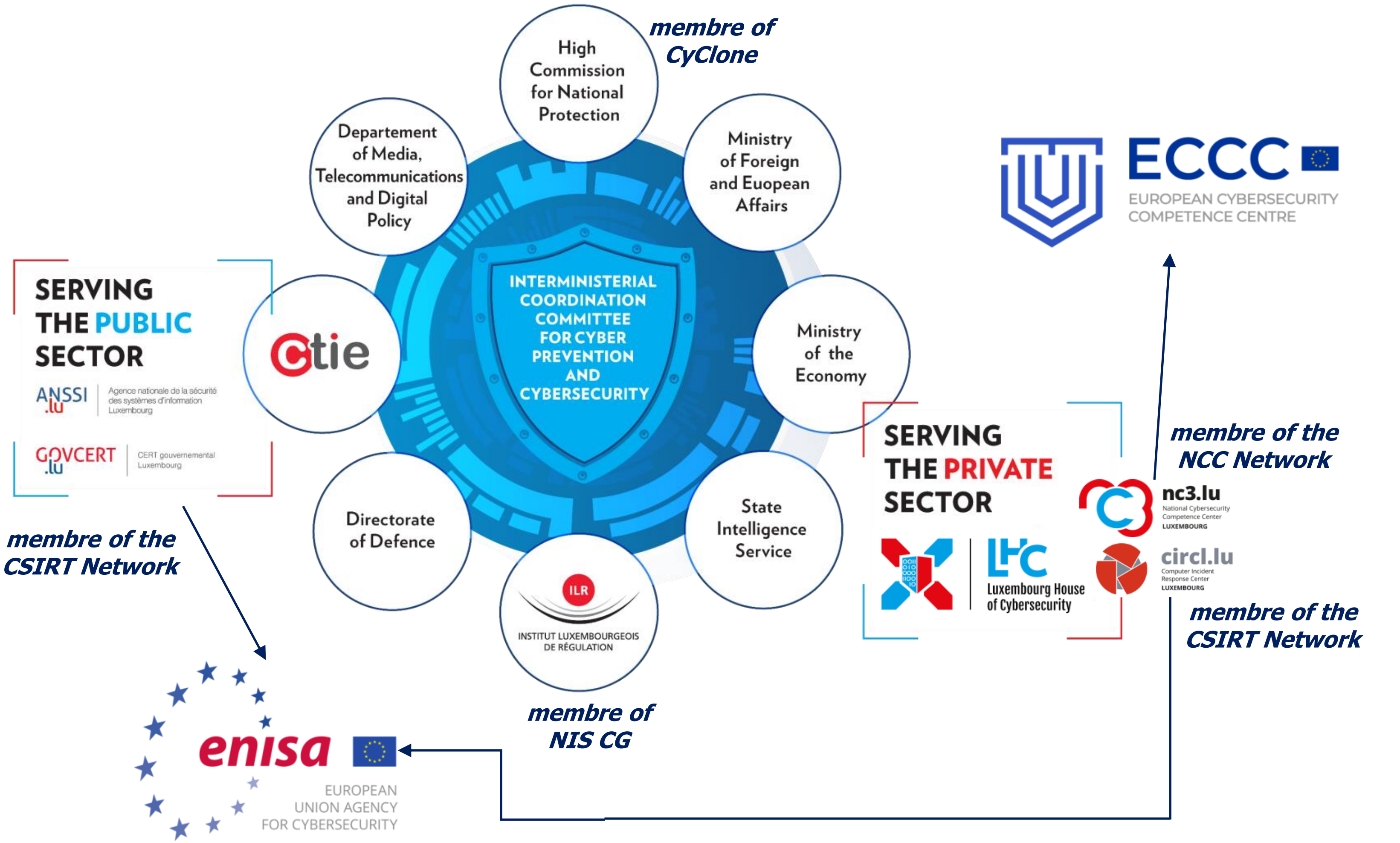
LUXEMBOURG HOUSE OF CYBERSECURITY

CYBERSECURITY
LUXEMBOURG

National Governance



INTERMINISTERIAL COORDINATION COMMITTEE FOR CYBER PREVENTION AND CYBERSECURITY

High Commission for National Protection

membre of CyClone

Ministry of Foreign and Euopean Affairs

Ministry of the Economy

State Intelligence Service

INSTITUT LUXEMBOURGEOIS DE RÉGULATION

ILR

membre of NIS CG

Directorate of Defence

ctie

Departement of Media, Telecommunications and Digital Policy

SERVING THE PUBLIC SECTOR

ANSSI .lu Agence nationale de la sécurité des systèmes d'information Luxembourg

GOVCERT .lu CERT gouvernemental Luxembourg

membre of the CSIRT Network

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

SERVING THE PRIVATE SECTOR

LHC Luxembourg House of Cybersecurity

nc3.lu National Cybersecurity Competence Center LUXEMBOURG

circl.lu Computer Incident Response Center LUXEMBOURG

membre of the NCC Network

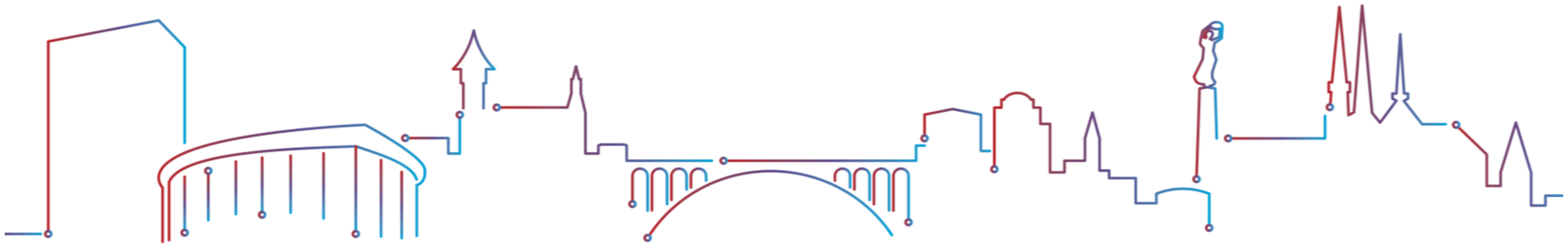
membre of the CSIRT Network

ECCC

EUROPEAN CYBERSECURITY COMPETENCE CENTRE

LHC
Luxembourg House
of Cybersecurity

THE GATEWAY TO CYBER RESILIENCE



**Luxembourg,
a pioneer in the open
cybersecurity data economy**

lhc.lu

310+ ACTIVE ACTORS IN CYBERSECURITY

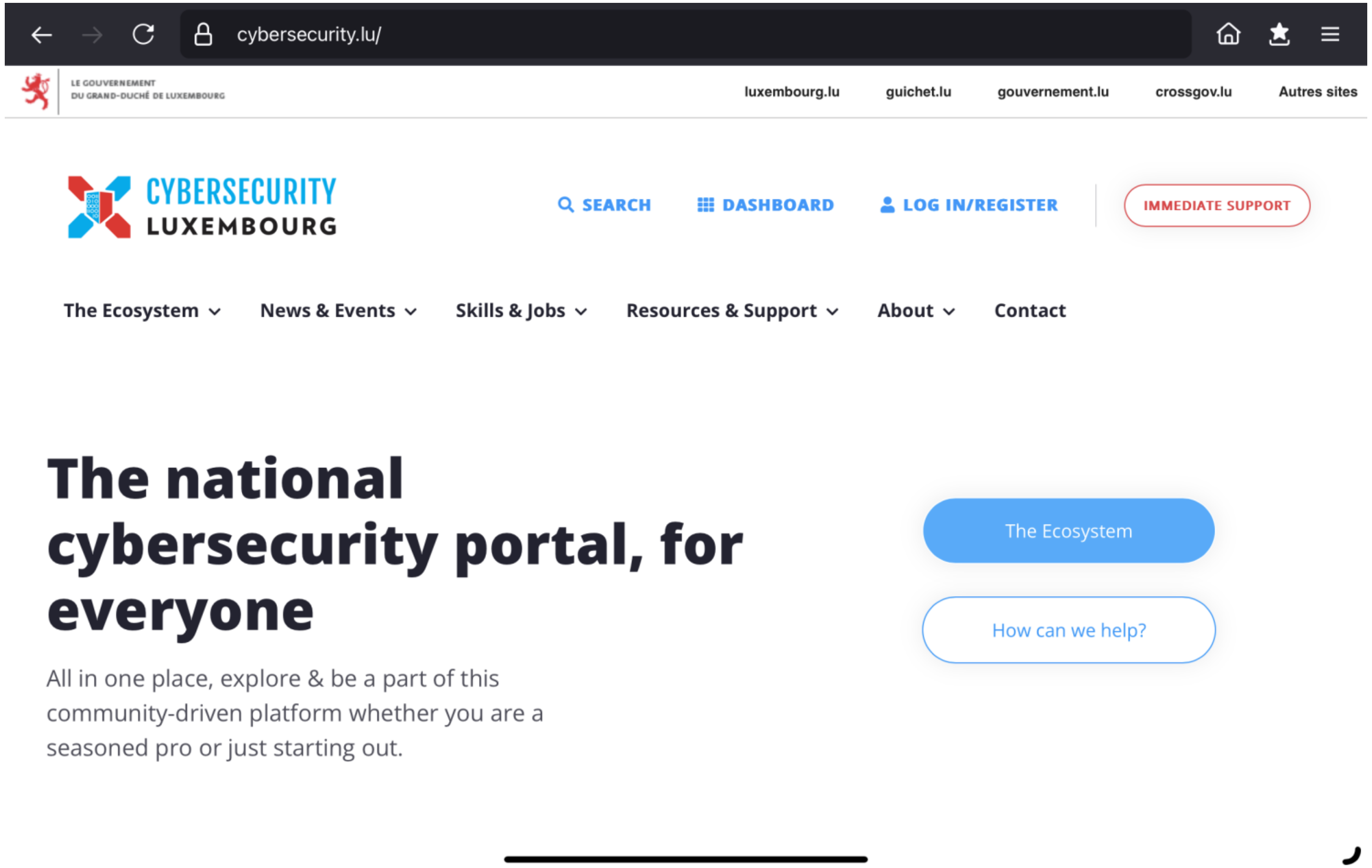
90+ WITH CYBERSECURITY AS A CORE BUSINESS

