EUROPEAN UNION AGENCY
FOR CYBERSECURITY

HOW WILL EUROPE CERTIFY INNOVATIVE CRYPTO SYSTEMS?

Eric Vetillard, Ph.D.
Lead Certification Expert, MCS, ENISA
Chair, EUCS AHWG and EUDIW AHWG

21 | 05 | 2025

THE FUTURE CRYPTOGRAPHY CONFERENCE

THE ISSUE OF TRUST

The relationship between certification and trust is more complex than expected.

Trust is a relationship, not a property of an entity:

trust relationship between two entities or elements, consisting of a set of activities and a security policy in which element x trusts element y if and only if x has confidence that y will behave in a well-defined way (with respect to the activities) that does not violate the given security policy
[ISO 27036-1:2021, 3.12

Trust is about the confidence that x places in y

- Cryptography can go a long way about establishing trust about some aspects
- A certification can improve the level of confidence, but confidence is a belief, which cannot be created
- It is perfectly normal not to trust an entity, even in the presence of certificates. This happens every day in our relationship with companies and suppliers.

ASSURANCE AND CERTIFICATION

The concept of assurance is essential but never really defined.

Here is an attempt from mixing Common Criteria and ISAE

assurance grounds for justified confidence that a product, service or process meets specified requirements

Assurance cannot be quantified, and it's often very hard to compare, so how to define levels?

- Common Criteria and EUCC have two (related) scales
  - Evaluation Assurance Levels (EAL), from EAL1 to EAL7 ➔ Evaluation activities (generic)
  - Vulnerability assessment levels (AVA_VAN), from AVA_VAN.1 to AVA_VAN.5) ➔ Resistance to attacks (specific)
- Audit defines two levels of assurance, also reused in the EUCS

  limited assurance negative attestation that the attester is unaware of any significant issues

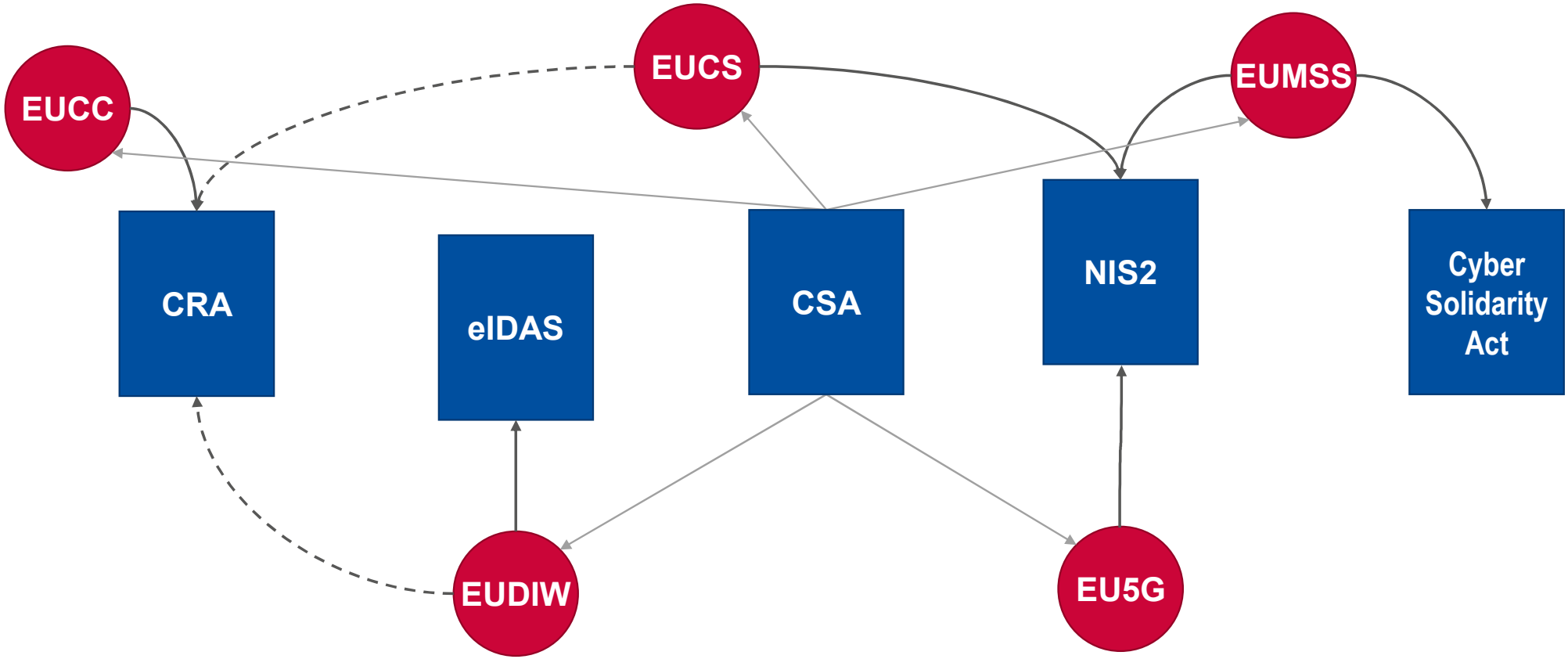
  reasonable assurance affirmative attestation that all information is fairly stated

