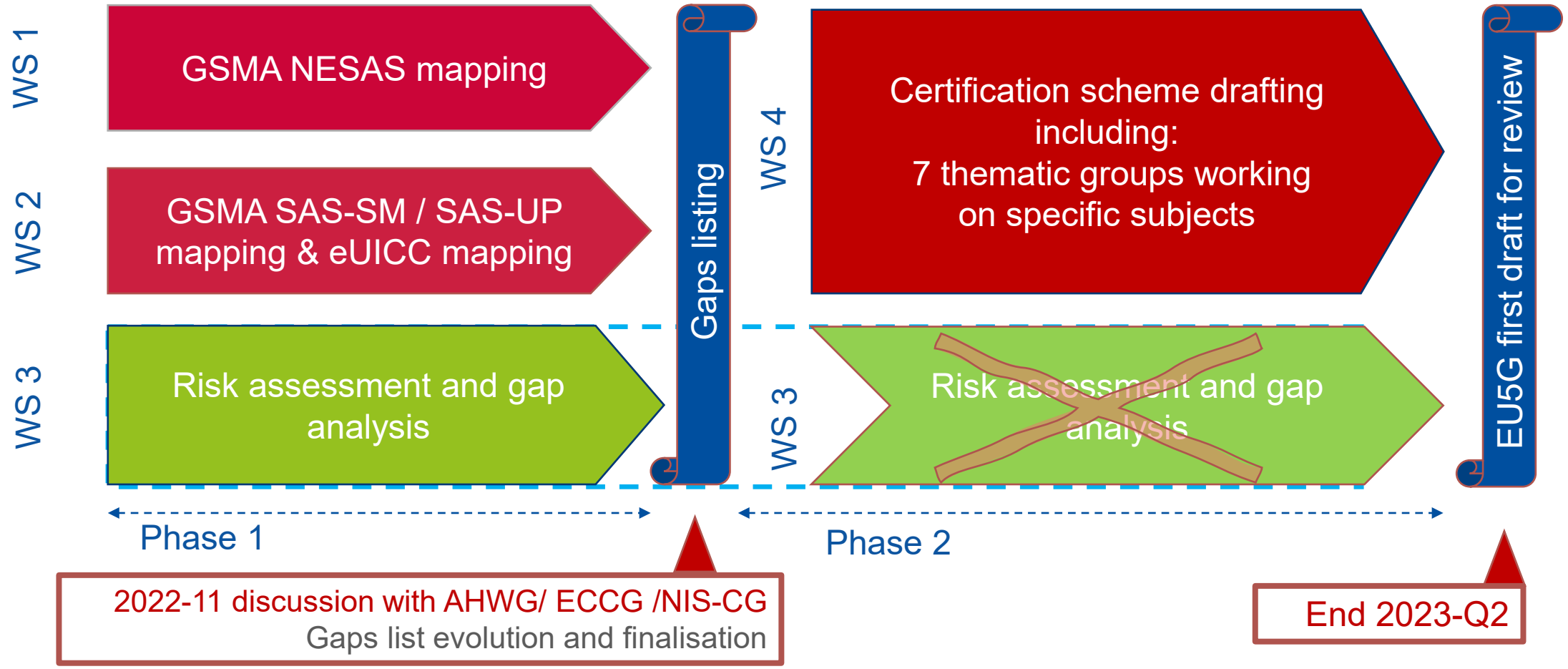
Inspired from GSMA's existing schemes

- NESAS, targeting network equipment
- eUICC, targeting embedded SIM components, and based on EUCC
- SAS-UP and SAS-SM, targeting the eUICC production and subscription management processes

Starting from existing schemes, like EUCC, but with a less established private scheme

- The Cybersecurity Act needs to be considered, so updates are required everywhere
- The scheme needs to handle the certification of processes