70+ STARTUPS

CYBERSECURITY
LUXEMBOURG

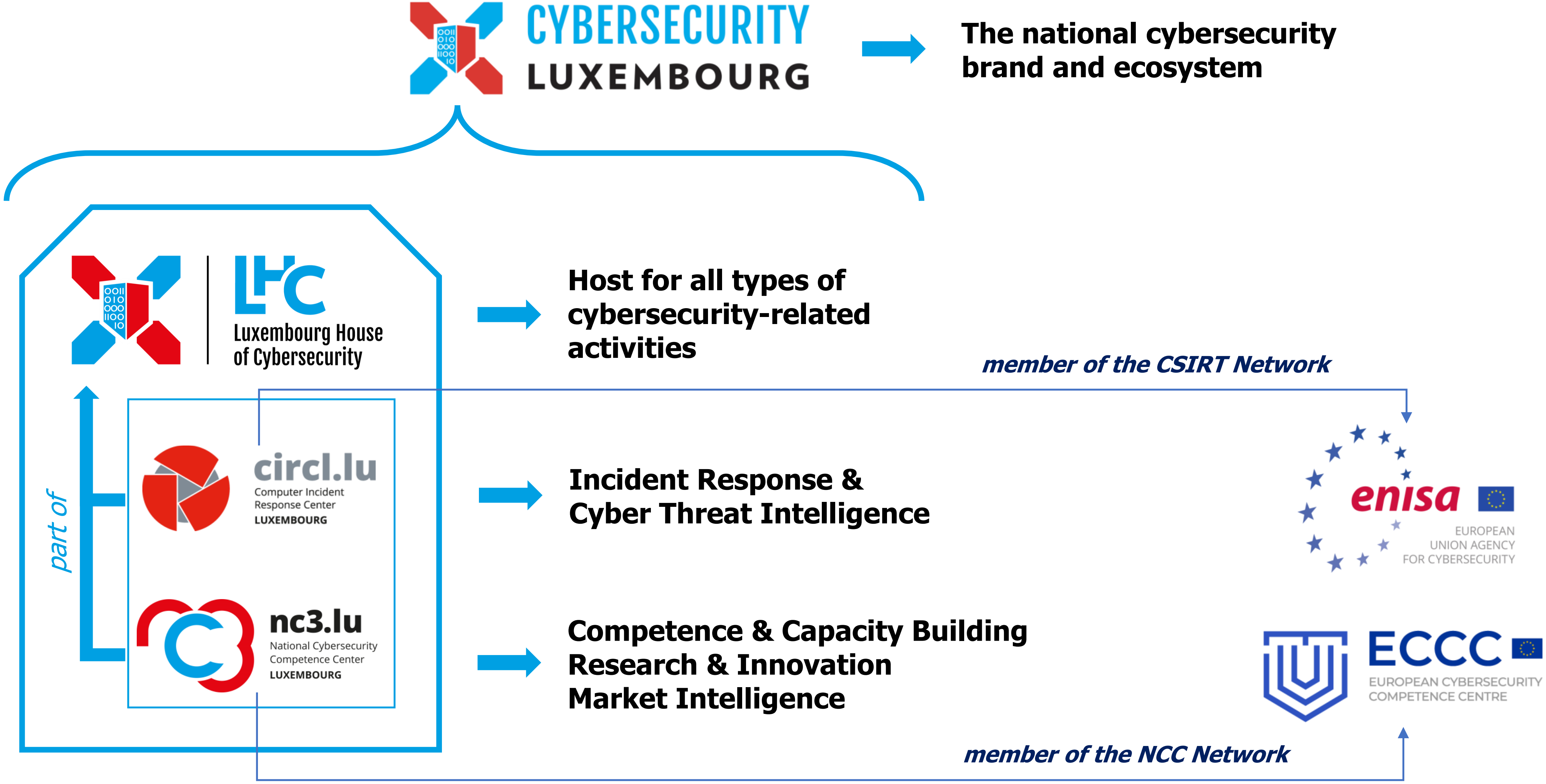
More about
the ecosystem

National *cybersecurity* Portal



The national cybersecurity portal, for everyone

All in one place, explore & be a part of this community-driven platform whether you are a seasoned pro or just starting out.


CYBERSECURITY LUXEMBOURG
LHC
Luxembourg House of Cybersecurity
part of
circl.lu
Computer Incident Response Center
LUXEMBOURG
nc3.lu
National Cybersecurity Competence Center
LUXEMBOURG
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

The national cybersecurity brand and ecosystem

Host for all types of cybersecurity-related activities

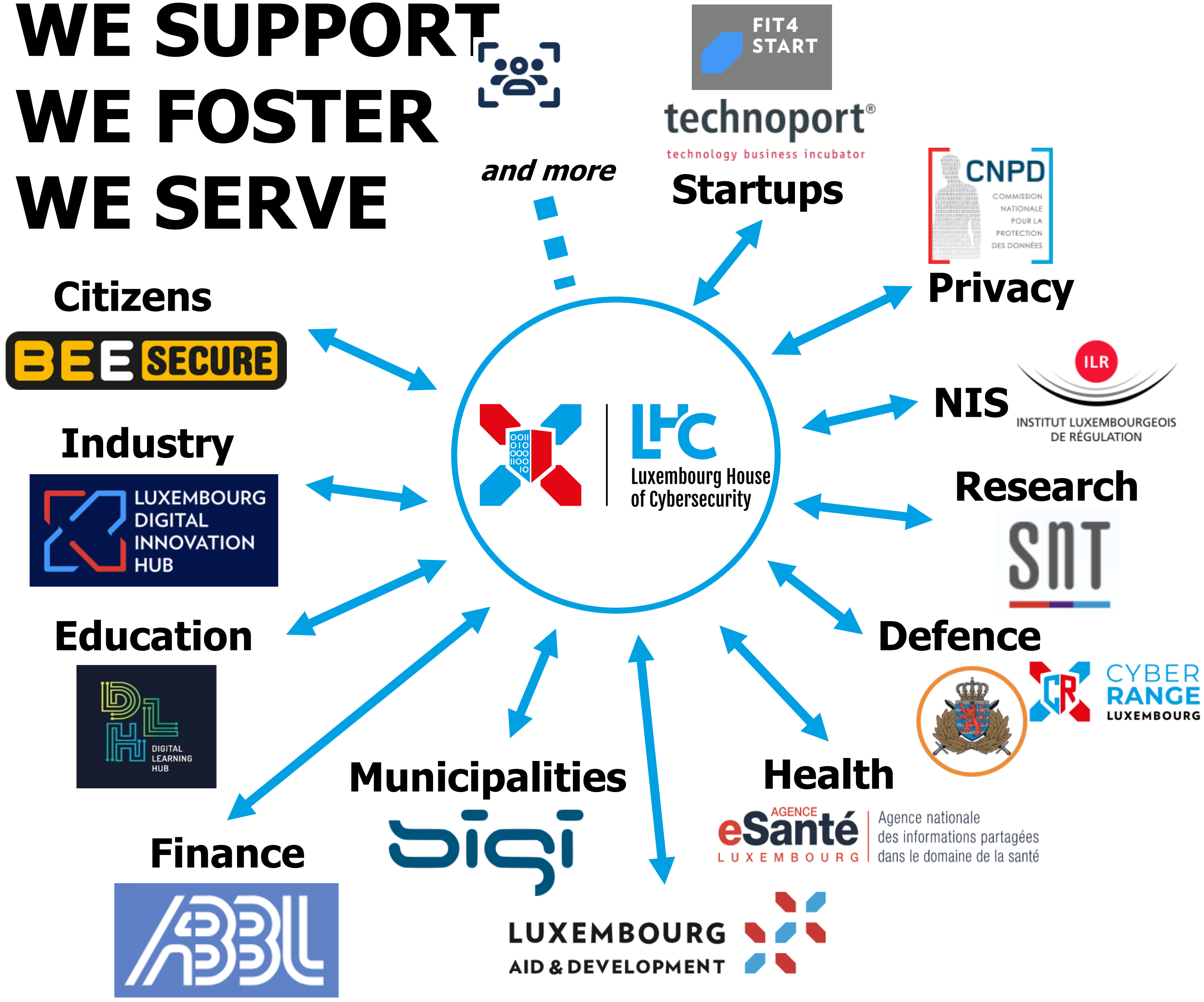
member of the CSIRT Network

Incident Response & Cyber Threat Intelligence

Competence & Capacity Building
Research & Innovation
Market Intelligence

member of the NCC Network

WE SUPPORT
WE FOSTER
WE SERVE



LHC
Luxembourg House of Cybersecurity

and more

FIT4 START
technoport®
technology business incubator
Startups

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES
Privacy

NIS
ILR
INSTITUT LUXEMBOURGEOIS DE RÉGULATION

Research
SnT

Defence
CYBER RANGE LUXEMBOURG

Health
AGENCE eSanté LUXEMBOURG
Agence nationale des informations partagées dans le domaine de la santé