There is very little in common between these two concepts, but both are essential
Robustness testing is essential for algorithms/products, audit for their operation

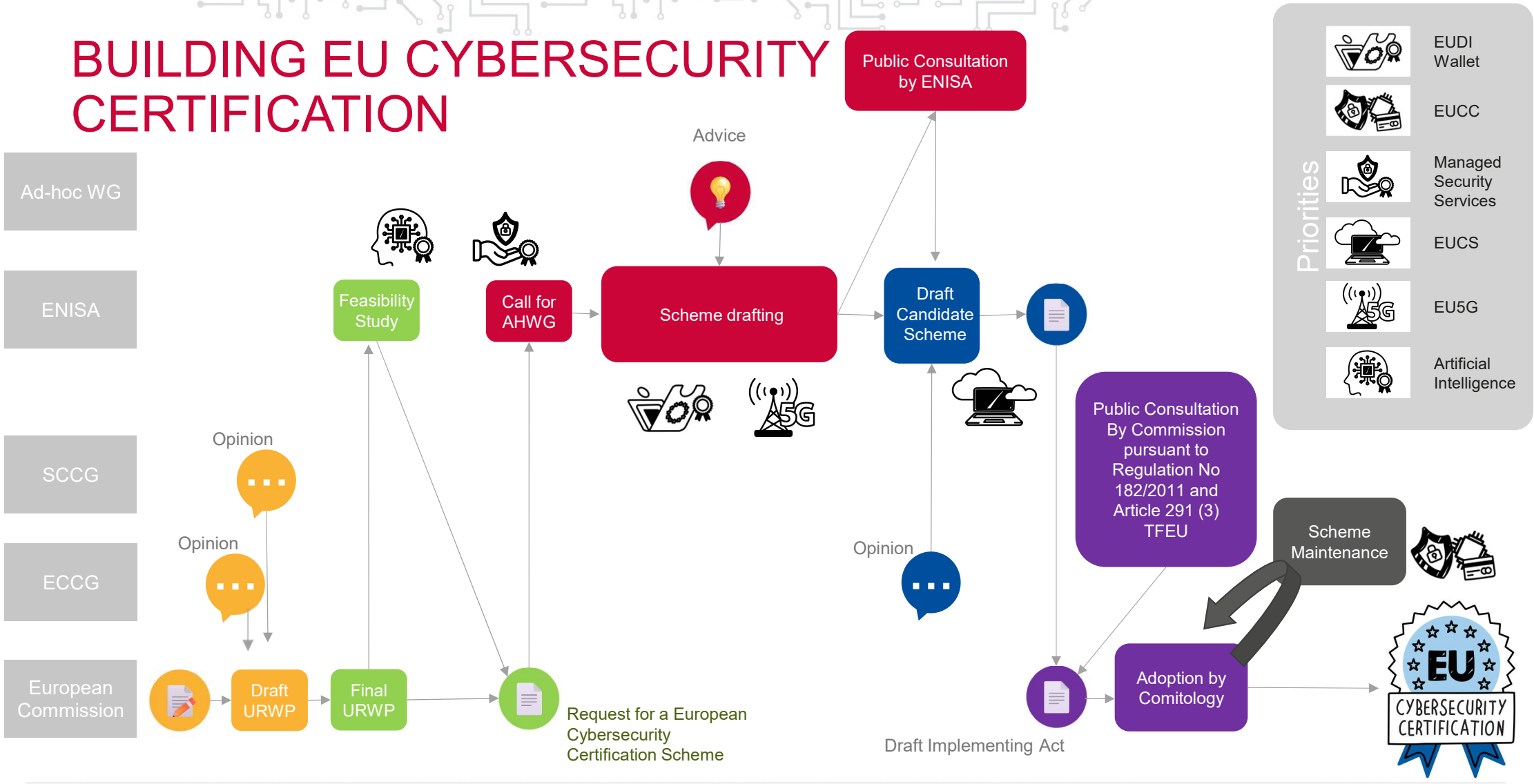
PART 1

STATUS OF EUROPEAN CYBERSECURITY CERTIFICATION

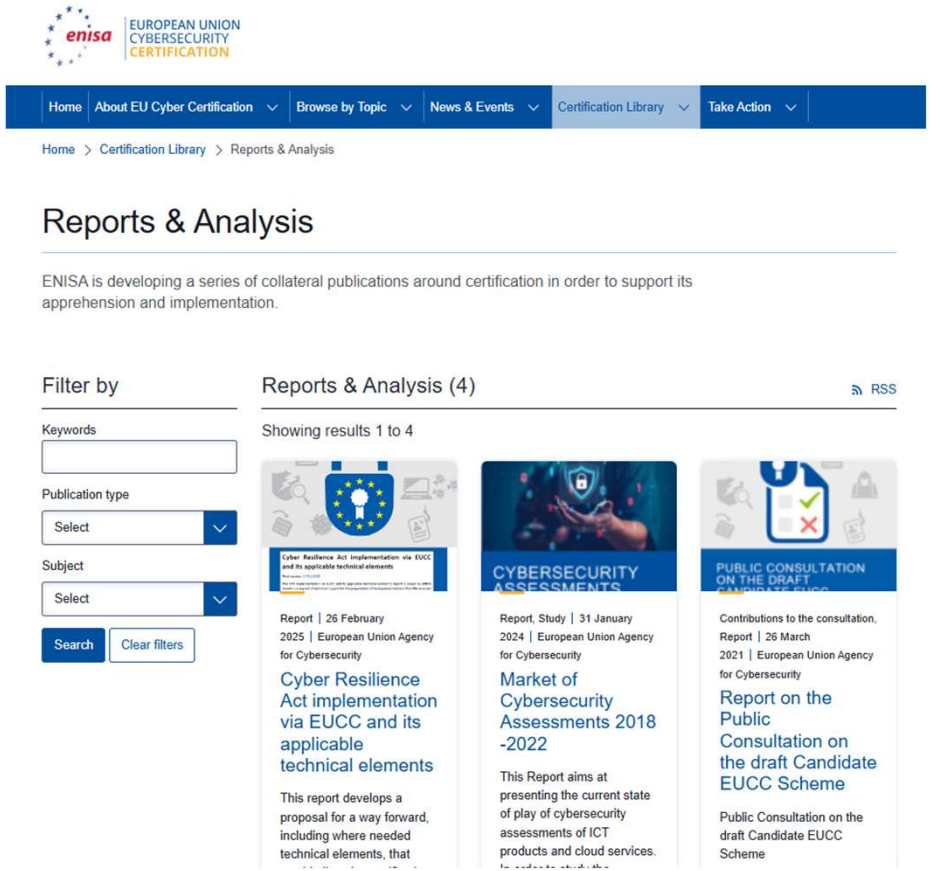
A STRONG LINK TO EU REGULATION



BUILDING EU CYBERSECURITY CERTIFICATION



EU CYBER RESILIENCE ACT (CRA) & CERTIFICATION



Deadlines

- 27/02/2024 – EUCC Entry into force.
- 11/12/2024 – CRA Entry into force. (20 days)
- 27/02/2025 – EUCC into application.
- 11/09/2026 – Notification provisions to the CSIRT and ENISA. (21 Month)

- 11/12/2027 – CRA Application (36 Months).
- 31/12/2027 – ST Conformant to CC:2022 on PP CC v3.1

A SMALL NOTE ON CRYPTOGRAPHY AND CRA

There is only one direct mention of cryptography in CRA.

It is in the list of critical products with digital elements, though:

2. Smart meter gateways within smart metering systems as defined in Article 2, point (23) of Directive (EU) 2019/944 of the European Parliament and of the Council (1) and **other devices for advanced security purposes, including for secure cryptoprocessing**

But there are many mentions of important products that rely heavily on cryptography, including:

1. Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers

9. Public key infrastructure and digital certificate issuance software

There are also several mentions of microprocessors and microcontrollers, most of which embed basic cryptographic capabilities.