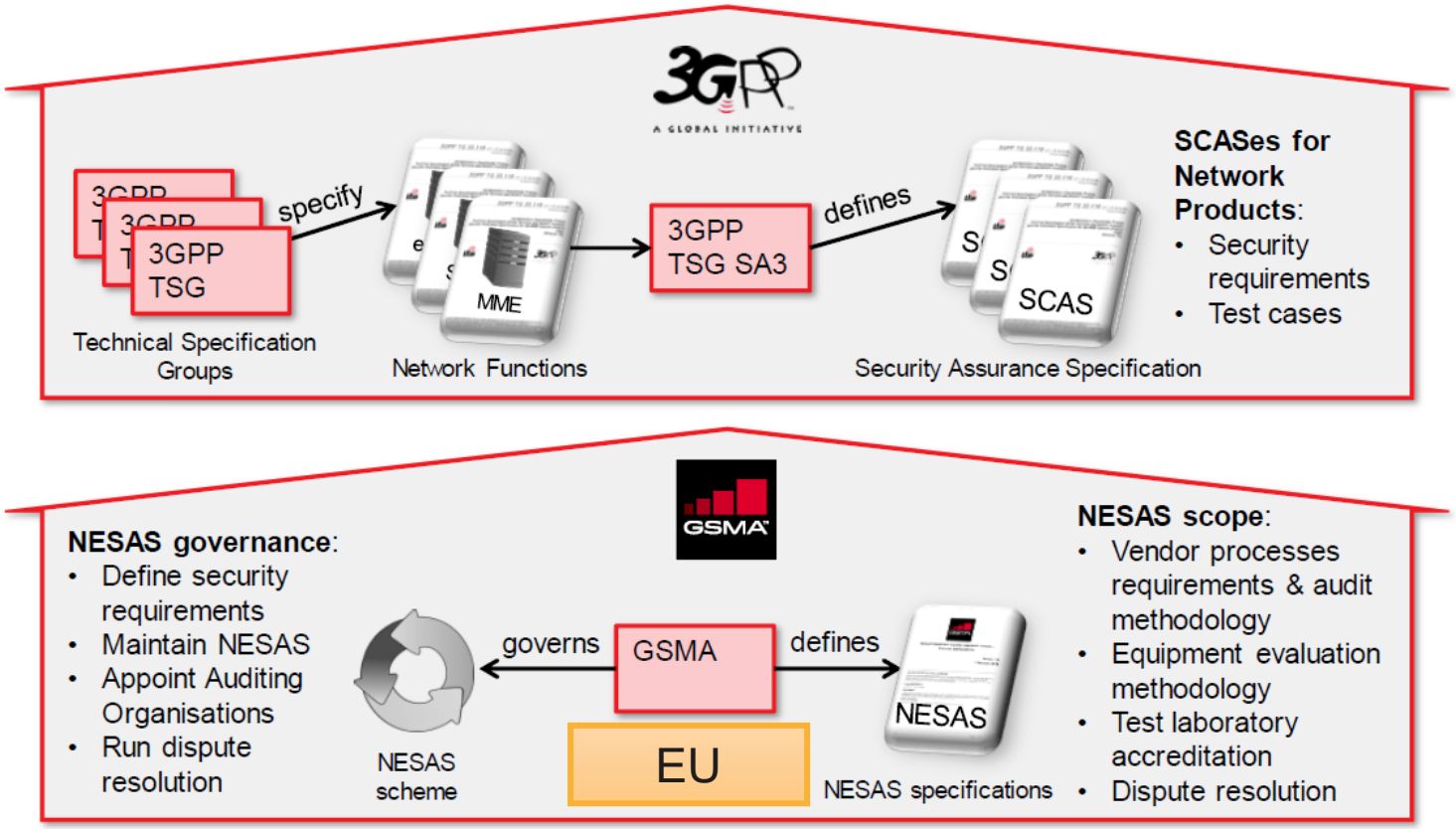
EU 5G TIMELINE OF DRAFTING



CHAPTER 5

STANDARDIZATION AROUND EU5G

CURRENT FRAMEWORK FOR NESAS



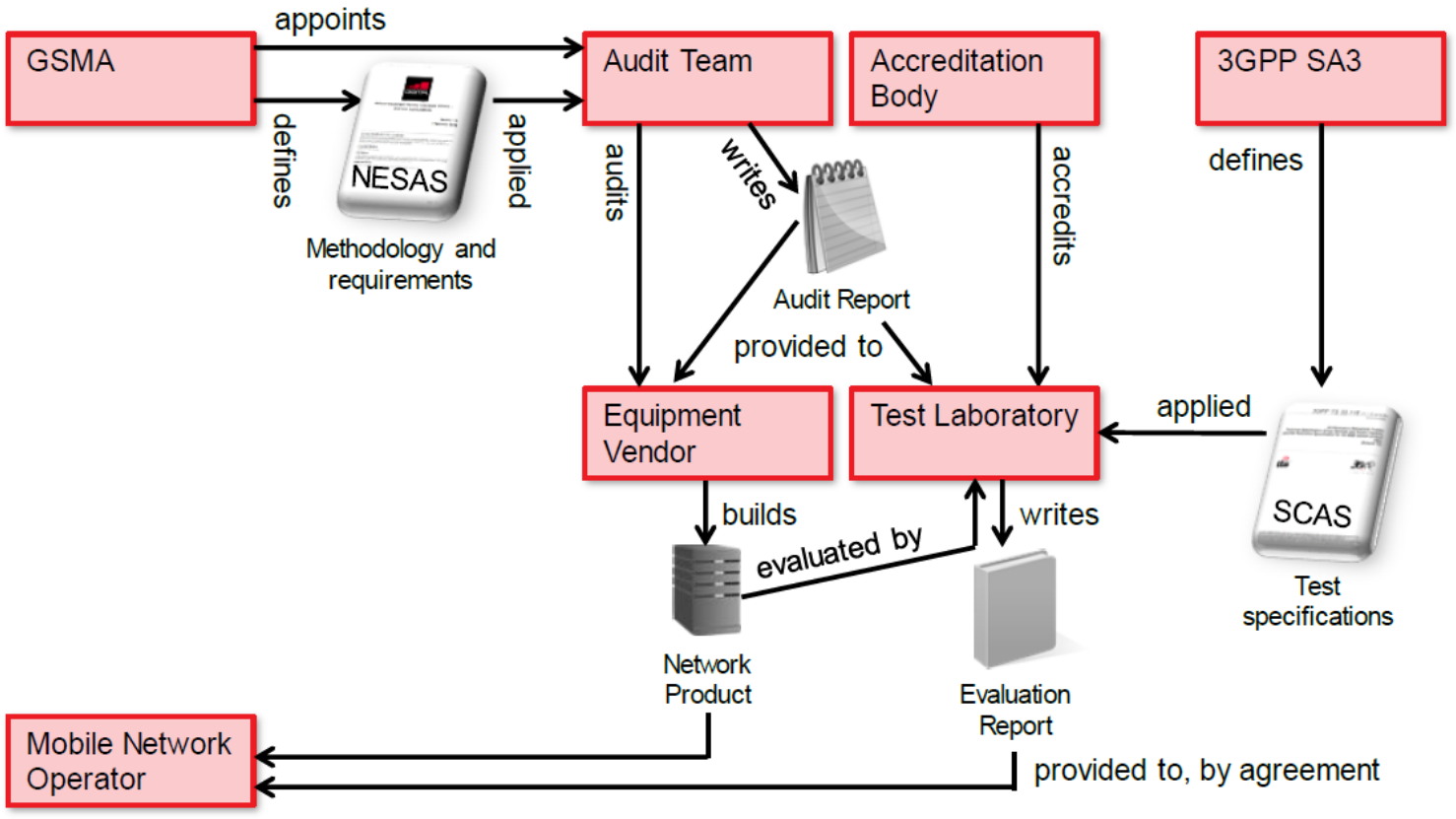
The framework will need to evolve slightly.

The vertical requirements will stay with 3GPP/ETSI.

The governance and assessment methods will have at least to be adapted to the Cybersecurity Act.

Relationship with GSMA still to be redefined.