LUXEMBOURG AID & DEVELOPMENT

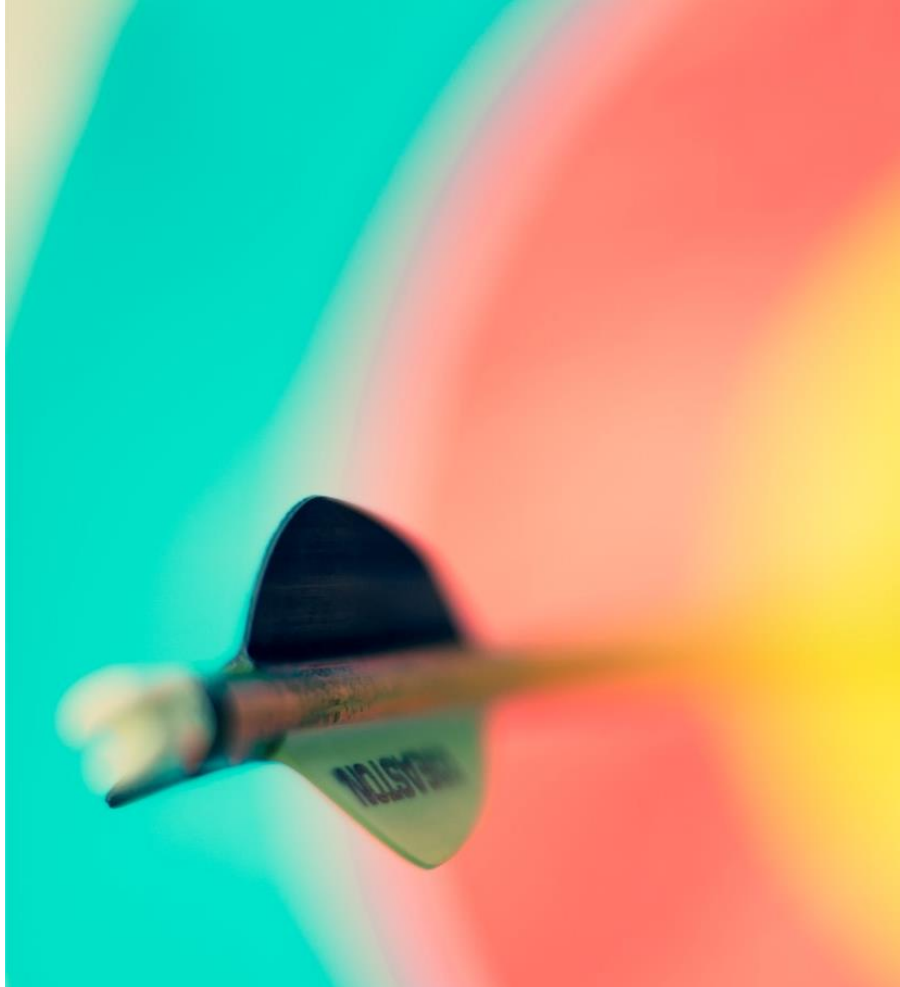
Municipalities
SIGI

Finance
ABBL

Education
DIGITAL LEARNING HUB

Industry
LUXEMBOURG DIGITAL INNOVATION HUB

Citizens
BEE SECURE



WE HOST

ENCRYPTION EUROPE

ISACA
Luxembourg Chapter

CWF
DIVERSITY & INNOVATION IN CYBERSECURITY
BRUSSELS | LUXEMBOURG

Women Cyber Force

clusil

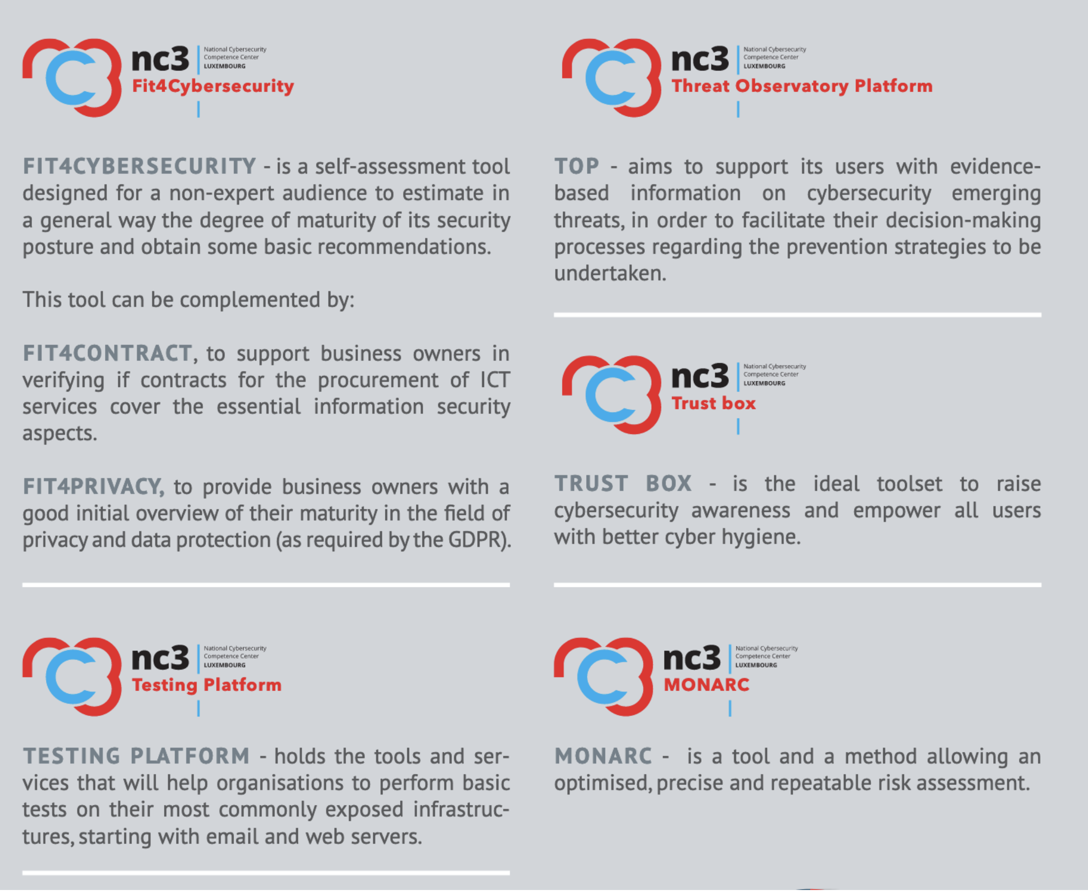
National Cybersecurity Competence Centre

nc3.lu
National Cybersecurity
Competence Center
LUXEMBOURG

- Competence and Capabilities Building
- Ecosystem and Industrialisation
- Research, Data and Innovation
- NCC-LU

ROOM #42
room42.eu
DØ[N'T]PANIC

SPAMBEE



nc3 National Cybersecurity Competence Center LUXEMBOURG
Fit4Cybersecurity

FIT4CYBERSECURITY - is a self-assessment tool designed for a non-expert audience to estimate in a general way the degree of maturity of its security posture and obtain some basic recommendations.

This tool can be complemented by:

FIT4CONTRACT, to support business owners in verifying if contracts for the procurement of ICT services cover the essential information security aspects.

FIT4PRIVACY, to provide business owners with a good initial overview of their maturity in the field of privacy and data protection (as required by the GDPR).

nc3 National Cybersecurity Competence Center LUXEMBOURG
Testing Platform

TESTING PLATFORM - holds the tools and services that will help organisations to perform basic tests on their most commonly exposed infrastructures, starting with email and web servers.

nc3 National Cybersecurity Competence Center LUXEMBOURG
Threat Observatory Platform

TOP - aims to support its users with evidence-based information on cybersecurity emerging threats, in order to facilitate their decision-making processes regarding the prevention strategies to be undertaken.

nc3 National Cybersecurity Competence Center LUXEMBOURG
Trust box

TRUST BOX - is the ideal toolset to raise cybersecurity awareness and empower all users with better cyber hygiene.

nc3 National Cybersecurity Competence Center LUXEMBOURG
MONARC

MONARC - is a tool and a method allowing an optimised, precise and repeatable risk assessment.

Computer Incident Response Center Luxembourg

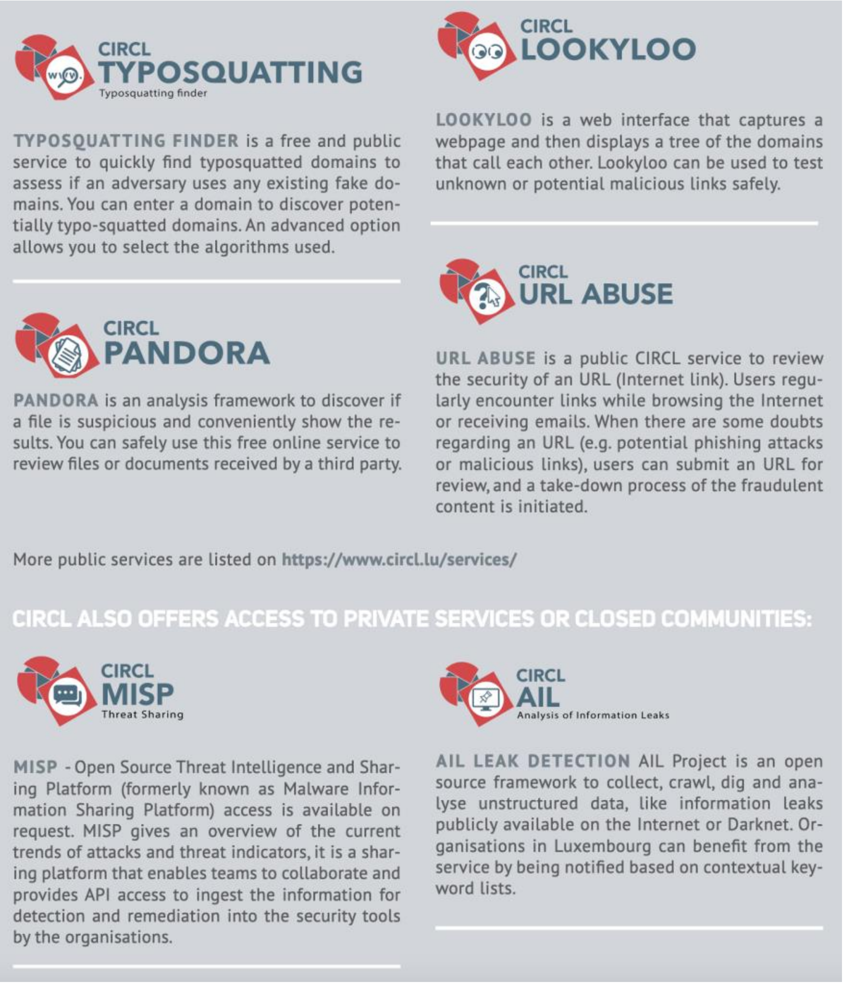
circl.lu
Computer Incident
Response Center
LUXEMBOURG

- CSIRT (Incident Coordination and Incident Handling)
- Cyber Threat Intel and support tools
- CSIRT NIS

pandora

MISP
Threat Sharing

ail project



CIRCL
TYPOSQUATTING
Typosquatting finder

TYPOSQUATTING FINDER is a free and public service to quickly find typosquatted domains to assess if an adversary uses any existing fake domains. You can enter a domain to discover potentially typo-squatted domains. An advanced option allows you to select the algorithms used.

CIRCL
PANDORA

PANDORA is an analysis framework to discover if a file is suspicious and conveniently show the results. You can safely use this free online service to review files or documents received by a third party.

CIRCL
LOOKYLOO

LOOKYLOO is a web interface that captures a webpage and then displays a tree of the domains that call each other. Lookyloo can be used to test unknown or potential malicious links safely.

CIRCL
URL ABUSE

URL ABUSE is a public CIRCL service to review the security of an URL (Internet link). Users regularly encounter links while browsing the Internet or receiving emails. When there are some doubts regarding an URL (e.g. potential phishing attacks or malicious links), users can submit an URL for review, and a take-down process of the fraudulent content is initiated.

More public services are listed on **https://www.circl.lu/services/**

CIRCL ALSO OFFERS ACCESS TO PRIVATE SERVICES OR CLOSED COMMUNITIES:

CIRCL
MISP
Threat Sharing

MISP - Open Source Threat Intelligence and Sharing Platform (formerly known as Malware Information Sharing Platform) access is available on request. MISP gives an overview of the current trends of attacks and threat indicators, it is a sharing platform that enables teams to collaborate and provides API access to ingest the information for detection and remediation into the security tools by the organisations.

CIRCL
AIL
Analysis of Information Leaks

AIL LEAK DETECTION AIL Project is an open source framework to collect, crawl, dig and analyse unstructured data, like information leaks publicly available on the Internet or Darknet. Organisations in Luxembourg can benefit from the service by being notified based on contextual keyword lists.

Thank you for your attention

Time to discover the

LHC

Luxembourg House of Cybersecurity

Digital Trust White Paper 4.0

TRUST-ENABLING MISSIONS FOR THE DIGITAL MARKET

Presentation of ILNAS

14th December 2023

Dr. Jean-Philippe Humbert
Adjoint à la Direction - ILNAS

CONTENT

I - PRESENTATION OF ILNAS AND ANEC EIG

II - PRESENTATION OF THE NATIONAL STANDARDS BODY

III - PARTICIPATION IN TECHNICAL STANDARDIZATION

IV - WHITE PAPERS, TECHNICAL REPORTS AND GUIDES

V - RESEARCH ACTIVITIES

VI - EDUCATION ABOUT STANDARDIZATION

CONTENT

I - PRESENTATION OF ILNAS AND ANEC EIG

II - PRESENTATION OF THE NATIONAL STANDARDS BODY

III - PARTICIPATION IN TECHNICAL STANDARDIZATION

IV - WHITE PAPERS, TECHNICAL REPORTS AND GUIDES

V - RESEARCH ACTIVITIES

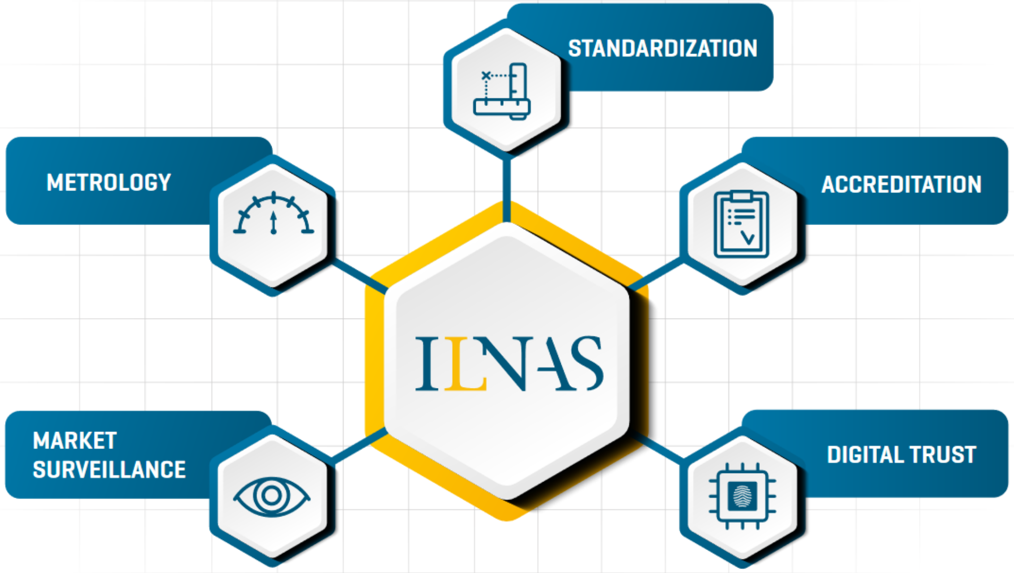
VI - EDUCATION ABOUT STANDARDIZATION

I. Presentation of ILNAS & ANEC EIG

- **ILNAS**
  - Public administration under the authority of the Minister of the Economy
  - Creation: Law of May 20, 2008
  - Legislation in force: amended Law of July 4, 2014 reorganizing ILNAS
  - Total staff: 62 (December 2023)
  - ISO 9001:2015 certification (Budget and administration department, OLN, Digital Trust department, Market surveillance department, BLM, OEC)

