Welcome

Bienvenue

Willkommen

ILNAS

Cybersécurité et Accréditation

06/10/2023, Ministère de L'Environnement, du Climat et du Développement Durable

JFG ou AW
Titre – *Département Confiance Numérique*, ILNAS

ILNAS' role in Digital Trust

What ILNAS does

ILNAS DIGITAL TRUST

MISSIONS IN GENERAL

Directly in the Luxembourg market

- Monitor the activities and compliance of Trust Service Providers in the context of the eIDAS Regulation
- Maintain of the Luxembourgish Trusted List

- Monitor the activities and compliance of *Perstataires de Services de Dématérialisation et de Conservation* in the context of the Luxembourg e-archiving framework

- New: National Cybersecurity Certification Authority (NCCA) – Supervision in the context of the CSA (topic of this presentation)

ACTIVITIES AND CONTACTS

Contact info

- Alain WAHL (Head of the Digital Trust department)
- Michèle FELTZ (Trust Services)
- Michel LUDWIG (e-archiving)
- Department email confiance-numerique@ilnas.etat.lu
- Department phone (+352) 247 743 50
- https://portail-qualite.public.lu/fr/cybersecurity-act.html

ILNAS' role in Digital Trust

What ILNAS does

ILNAS DIGITAL TRUST

MISSIONS IN THE CSA

Directly in the Luxembourg market

- Monitor that schemes' rules are being respected by products, processes, and services that are certified or the subject of a conformity self-assessment
- Cooperate with other market surveillance authorities
- Collaborate actively with OLAS to monitor CAB activity and if needed give authorizations

Within CSA governance

- Participate in the ECCG
- Collaborate with the Commission and other NCCAs in sharing knowledge and for continuous improvement of schemes

ACTIVITIES AND CONTACTS

Why we're here today ☺

Ongoing

- Updating the DTD documentation to accommodate supervision requests
- Collaborating with OLAS to:
  - cooperate efficiently in CAB supervision
  - Support in the establishment of the accreditation program related to the CSA

Contact info

- Alain WAHL (Head of the Digital Trust department)
- Jean-François GILLET and Jean LANCRENON
- CSA-matters email supervision-cybersecurite@ilnas.etat.lu
- Department phone (+352) 247 743 50
- https://portail-qualite.public.lu/fr/cybersecurity-act.html

The Cybersecurity Act

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

Here

Adopted on 17 April 2019

Fully entered into force on 28 June 2021

Two major parts

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

EU-wide cybersecurity certification framework

Main objectives: Increase cybersecurity in the Union and support the digital single market

The Cybersecurity Act

ENISA

Status, governance, structure

ENISA's mandate as the European cybersecurity agency is made permanent

Chapters 3 to 6 give its broad organization

Scope, objectives

Cybersecurity

Knowledge center

Support to Member States, the Union

Research

Capacity building, education

Improving the EU's general cybersecurity level

Specific tasks in the CSA

Article 8 Market, cybersecurity certification, and standardization

Article 20(4) on ad hoc working groups

Article 22 Stakeholder Cybersecurity Certification Group (SCCG)

Visit ENISA (online) here.

The Cybersecurity Act

The certification framework: Summary

Schemes cover the security of ICT products, services, or processes

A neat feature for 'basic': the ability to produce conformity self-assessments that are also recognized EU-wide

Certificates issued in any Member State are recognized EU-wide

Three built-in levels of assurance: 'basic', 'substantial', and 'high'

As much as possible, built on international standards

Creation of an EU-wide governance framework for certificate issuance and compliance monitoring

Attribution of the task of drafting certification schemes

Requirements for certification schemes

Certification framework

The Cybersecurity Act

The certification framework: Overall governance

Union level

- Commission prepares topics (Union Rolling Work Program) supported by SCCG
- ENISA drafts schemes
- Commission approves and launches schemes with implementing acts
- ECCG (European Cybersecurity Certification Group) issues opinions on schemes

National Level

E.g.:

- Each MS appoints at least one NCCA to supervise and/or certify
- National Accreditation Bodies accredit the CABs
- CABs are welcome to be private sector entities