CURRENT PROCESS FOR NESAS



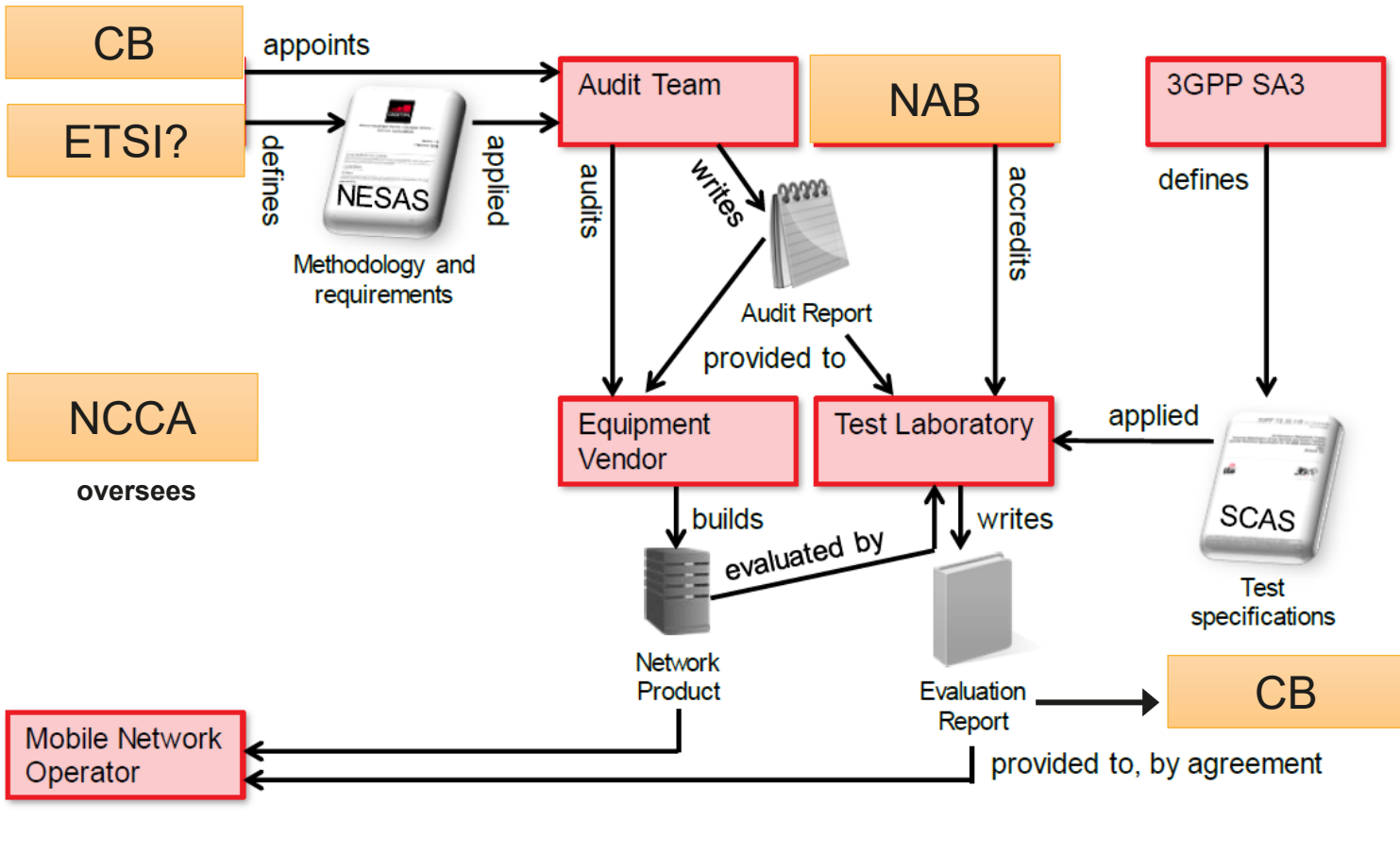
The process will need to evolve significantly.

First, a certificate will need to be issued.

Accreditation will be taken over by the National Accreditation Bodies.

Relationship with GSMA still to be redefined, with governance shifting to the EU.

UPDATED PROCESS FOR NESAS



The process will need to evolve significantly.

First, a certificate will need to be issued.

Accreditation will be taken over by the National Accreditation Bodies.