PORTAIL-QUALITE.LU
QUALITE · SECURITE · CONFORMITE
UNE INITIATIVE DE L' ILNAS

- **National Standards Body (OLN)**
  - Composed of 8 persons
  - Close collaboration with the E.I.G. ANEC-N



ILNAS I. Presentation of ILNAS & ANEC EIG

ANEC

- **Creation:** October 4, 2010

- **Status:** Economic Interest Group (EIG)

- **Objectives:** Promotion, awareness raising and training, applied research in the field of standardization and metrology in order to support companies' competitiveness in Luxembourg

- **Human resources:** 9 persons, including 4 employees in the standardization department (October 2023)

- **Partners:**

GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

ILNAS

CHAMBRE
DES METIERS
Luxembourg

CHAMBRE DE
COMMERCE
LUXEMBOURG

➔ Support for the implementation of the Luxembourg standardization strategy

CONTENT

I - PRESENTATION OF ILNAS AND ANEC EIG

II - PRESENTATION OF THE NATIONAL STANDARDS BODY

III - PARTICIPATION IN TECHNICAL STANDARDIZATION

IV - WHITE PAPERS, TECHNICAL REPORTS AND GUIDES

V - RESEARCH ACTIVITIES

VI - EDUCATION ABOUT STANDARDIZATION

II. Presentation of the National Standards Body (*Organisme luxembourgeois de normalisation* – OLN)

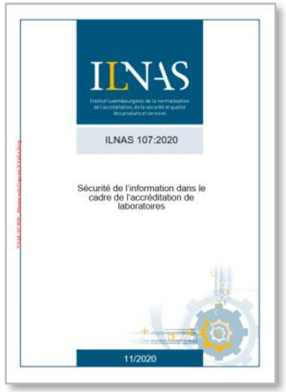
A. Main missions

ILNAS e-shop

- Coordinate and supervise the creation of national standards
- Make standards available to the market
  - ILNAS eShop
  - ILNAS reading stations
- Represent Luxembourg in the standardization related organizations

European Commission

- Manage the participation of national stakeholders in the international standardization organizations (ISO, IEC, CEN and CENELEC)
- Develop a normative culture in Luxembourg
  - Promotion
  - Education
  - Research



ILNAS

ILNAS 107:2020

Sécurité de l'information dans le cadre de l'accréditation de laboratoires

11/2020

ILNAS

ILNAS 106:2022

ARCHIVAGE ÉLECTRONIQUE - RÉFÉRENTIEL D'EXIGENCES POUR LA CERTIFICATION DES PRESTATAIRES DE SERVICES DE DÉMATÉRIALISATION OU DE CONSERVATION (PSDC)

© ILNAS 2022

07/2022

MEMBER OF THE ILNAS NETWORK

ILNAS ANEC

2023

CATALOGUE

NORMALISATION TECHNIQUE

TECHNICAL STANDARDIZATION

Formations en ligne - Online trainings

Formations techniques en normalisation

Formations personnalisées /

ILNAS ANEC

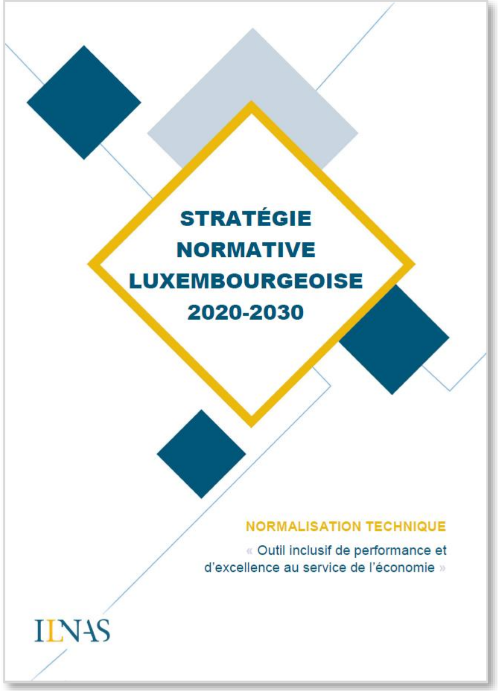
your standardization partners in Luxembourg

MAKE ICT STANDARDS YOURS!

SETTING THE STANDARDS MEANS SETTING THE MARKET

II. Presentation of the National Standards Body (*Organisme luxembourgeois de normalisation* – OLN)

B. Luxembourg standardization strategy 2020-2030



STRATÉGIE NORMATIVE LUXEMBOURGEOISE 2020-2030

NORMALISATION TECHNIQUE

« Outil inclusif de performance et d'excellence au service de l'économie »

ILNAS

→ Strategy signed by the Minister of the Economy of Luxembourg

Technical standardization

"Inclusive tool for performance and excellence to serve the economy"

PERFORMANCE

□ Pillar 1 – Use of relevant technical standards

□ Pillar 2 – Involvement in the standardization process

EXCELLENCE

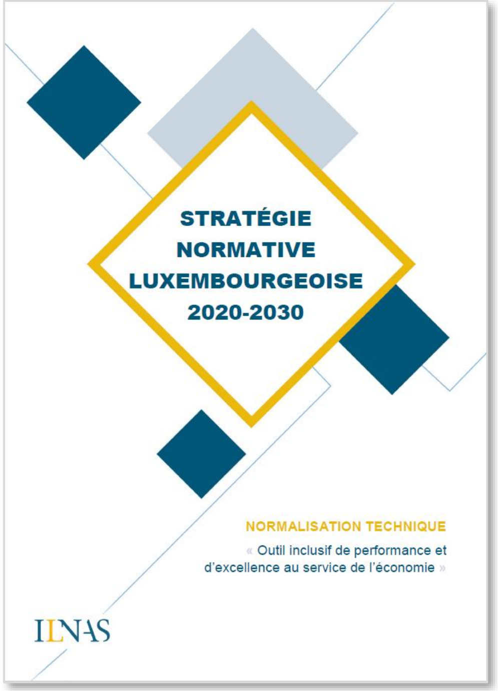
□ Pillar 3 – Active participation of the NSB in the European and international standardization organizations

□ Pillar 4 – Development of research and education about standardization

https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/strategie-normative-luxembourgeoise-2020-2030.pdf

II. Presentation of the National Standards Body (*Organisme luxembourgeois de normalisation* – OLN)

B. Luxembourg standardization strategy 2020-2030



STRATÉGIE NORMATIVE LUXEMBOURGEOISE 2020-2030

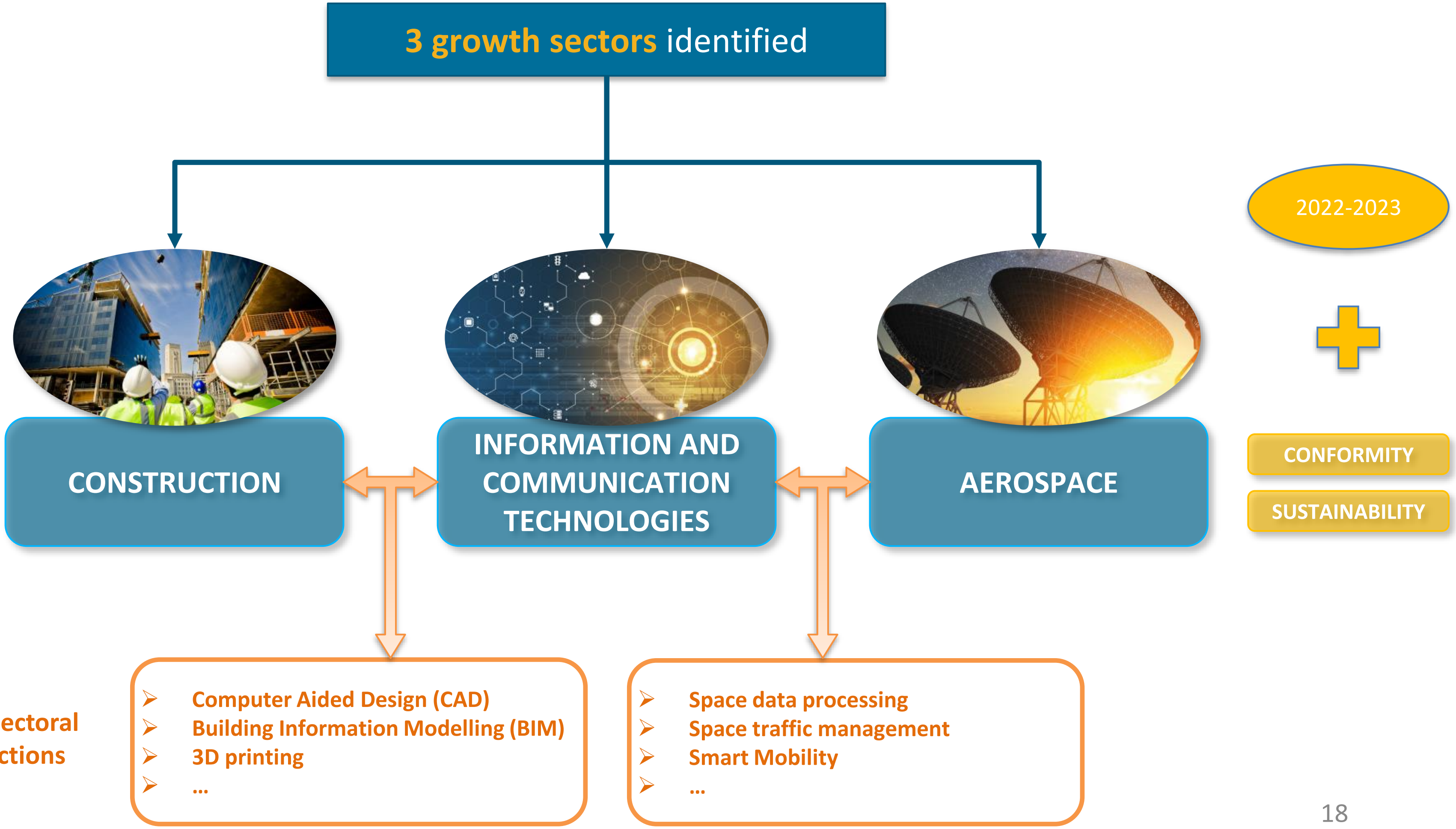
NORMALISATION TECHNIQUE

« Outil inclusif de performance et d'excellence au service de l'économie »

