Welcome
Bienvenue
Willkommen

ILNAS

The Cybersecurity Act and the role of ILNAS

18/10/2023, CORAL event - LHC

Jean Lancrenon
Project Officer – Digital Trust department, ILNAS

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

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

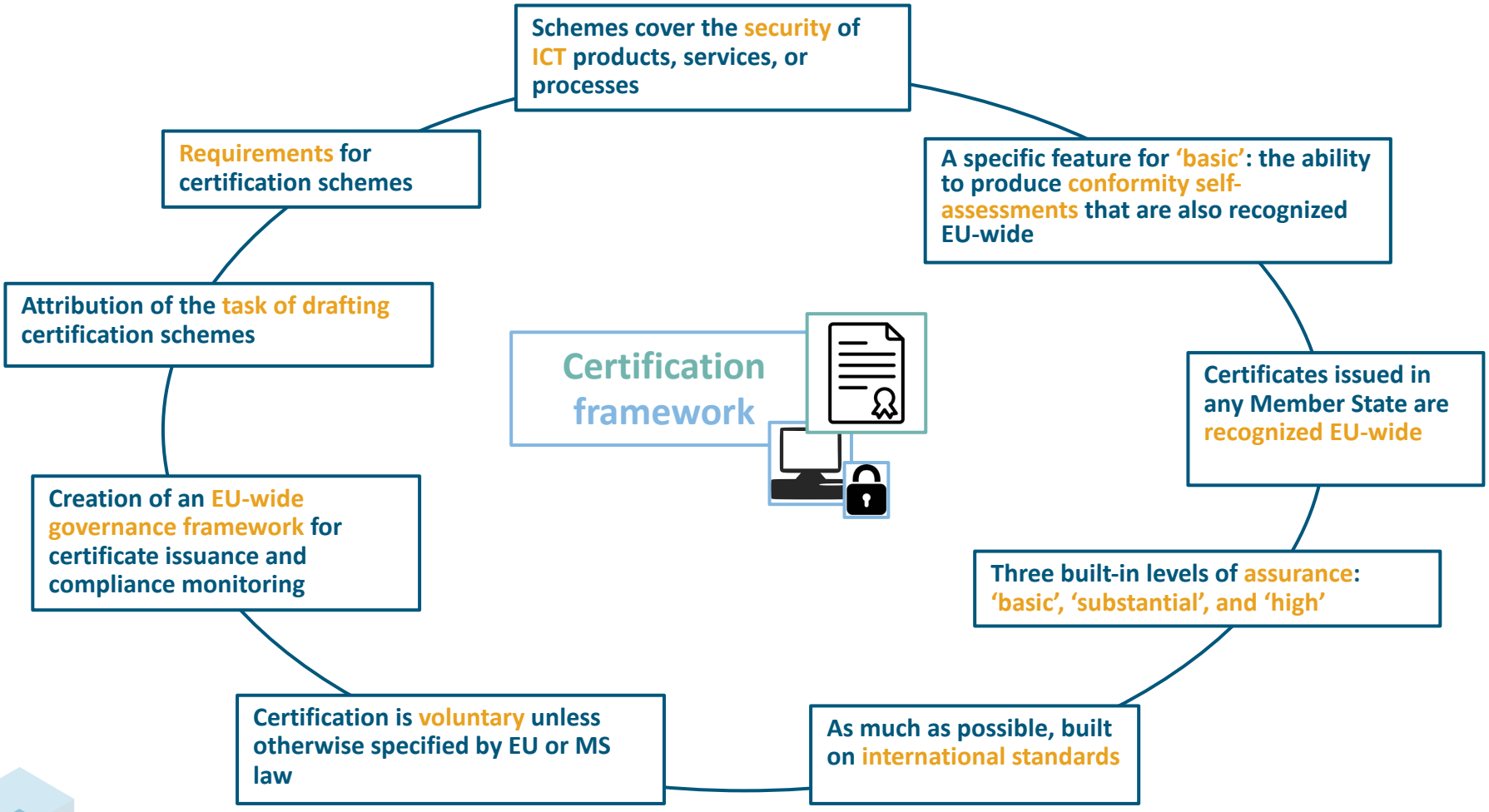
Article 20(4) on ad hoc working groups

Article 22 Stakeholder Cybersecurity Certification Group (SCCG)

Visit ENISA (online) here.