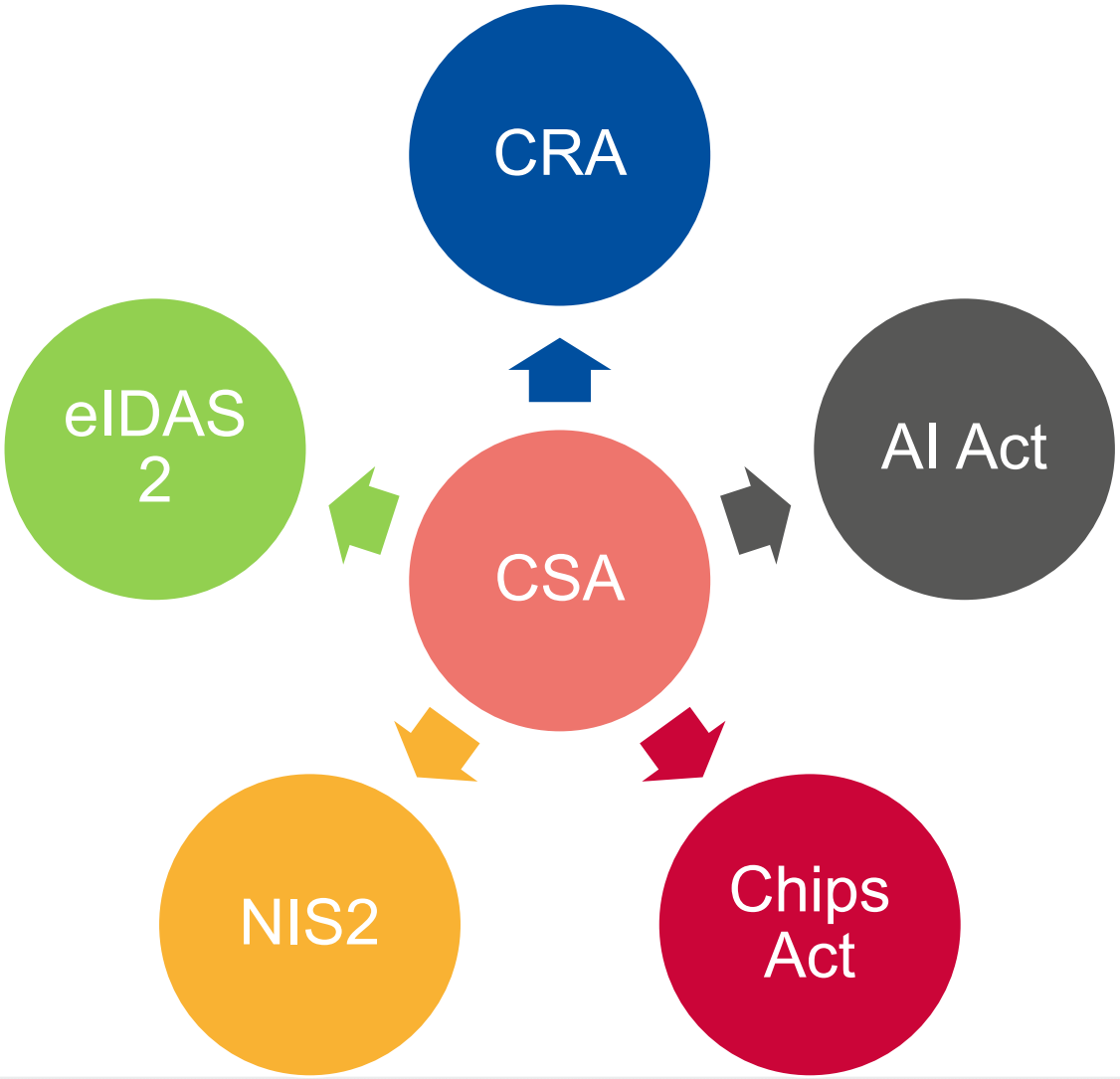
Relationship with GSMA still to be redefined, with governance shifting to the EU.

CHAPTER 6

BEYOND EXISTING SCHEMES

STRATEGIC VIEWS ON SCHEME DEVELOPMENT

Cybersecurity Certification referenced in the different EU Laws



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