ILNAS

Technical standardization

"Inclusive tool for performance and excellence to serve the economy"



3 growth sectors identified

- CONSTRUCTION
- INFORMATION AND COMMUNICATION TECHNOLOGIES
- AEROSPACE

2022-2023

+ CONFORMITY

+ SUSTAINABILITY

Identification of trans-sectoral standardization interactions

- Computer Aided Design (CAD)
- Building Information Modelling (BIM)
- 3D printing
- …

- Space data processing
- Space traffic management
- Smart Mobility
- …

Policy on ICT Technical Standardization (2022-2025)

ILNAS

“Foster and strengthen the national ICT sectors involvement in standardization work”

1 Promoting the ICT technical standardization to the market

2 Reinforcing the valorization and the involvement regarding ICT technical standardization

3 Supporting and strengthening the EaS and the related research activities

ILNAS

STANDARDS ANALYSIS

ICT SECTOR

LUXEMBOURG

Version 12.0 - June 2022

ANEC

Politique normative nationale « ISO CASCO » 2022-2030

ILNAS

Politique pour la normalisation technique du secteur de la construction (2020-2025)

ILNAS

Policy on Aerospace Technical Standardization (2021-2025)

ILNAS

Policies for the Construction, Aerospace and Conformity domains are based on similar lead projects

CONTENT

I - PRESENTATION OF ILNAS AND ANEC EIG

II - PRESENTATION OF THE NATIONAL STANDARDS BODY

III - PARTICIPATION IN TECHNICAL STANDARDIZATION

IV - WHITE PAPERS, TECHNICAL REPORTS AND GUIDES

V - RESEARCH ACTIVITIES

VI - EDUCATION ABOUT STANDARDIZATION

III. Participation in technical standardization

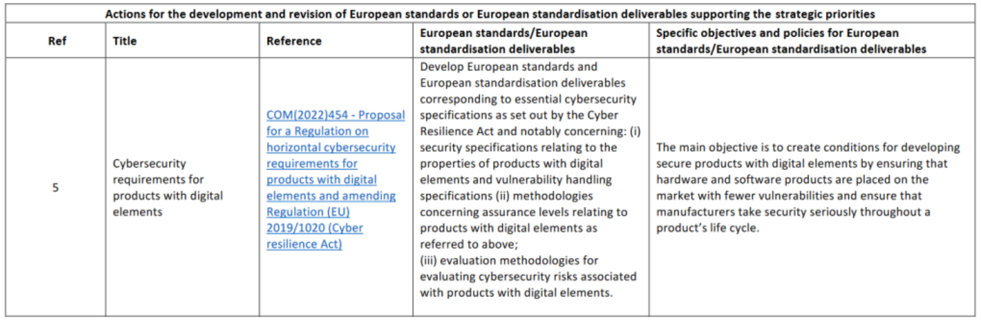
- **New paradigm in the European standardization ecosystem - European Standardisation Strategy (COM(2022) 31)**

  - Five key sets of actions:
    1. Anticipate, prioritize and address **standardization needs in strategic areas**
    2. Improve the governance and integrity of the European standardization system
    3. Enhance **European leadership** in global standards
    4. Support innovation
    5. Enable the **next generation** of standardization experts

> *“Technical standards are of strategic importance. Europe's **technological sovereignty**, **ability to reduce dependencies** and **protection of EU values** will rely on our **ability to be a global standard-setter**. With today's Strategy, we are crystal-clear on our standardisation priorities and create the conditions for European standards to become global benchmarks. **We take action to preserve the integrity of the European standardisation process, putting European SMEs and the European interest at the centre**”*
>
> Commissioner for the Internal Market, Thierry Breton

III. Participation in technical standardization

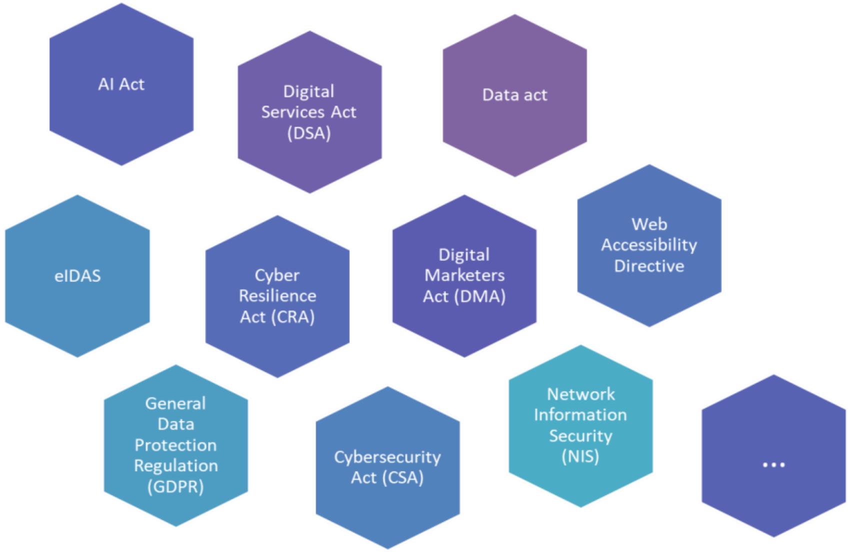
Technical standardization
A support for complying with the EU regulatory ecosystem



Actions for the development and revision of European standards or European standardisation deliverables supporting the strategic priorities				
Ref	Title	Reference	European standards/European standardisation deliverables	Specific objectives and policies for European standards/European standardisation deliverables
5	Cybersecurity requirements for products with digital elements	[COM(2022)454 - Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber resilience Act)]	Develop European standards and European standardisation deliverables corresponding to essential cybersecurity specifications as set out by the Cyber Resilience Act and notably concerning: (i) security specifications relating to the properties of products with digital elements and vulnerability handling specifications (ii) methodologies concerning assurance levels relating to products with digital elements as referred to above; (iii) evaluation methodologies for evaluating cybersecurity risks associated with products with digital elements.	The main objective is to create conditions for developing secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle.

The 2023 annual EU work program for European standardization (02/2023) - https://ec.europa.eu/docsroom/documents/53720

A more and more complex EU regulatory ecosystem for the ICT sector



AI Act

Digital Services Act (DSA)

Data act

eIDAS

Cyber Resilience Act (CRA)

Digital Marketers Act (DMA)

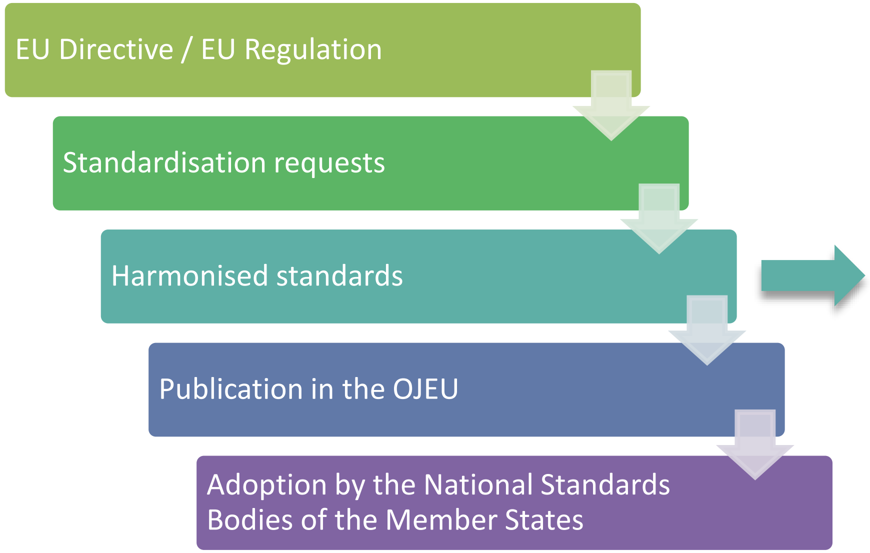
Web Accessibility Directive

General Data Protection Regulation (GDPR)

Cybersecurity Act (CSA)

Network Information Security (NIS)

…



EU Directive / EU Regulation

Standardisation requests

Harmonised standards

Publication in the OJEU

Adoption by the National Standards Bodies of the Member States

Can be used by manufacturers, other economic operators and conformity assessment bodies to demonstrate that their product, service or process complies with relevant EU legislation

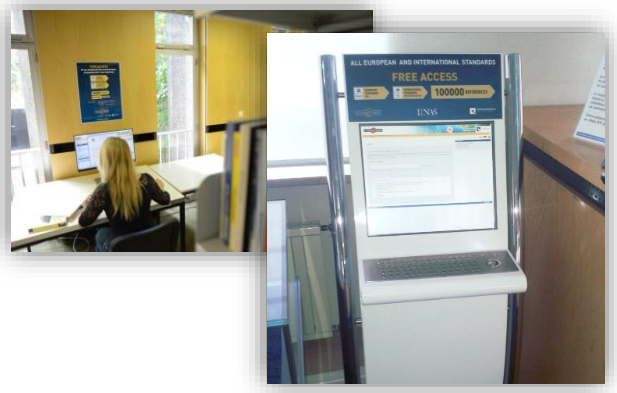
III. Participation in technical standardization

How to be involved in this framework?

Passive - Use Standards

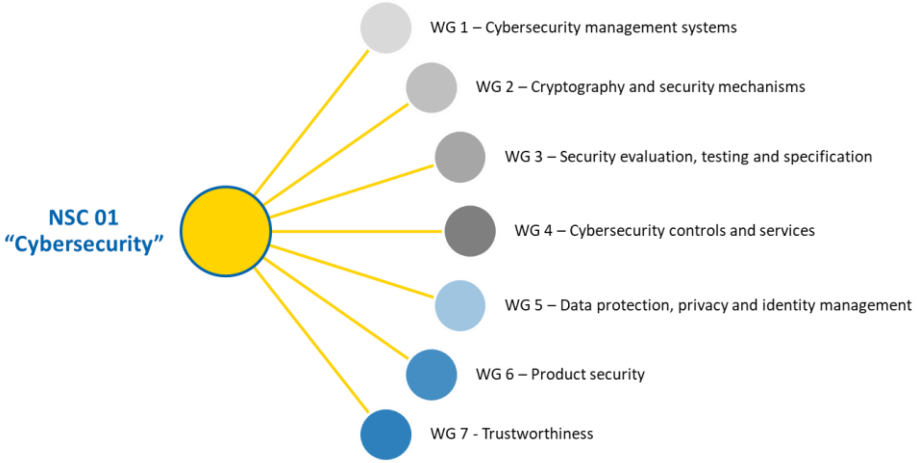
ILNAS eShop

Reading stations



Active - Participate in Standards' development

Become a national delegate in standardization



NSC 01 "Cybersecurity"

- WG 1 – Cybersecurity management systems
- WG 2 – Cryptography and security mechanisms
- WG 3 – Security evaluation, testing and specification
- WG 4 – Cybersecurity controls and services
- WG 5 – Data protection, privacy and identity management
- WG 6 – Product security
- WG 7 - Trustworthiness