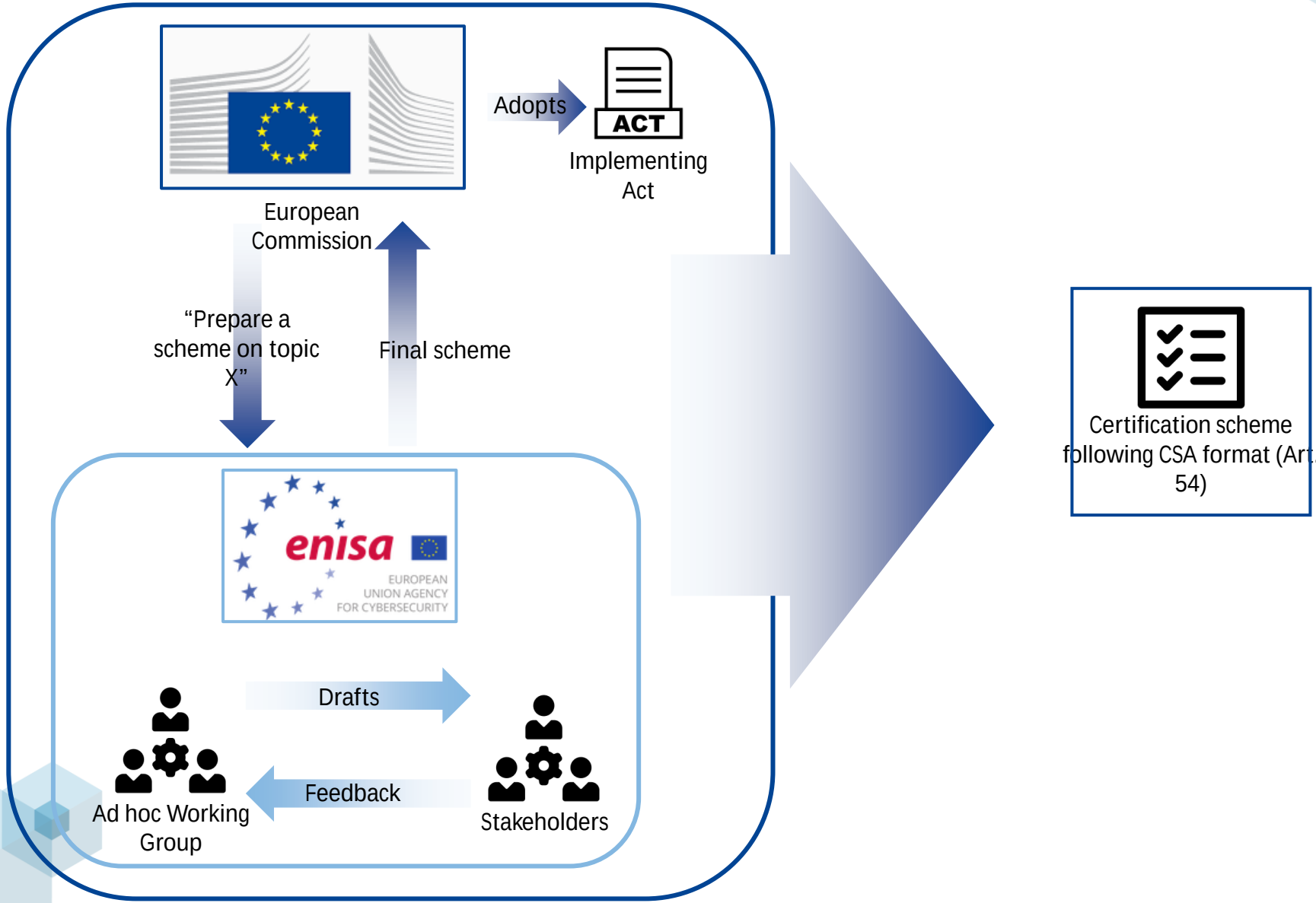
- The private sector (manufacturers) produce scheme-conform products/services/processes
- Manufacturers MAY issue declarations of conformity self-assessment (where the schemes allow it)
- Manufacturers MAY ask to get certificates from accredited Conformity Assessment Bodies (CABs)

By default, certification/conformity self-assessment is voluntary, unless specified by Union or Member State law

Planned deactivation of any existing national cybersecurity certification scheme covering the same topic