EUDI WALLET - THE WORK WAS KICKED OFF IN JANUARY

25 Experts, some support

The AHWG includes 25 experts

- Many CABs, some implementers and consultants
- From different Member States

Some EUIs are also represented

- The Commission is represented, as well as EA
- Also observers from ECB and Frontex

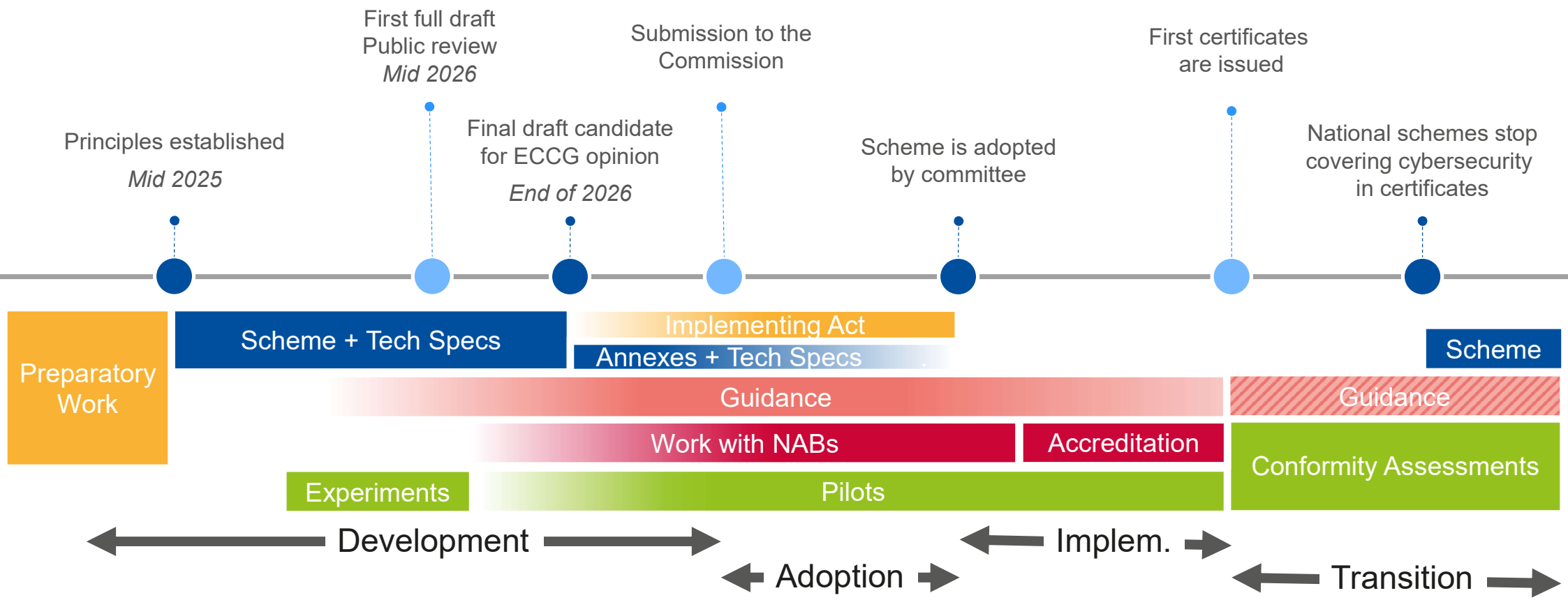
22 Member States registered

This is a higher representation than in any other certification AHWG in the past

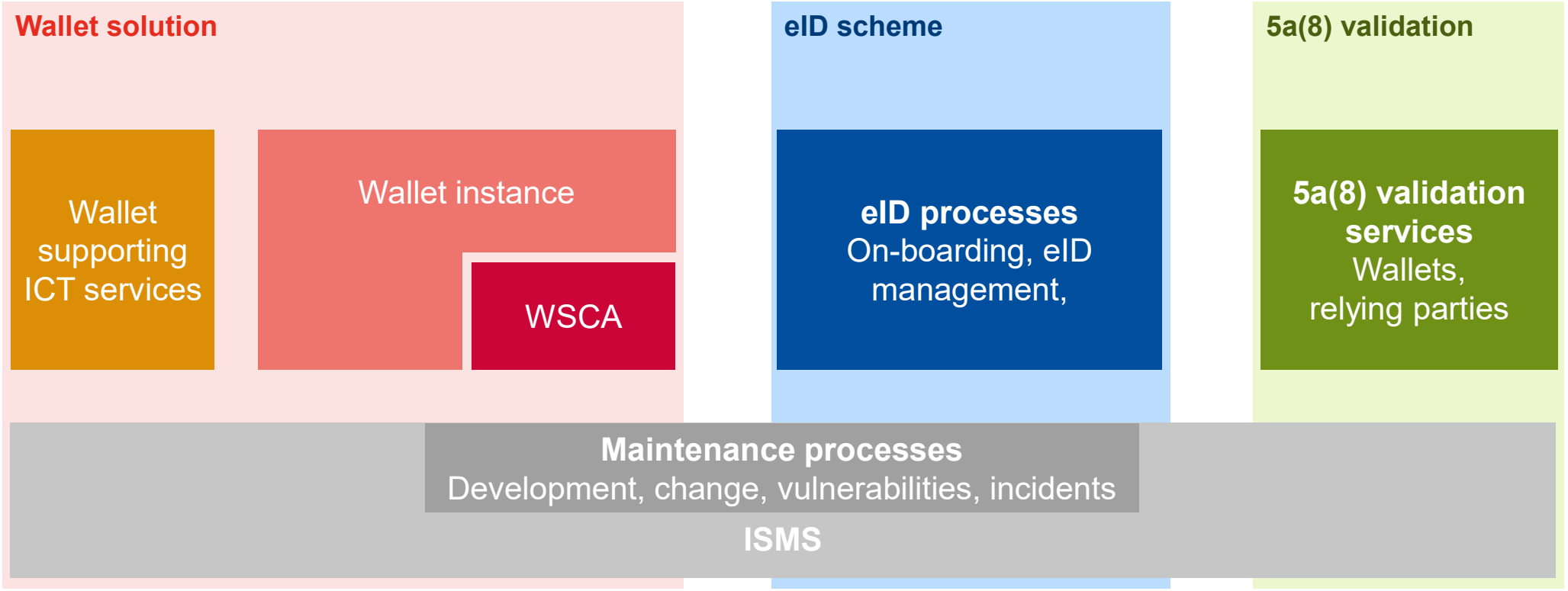
MS are officially observers, but active participation is very welcome