CONTENT

I - PRESENTATION OF ILNAS AND ANEC EIG

II - PRESENTATION OF THE NATIONAL STANDARDS BODY

III - PARTICIPATION IN TECHNICAL STANDARDIZATION

IV - WHITE PAPERS, TECHNICAL REPORTS AND GUIDES

V - RESEARCH ACTIVITIES

VI - EDUCATION ABOUT STANDARDIZATION

IV. White Papers, Technical Reports and Guides

2023 – Recent ILNAS Research activities

STANDARDIZATION

ILNAS

TECHNICAL STANDARDIZATION

QUANTUM TECHNOLOGIES

Version 1.0 · November 2023

ISBN 978-99987-869-9-8

ANEC

21/11/2023

Technical Standardization Report on Quantum Technologies

ILNAS

WHITE PAPER

DIGITAL TRUST

TRUST-ENABLING MISSIONS FOR THE DIGITAL MARKET

Version 4.0 · December 2023

14/12/2023

White Paper Digital Trust 4.0

Trust services

Cybersecurity certification

Technical Standardization

DIGITAL TRUST

CONTENT

I - PRESENTATION OF ILNAS AND ANEC EIG

II - PRESENTATION OF THE NATIONAL STANDARDS BODY

III - PARTICIPATION IN TECHNICAL STANDARDIZATION

IV - WHITE PAPERS, TECHNICAL REPORTS AND GUIDES

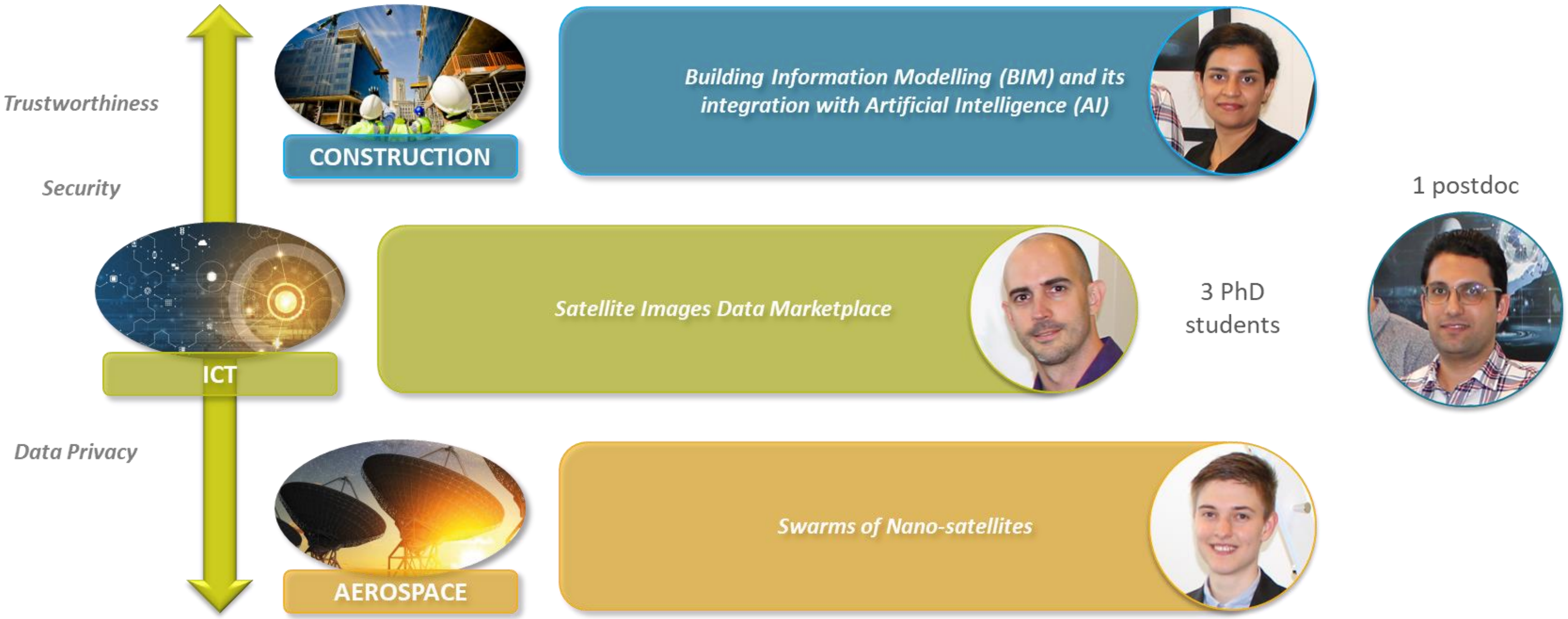
V - RESEARCH ACTIVITIES

VI - EDUCATION ABOUT STANDARDIZATION

V. Research activities

A. Research program “Technical Standardisation for Trustworthy ICT, Aerospace, and Construction” (2021-2024)

Research program “Technical Standardisation for Trustworthy ICT, Aerospace, and Construction” (2021-2024) in collaboration with the University of Luxembourg


Trustworthiness

Security

Data Privacy

CONSTRUCTION

ICT

AEROSPACE

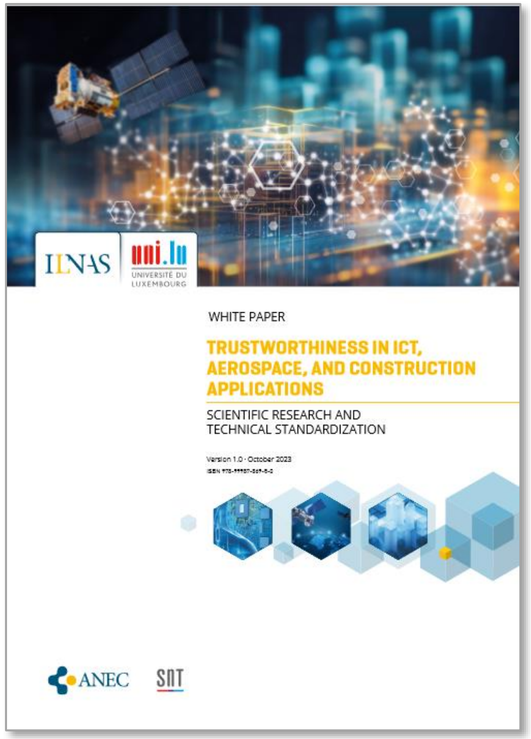
Building Information Modelling (BIM) and its integration with Artificial Intelligence (AI)

Satellite Images Data Marketplace

Swarms of Nano-satellites

3 PhD students

1 postdoc


WHITE PAPER

TRUSTWORTHINESS IN ICT, AEROSPACE, AND CONSTRUCTION APPLICATIONS

SCIENTIFIC RESEARCH AND TECHNICAL STANDARDIZATION

Version 1.0 · October 2023

ISBN 978-99987-867-6-2

https://gd.lu/8WJHCk

V. Research activities

B. Research project “cybersecurity Certification based On Risk evALuation and treatment (CORAL)” (2021-2023)

CORAL

Luxembourg House of Cybersecurity

ILNAS

ANEC

AGENCE POUR LA NORMALISATION ET L'ÉCONOMIE DE LA CONNAISSANCE

CORAL - cybersecurity Certification based On Risk evALuation and treatment

Co-financed by the Connecting Europe Facility of the European Union

The European CORAL project
Copier le li...
CORAL
cybersecurity Certification based On Risk evALuation
Regarder sur YouTube
Luxembourg House of Cybersecurity
ILNAS
ANEC

https://youtu.be/kmMHJ-lj4FY

Overview

CORAL is a European Union-funded project under CEF Telecom Call, that **aims to elaborate a toolkit and methodology to speed up the certification process in line with the EU Cybersecurity Act** or CSA (Regulation EU 2019/881). The project aims to address challenges concerning self-certification and the basic level of assurance, as well as to enhance the exchange of good practices, collaboration and information sharing related to performing evaluations in line with the CSA.

The CORAL project is being developed in a Luxembourgish context, but it aims to become known and used beyond the Luxembourg market and borders. Its target audience is primarily small and medium enterprises who have a product or service for which, they wish to assess the basic cybersecurity requirements.

CORAL website: https://coral-project.org/ Fit4CSA tool: https://fit4csa.nc3.lu/

CONTENT

I - PRESENTATION OF ILNAS AND ANEC EIG

II - PRESENTATION OF THE NATIONAL STANDARDS BODY

III - PARTICIPATION IN TECHNICAL STANDARDIZATION

IV - WHITE PAPERS, TECHNICAL REPORTS AND GUIDES

V - RESEARCH ACTIVITIES

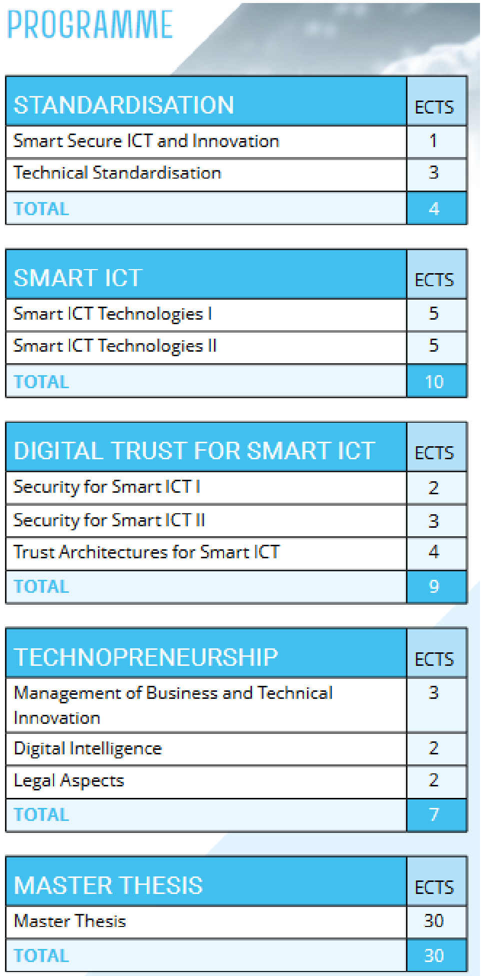
VI - EDUCATION ABOUT STANDARDIZATION

ILNAS

VI. Education about standardization

Master in Technopreneurship (MTECH)

Master MTECH – ILNAS in collaboration with the University of Luxembourg and the Chamber of Employees



PROGRAMME

STANDARDISATION	ECTS
Smart Secure ICT and Innovation	1
Technical Standardisation	3
TOTAL	4