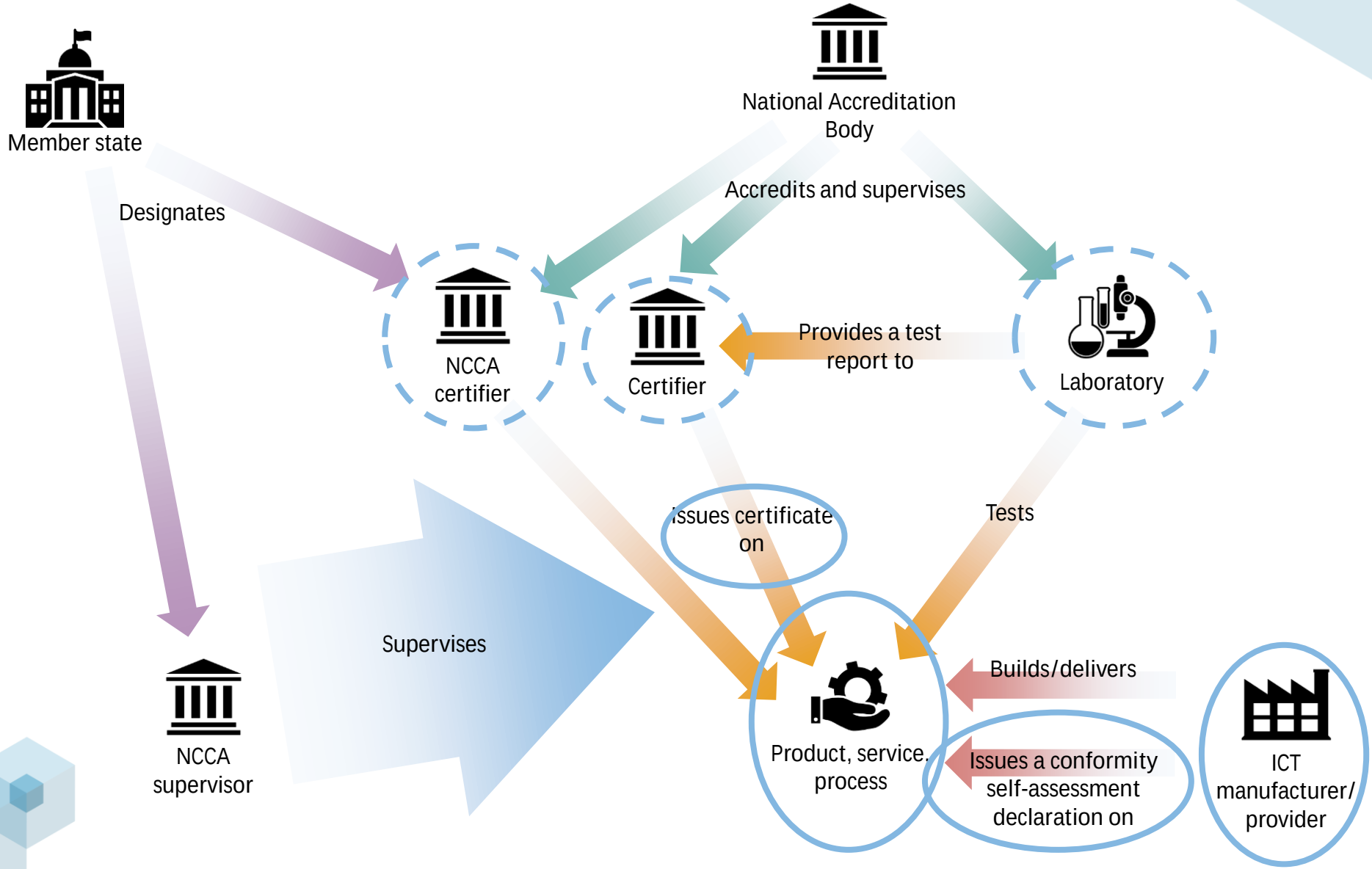
The Cybersecurity Act

The certification framework: Giving life to a scheme



The Cybersecurity Act

The certification framework: National entities and interactions



The Cybersecurity Act

The certification framework: What does a scheme look like?

Article 54(1), paragraphs a) to v)

22 elements

(a) the subject matter and scope of the certification scheme [...]

(d) where applicable, one or more assurance levels

(e) an indication of whether conformity self-assessment is permitted under the scheme

(c) references to the international, European or national standards applied in the evaluation [...] or other cybersecurity requirements [...]