- For some questions, you have the answers, for instance on actual Wallet implementations

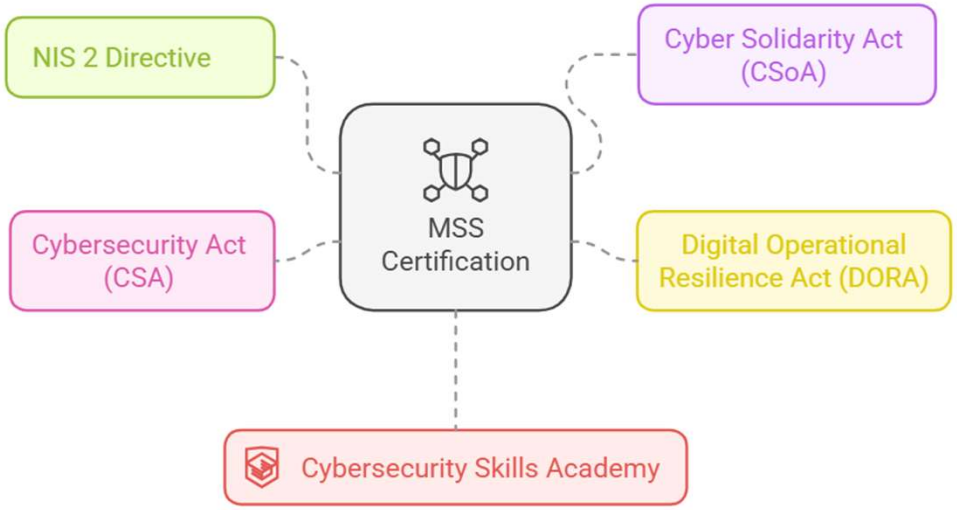
EUDI WALLET - PROCESS OVERVIEW



EUDI WALLET - ARCHITECTURE



MANAGED SECURITY SERVICES – STARTING



We started by a pre-study

- **Understand the state of play**
  - Mapping the EU legislative panorama
  - Deciphering the market
  - Identifying key standards
  - Recognising existing MS schemes
- **Bring awareness on the topic**
- **Build Knowledge amongst stakeholders**