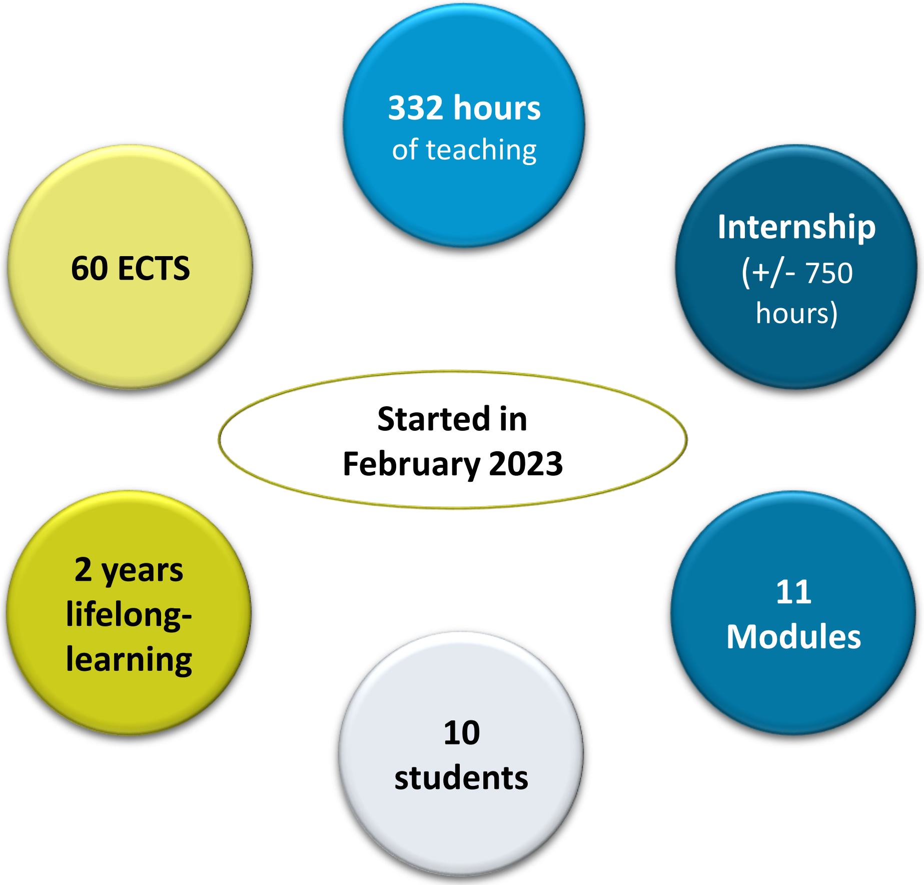
SMART ICT	ECTS
Smart ICT Technologies I	5
Smart ICT Technologies II	5
TOTAL	10

DIGITAL TRUST FOR SMART ICT	ECTS
Security for Smart ICT I	2
Security for Smart ICT II	3
Trust Architectures for Smart ICT	4
TOTAL	9

TECHNOPRENEURSHIP	ECTS
Management of Business and Technical Innovation	3
Digital Intelligence	2
Legal Aspects	2
TOTAL	7

MASTER THESIS	ECTS
Master Thesis	30
TOTAL	30

mtech.uni.lu



Started in February 2023

332 hours of teaching

Internship (+/- 750 hours)

11 Modules

10 students

2 years lifelong-learning

60 ECTS

With the support of: THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG
Ministry of the Economy

cen CENELEC ETSI

Digital Trust White Paper 4.0

TRUST-ENABLING MISSIONS FOR THE DIGITAL MARKET

Introduction

14th December 2023

Mr. Alain Wahl
Chef du *Département de la Confiance Numérique - ILNAS*

ILNAS

I. Digital Trust Department

Missions

- **National supervisory body for**
  - Trust service providers
  - Digitisation or e-archiving service providers (PSDCs – « Prestataires de Services de Dématérialisation ou de Conservation »)
- **Management and publication of Luxembourg’s trusted list**
- **Member of the European Cybersecurity Certification Group (‘ECCG’) and National cybersecurity certification authority (‘NCCA’)**
- **Promotion of good practices**
- **National participant in the *European Multistakeholder platform on ICT standardisation***

CC EUCC EUCS EU5G

Find more information:

❑ News and newsletters

❑ DLH trainings, Master in Technopreneurship

❑ https://portail-qualite.public.lu

European Commission

ROLLING PLAN FOR ICT STANDARDISATION 2023

I. Digital Trust Department

Objective

Strengthen the national and EU Single Market by boosting TRUST and CONVENIENCE in secure and seamless cross-border electronic transactions.

Trust services

Ensure a level playing field for the security of trust services

- ➢ Contributing to the protection of users
- ➢ Contributing to the functioning of the EU internal market (Recital (36) eIDAS Regulation)

E-archiving services

Guarantee that the dematerialization and preservation process of documents meets specific technical and organizational requirements based on ISO/IEC 27001

- ➢ Ensure confidentiality, integrity, availability (ISO/IEC 27001)
- ➢ Authenticity, trustworthiness, and operability
  for digitized or preserved documents

Cybersecurity certification

Ensure a level playing field for the certification of
ICT products, ICT services and ICT processes

I. Digital Trust Department

Publications

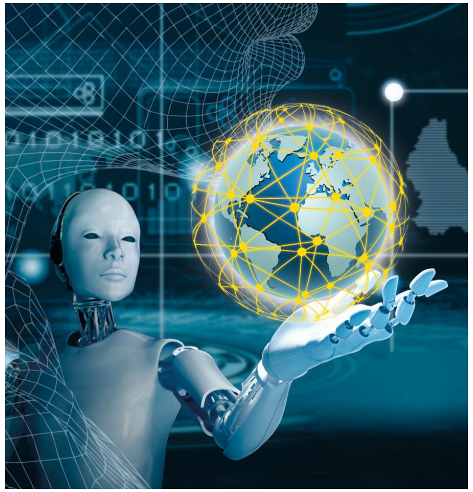
1. Introduction
2. Electronic identification and electronic signatures
3. E-archiving and dematerialization
4. Cybersecurity certification
5. Technical standardization

I. Digital Trust Department

Outlook

eIDAS revision => eIDAS 2

- European Digital Identity Wallet
- *Electronic archiving services*
- *Electronic ledgers*
- *Management of remote electronic signature devices*
- *Electronic attestation of attributes*



Cyber Resilience Act

- *Proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements*

AI Act

- *Proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on AI*

ILNAS

Digital Trust White Paper 4.0

TRUST-ENABLING MISSIONS FOR THE DIGITAL MARKET

Electronic identification and electronic signatures

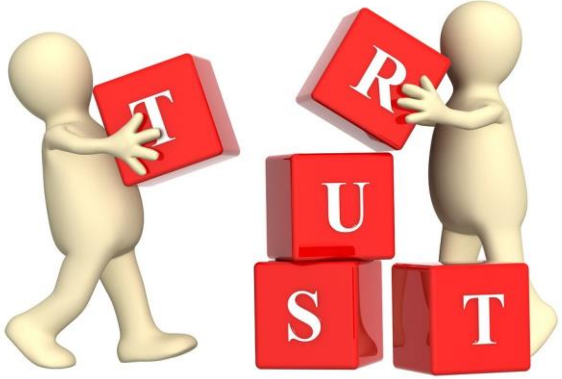
14th December 2023

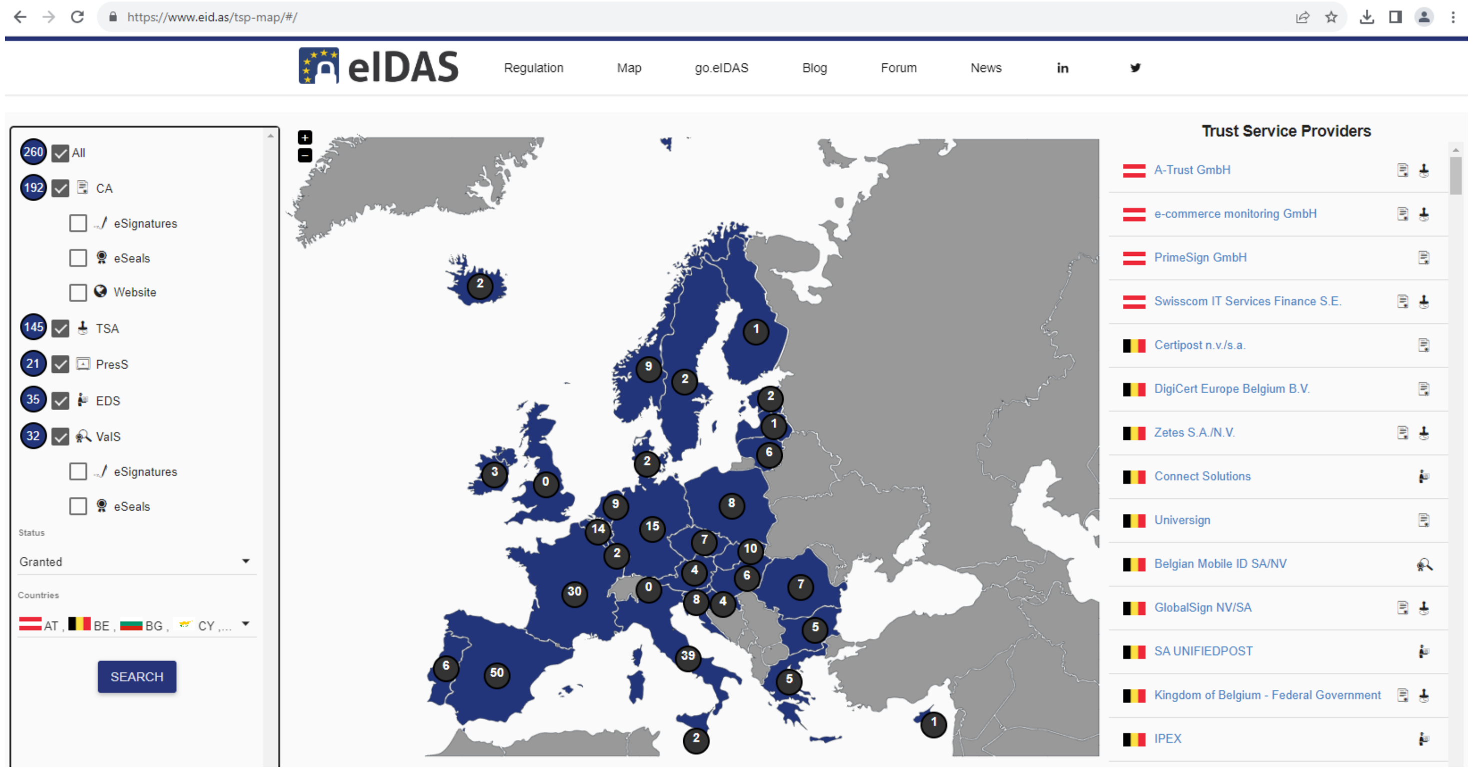
Mr. Jean-François Gillet
Chargé de mission – *Département Confiance Numérique - ILNAS*

I. eIDAS REGULATION

Regulation (EU) No 910/2014 on electronic identification and trust services

Strengthen the national and EU Single Market by boosting **TRUST** and **CONVENIENCE** in secure and seamless cross-border electronic transactions





260 ☑ All

192 ☑ CA

- □ eSignatures
- □ eSeals
- □ Website

145 ☑ TSA

21 ☑ PresS

35 ☑ EDS

32 ☑ ValS

- □ eSignatures
- □ eSeals

Status: Granted

Countries: AT , BE , BG , CY ,...