(g) the specific evaluation criteria and methods to be used including types of evaluation [...]

(f) where applicable, specific or additional requirements to which conformity assessment bodies are subject [...]

(j) rules for monitoring compliance of ICT products, ICT services and ICT processes [...]

Certification scheme following CSA format

...and others...

(p) the content and the format of the European cybersecurity certificates and the EU statements of conformity [...]

(q) the period of the availability of the EU statement of conformity [...]

(r) maximum period of validity of European cybersecurity certificates [...]

The Cybersecurity Act

The certification framework: A few words on the EUCC

- Common Criteria based European candidate cybersecurity certification scheme (EUCC)
- Final version May 25th, 2021
- For IT products
- Product evaluation based on the Common Criteria standards
  - ISO/IEC 15408 series on Information security, cybersecurity and privacy protection — Evaluation criteria for IT security Revised in 2022. Now 5 parts
  - ISO/IEC 18045 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation Revised in 2022
  - See also the Common Criteria Portal for the publically available versions ("CC" and "CEM")
- Conformity assessment body accreditation
  - ISO/IEC 17065:2012 Conformity assessment — Requirements for bodies certifying products, processes and services
  - ISO/IEC 17025:2017 General requirements for the competence of testing and calibration laboratories
  - ISO/IEC TS 23532-1:2021 Information security, cybersecurity and privacy protection — Requirements for the competence of IT security testing and evaluation laboratories — Part 1: Evaluation for ISO/IEC 15408
- Evaluator competence
  - ISO/IEC 19896-1:2018 IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements Under revision
  - ISO/IEC 19896-3:2018 IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators Under revision
- Assurance levels covered are 'substantial' and 'high' (so, no conformity self-assessment possible), with a detailed mapping of these to the Common Criteria assurance components
- Expect the EU Commission's implementing act either at the end of 2023, or at the "very beginning" of 2024...

The Cybersecurity Act

The certification framework: A few words on the EUCS

- European Cybersecurity Certification Scheme for Cloud Services (EUCS)
- Last public version December 22nd, 2020
- For Cloud services according to capabilities type (application, platform, infrastructure)
- Product evaluation based on the Custom requirements (Annex A of the scheme). Sources:
  - ISO/IEC ISO/IEC 22123 Information technology — Cloud computing Formerly ISO/IEC 17788. For vocabulary
  - ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27017. For security vocabulary and controls

  CEN/CLC/JTC 13 Currently standardizing Annex A: FprCEN/CLC/TS 18026 Three-level approach for a set of cybersecurity requirements for cloud services
- Conformity assessment body accreditation
  - Baseline: ISO/IEC 17065:2012 Conformity assessment — Requirements for bodies certifying products, processes and services
  - A CEN/CLC/JTC 13 standard is in preparation: prCEN/CLC/TS XXX Requirements for Conformity Assessment Bodies certifying Cloud Services
- Assurance levels covered are 'basic', 'substantial' and 'high'. Conformity self-assessment not authorized. Annex A requirements clearly directly mapped to the assurance levels
- Final scheme still under negotiation. No date on publication.