The Cybersecurity Act

The certification framework: Summary



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

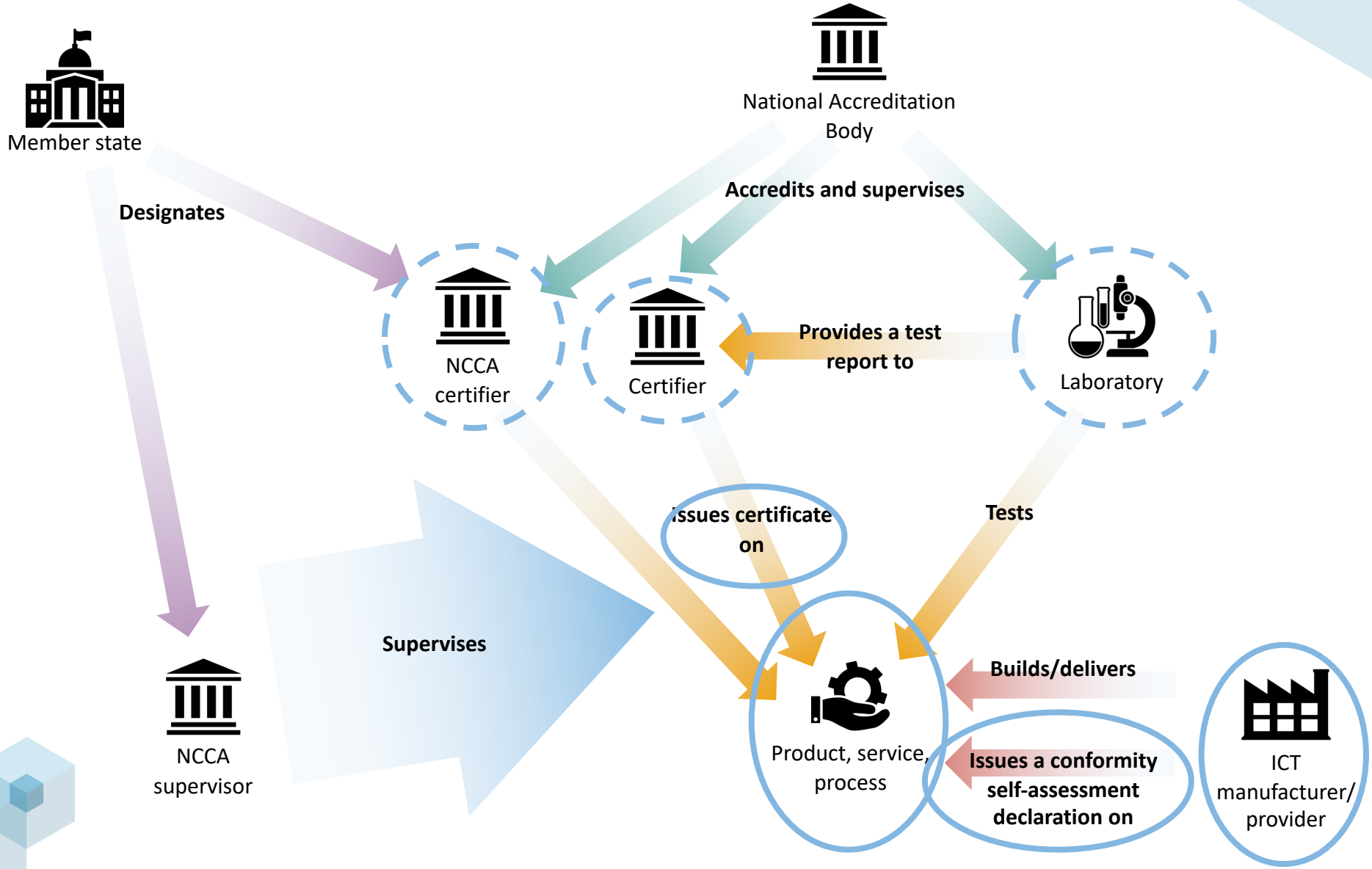
- The private sector (manufacturers) produce scheme-conform products/services/processes
- Manufacturers MAY issue declarations of conformity self-assessment (where the schemes allow it)
- Manufacturers MAY ask to get certificates from accredited Conformity Assessment Bodies (CABs)