Next Steps
Constitution of an Ad Hoc Working Group
Kickoff

PART 2

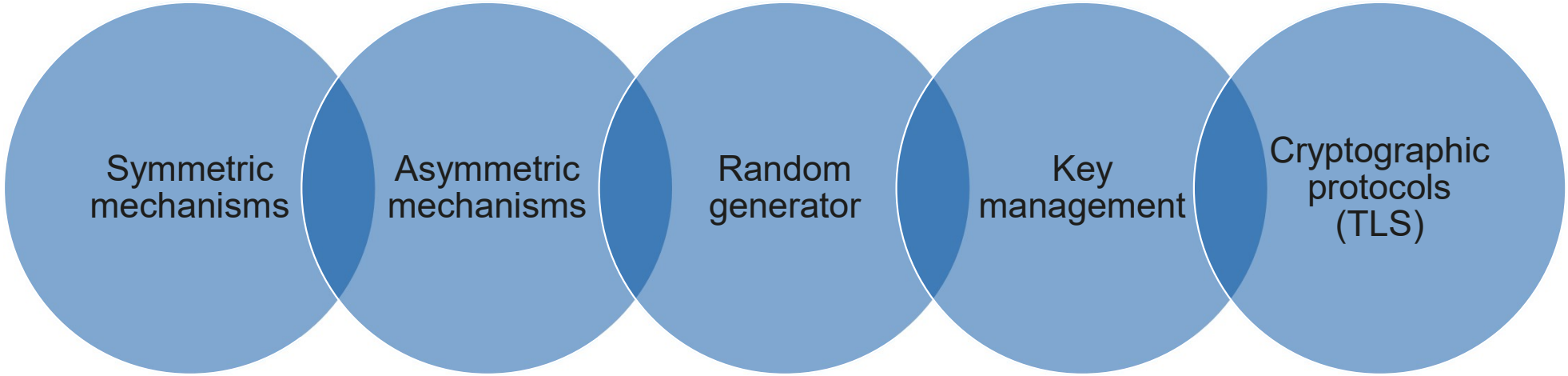
CRYPTOGRAPHY AND EUCC

AGREED CRYPTOGRAPHIC MECHANISMS

Document developed by SOG-IS crypto group – v1.3 in SOG-IS

The version 2.0 has been adopted under EUCC as guidance document on May 6th:
https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en

"White" list of agreed algorithms including recommendations and warnings



AGREED CRYPTOGRAPHIC MECHANISMS V2.0

The main add-on of ACM v2.0 is to cover the Post-Quantum threat:

- Approved PQC schemes are now part of the agreed mechanisms
- Hybridization is key: Pair post-quantum and classical schemes such that if one breaks, the security remains
- Symmetric & hash parameters upgraded: Use ≥192-bit keys and ≥384-bit hash outputs in quantum-sensitive contexts

AGREED CRYPTOGRAPHIC MECHANISMS V2.0

ACM v2.0 includes the following new constructions.

For Digital Signature:

- ML-DSA – FIPS204
- SLH-DSA – FIPS205
- XMSS
- LMS

For Key Establishment:

- ML-KEM – FIPS203
- FRODO-KEM

AGREED CRYPTOGRAPHIC MECHANISMS V2.0

Has a guidelines status for EUCC and certification:

"When deciding which cryptographic mechanisms should cover their need for cryptographic protection, e.g.:

confidentiality, integrity, data origin authentication, and authentication, in their protection profiles and ICT products submitted to EUCC certification, developers of protection profiles and developers of ICT products should consider using the agreed cryptographic mechanisms as defined in ECCG Agreed Cryptographic Mechanisms version 2, further referred to as ACM v2, available at EUCC Certification Scheme - EU Cybersecurity Certification When evaluating protection profiles and ICT products under the EUCC scheme, evaluators should verify that these protection profiles and ICT products preferably rely on agreed cryptographic mechanisms as defined in ACM v2 to provide the security services evaluated under this scheme."

Is also referred to in the EU PQC roadmap

HOW TO STAY TUNED?

ENISA dedicated website:

https://certification.enisa.europa.eu/

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

certification.enisa.europa.eu