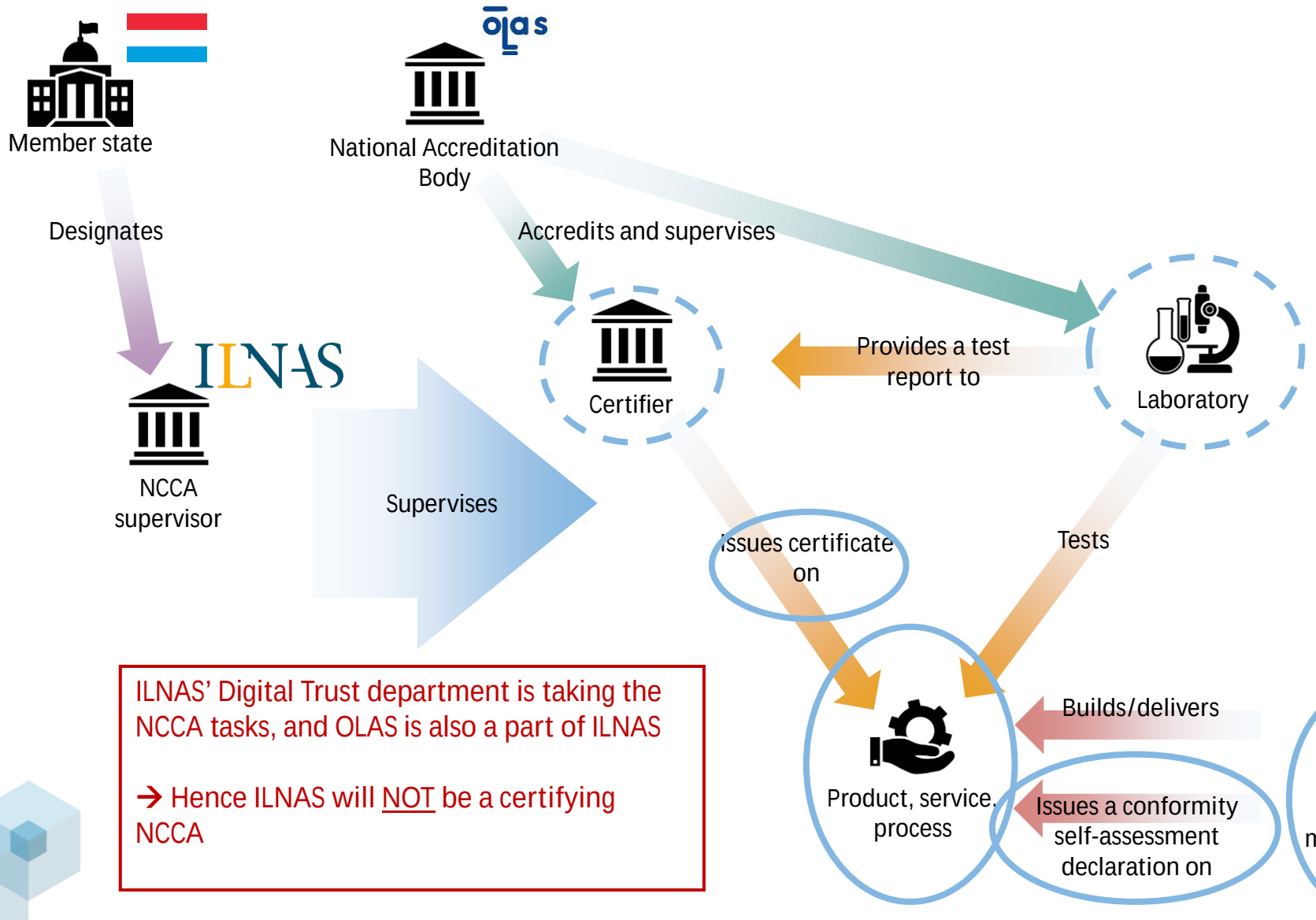
The Cybersecurity Act

The certification framework: A few words on the EU5G

- EU 5G Cybersecurity Certification Scheme (EUCS)
- No first draft available yet; only the terms of reference of the ENISA ad-hoc working group drafting the scheme
- For 5G network components and processes related to:
  - eUICC (embedded Universal Integrated Circuit Card), basically SIM cards
  - Processes for remote SIM provisioning
- Standards bodies and provider of major interest:
  - GSMA
  - ETSI/3GPP
- Synchronization required with the European 5G Toolbox

ILNAS' role

The overall general picture in Luxembourg at the moment



ILNAS' Digital Trust department is taking the NCCA tasks, and OLAS is also a part of ILNAS

→ Hence ILNAS will NOT be a certifying NCCA

The Cybersecurity Act

CSA in support of other legislation – Some examples

- Cyber Resilience Act:
  - Proposed legislation that introduces EC marking to "products with digital elements" in particular in terms of cybersecurity
  - Link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454
  - Certification of products following EUCC (or other schemes to be defined following the CSA, such as a scheme for IoT) could allow presumption of conformity to the CRA

- Artificial Intelligence Act:
  - Proposed legislation that introduces a framework for the safe deployment of products containing artificial intelligence components
  - Link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206
  - Certification of products or services following a CSA scheme could allow presumption of conformity to the AIA's cybersecurity requirements (Note: AIA goes further than cybersecurity)

- eIDAS revision:
  - Proposed revision to eIDAS that in particular mandates the implementation of national, interoperable digital identity wallets
  - Link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281
  - The Digital Identity Wallet itself, or major IT components thereof, could be the subject respectively of a CSA certification scheme, or of EUCC certification

The Cybersecurity Act

Accreditation for the CSA

The EUCC is most likely to be launched first.