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

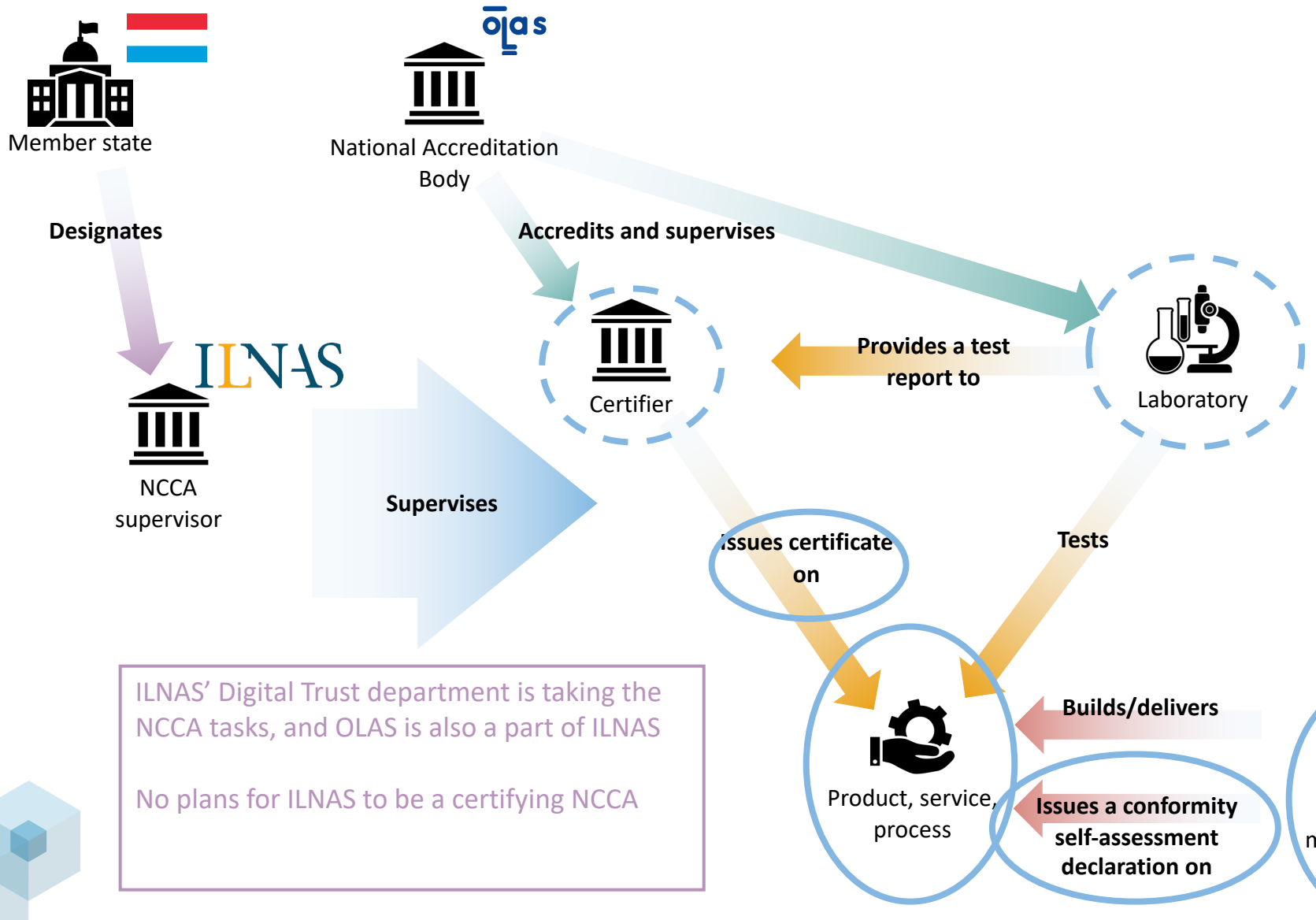
The Cybersecurity Act

The certification framework: National entities and interactions



The Cybersecurity Act

The certification framework: National entities and interactions in Luxembourg

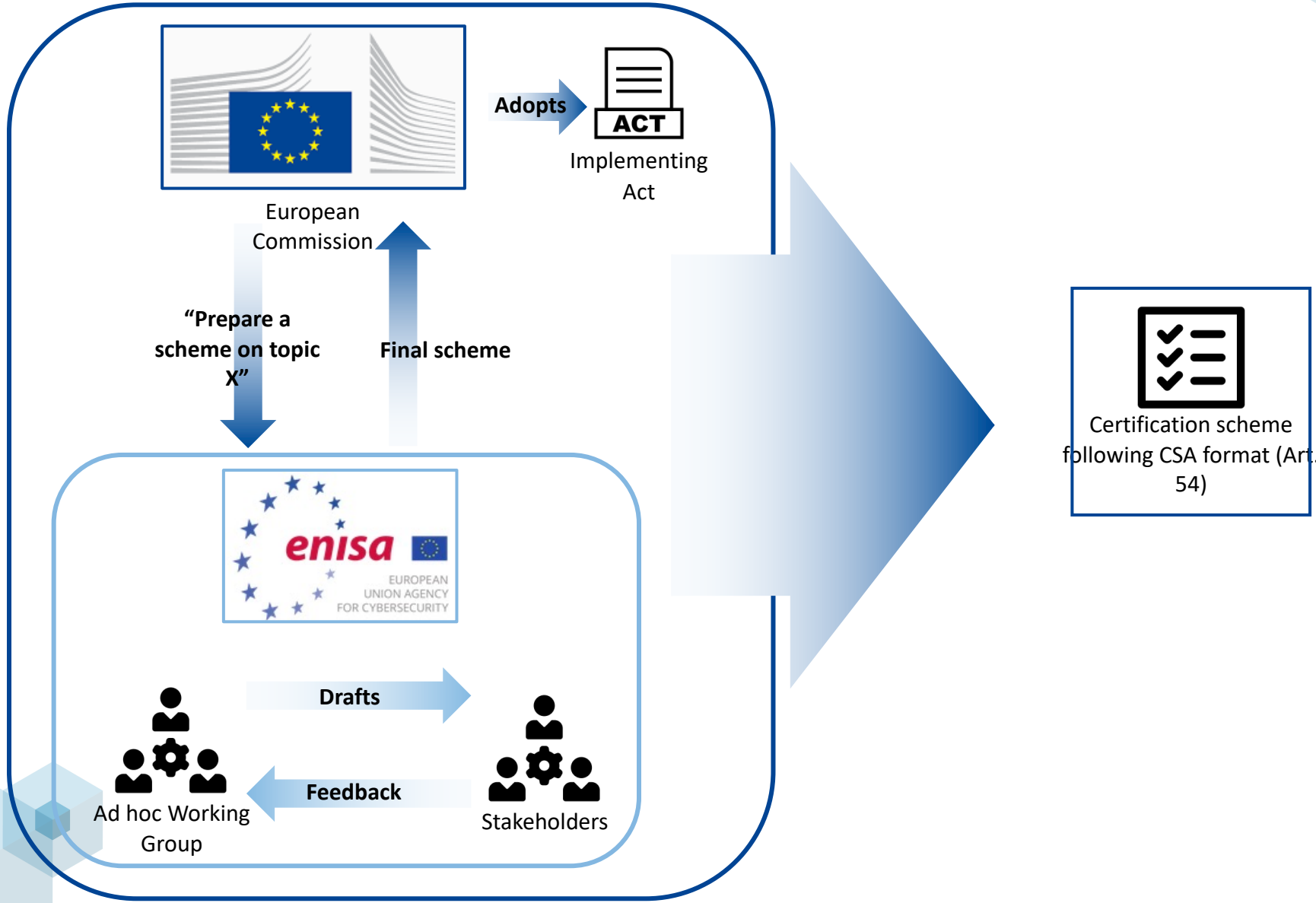


ILNAS' Digital Trust department is taking the NCCA tasks, and OLAS is also a part of ILNAS

No plans for ILNAS to be a certifying NCCA

The Cybersecurity Act

The certification framework: Giving life to a scheme



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
- 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
- The EU Commission's draft implementing act was just made available for public consultation: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13382-Cybersecurity-security-requirements-for-ICT-product-certification_en

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). These are currently being turned into standards by CEN/CLC/JTC 13
- 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 (EU5G)
- 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

What ILNAS does

ILNAS DIGITAL TRUST

MISSIONS RELATED TO 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

Ongoing

- Updating the DTD documentation to accommodate supervision requests
- Collaborating with OLAS to help put together an accreditation framework and to cooperate efficiently in CAB supervision

Contact info

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

OTHER DTD MISSIONS

- Monitor the activities and compliance of Trust Service Providers in the context of the eIDAS Regulation; maintenance of the Luxembourg Trusted List
- Monitor the activities and compliance of *Prestataires de Services de Dématérialisation et de Conservation* in the context of the Luxembourg e-archiving framework

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