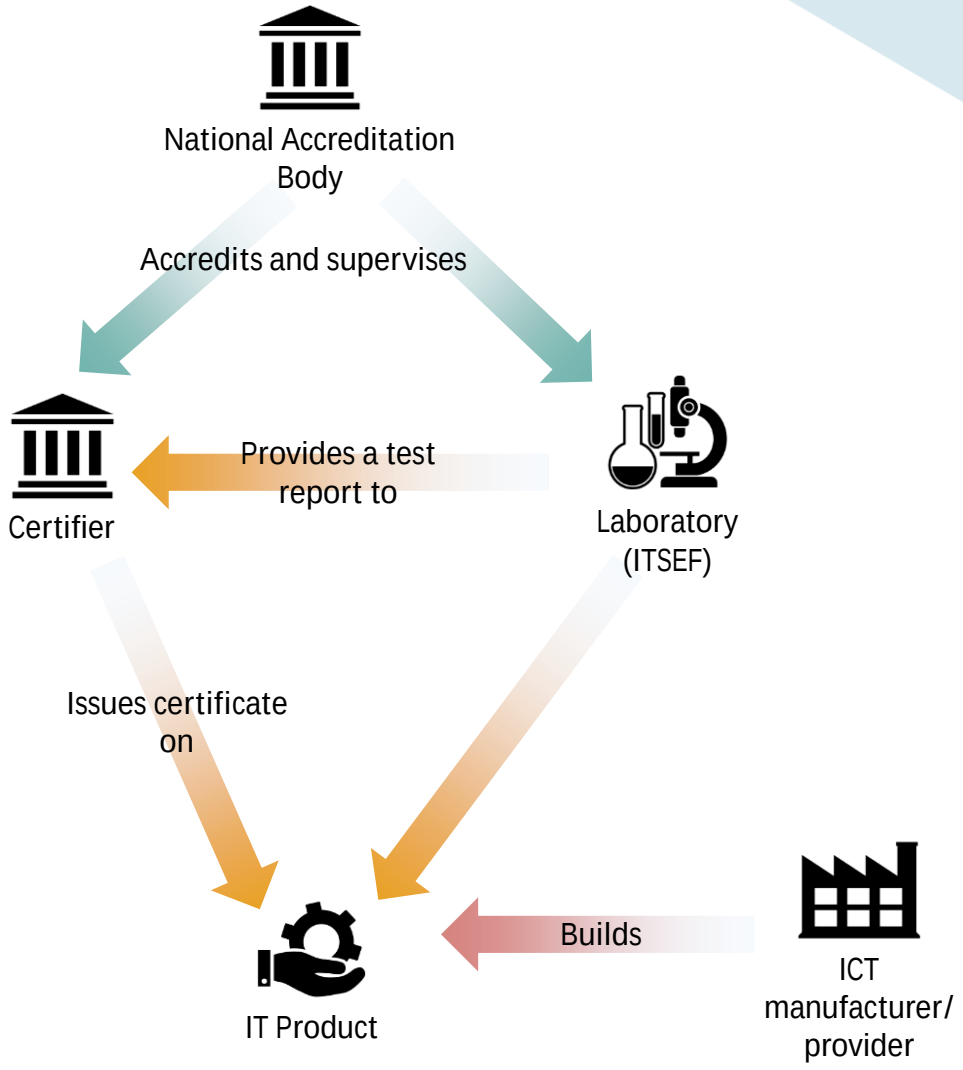
This is where accreditation might be the most needed soon.

ITSEF: IT Security Evaluation Facility

- Laboratory
- Subject to ISO/IEC 17025 accreditation
- Specialized in IT security testing

Typical IT security testing tasks:

- Penetration testing, including vulnerability analysis and exploitation
- Code review
- Functional testing
- Verification of cryptography implementation
- Physical security
- Documentation review (user and developer)
- ...



Thank you

Merci

Danke

ILNAS

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux

Tel. : (+352) 24 77 43 - 01 · Fax : (+352) 24 79 43 - 10

E-mail : info@ilnas.etat.lu

www.portail-qualite.lu