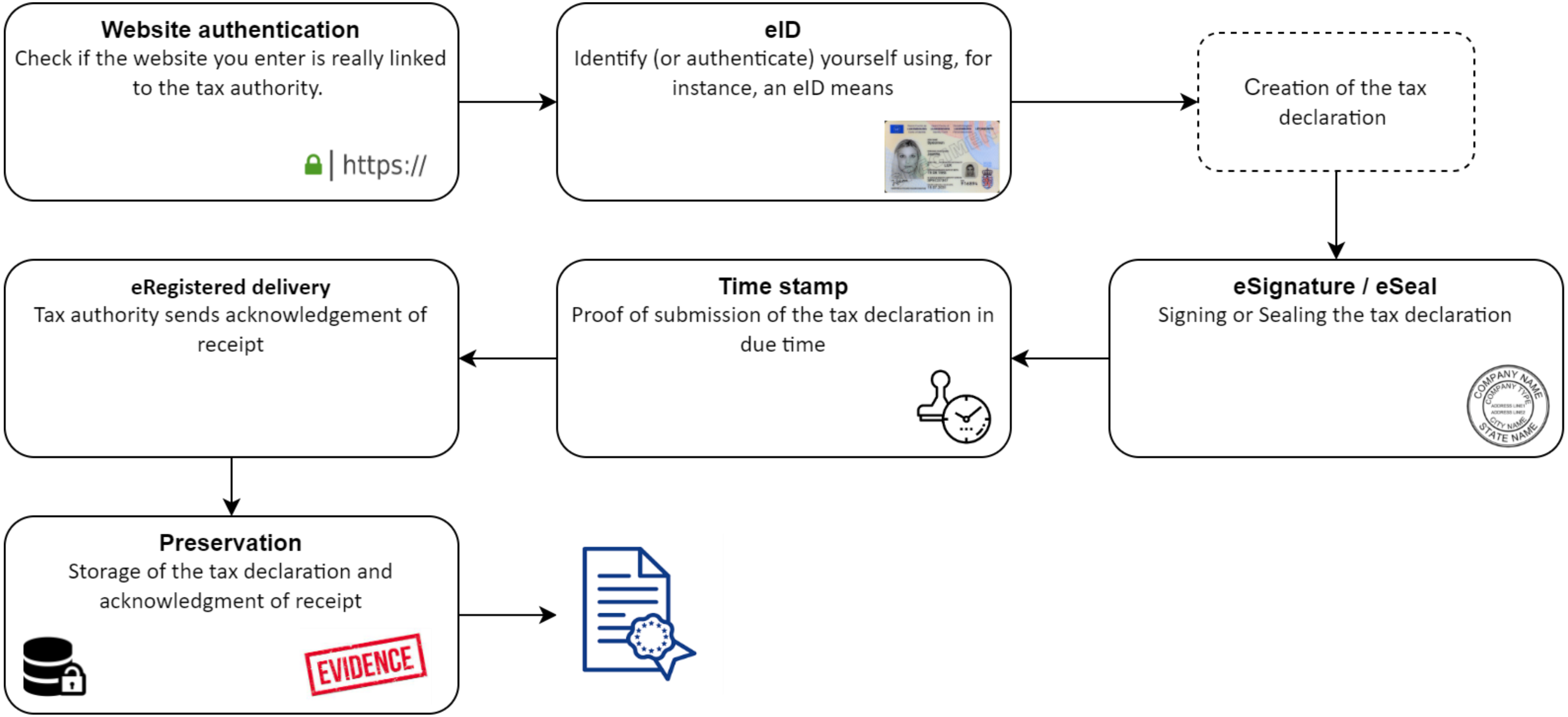
SEARCH

Trust Service Providers

- A-Trust GmbH
- e-commerce monitoring GmbH
- PrimeSign GmbH
- Swisscom IT Services Finance S.E.
- Certipost n.v./s.a.
- DigiCert Europe Belgium B.V.
- Zetes S.A./N.V.
- Connect Solutions
- Universign
- Belgian Mobile ID SA/NV
- GlobalSign NV/SA
- SA UNIFIEDPOST
- Kingdom of Belgium - Federal Government
- IPEX

I. eIDAS REGULATION

Use case – Tax declaration



Website authentication
Check if the website you enter is really linked to the tax authority.

eID
Identify (or authenticate) yourself using, for instance, an eID means

Creation of the tax declaration

eSignature / eSeal
Signing or Sealing the tax declaration

Time stamp
Proof of submission of the tax declaration in due time

eRegistered delivery
Tax authority sends acknowledgement of receipt

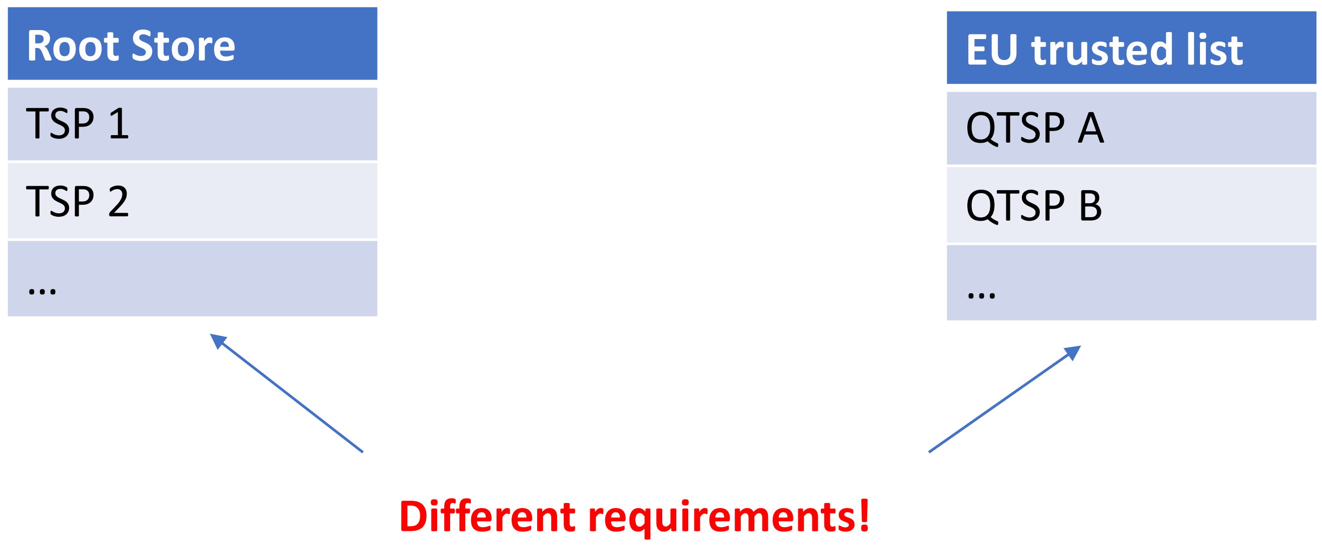
Preservation
Storage of the tax declaration and acknowledgment of receipt

I. eIDAS REGULATION

Website authentication certificate (WAC) and Qualified website authentication certificate (QWAC)

Browser:

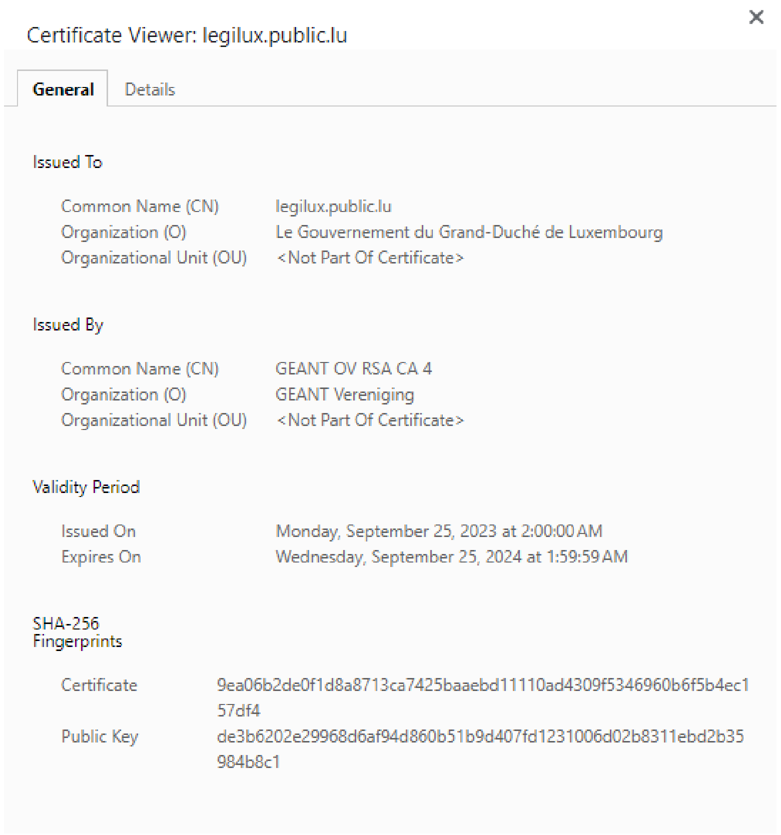
Supervisory bodies of EU Member States:



Root Store
TSP 1
TSP 2
…

EU trusted list
QTSP A
QTSP B
…

Different requirements!



Certificate Viewer: legilux.public.lu

Issued To

Common Name (CN)	legilux.public.lu
Organization (O)	Le Gouvernement du Grand-Duché de Luxembourg
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	GEANT OV RSA CA 4
Organization (O)	GEANT Vereniging
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Monday, September 25, 2023 at 2:00:00 AM
Expires On	Wednesday, September 25, 2024 at 1:59:59 AM

SHA-256 Fingerprints

Certificate	9ea06b2de0f1d8a8713ca7425baaebd11110ad4309f5346960b6f5b4ec157df4
Public Key	de3b6202e29968d6af94d860b51b9d407fd1231006d02b8311ebd2b35984b8c1

- **Qualified website authentication certificate (QWAC)**
  - ○ *"a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV"* (Article 3(39) eIDAS)

I. eIDAS REGULATION

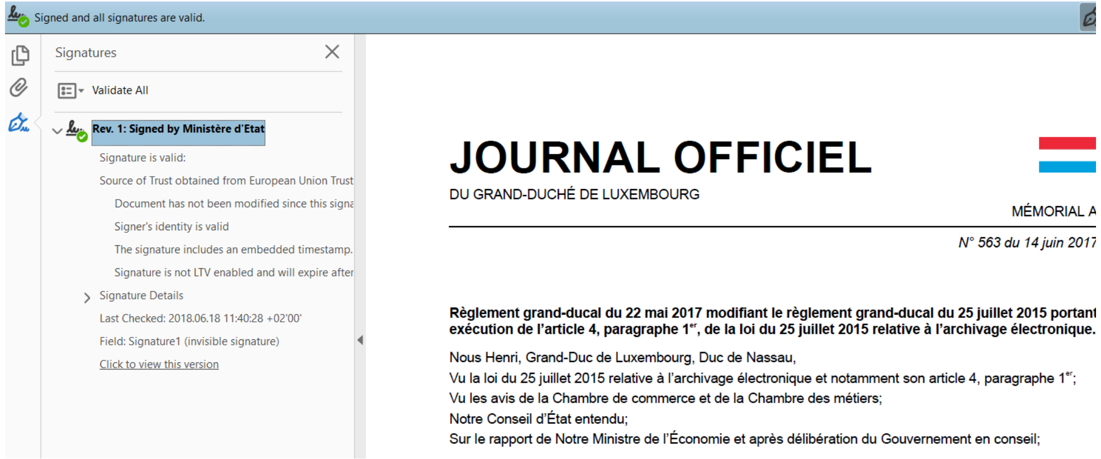
Certificates for electronic seals vs Certificates for electronic signatures

- Electronic **seal**: *"data in electronic form, which is attached to or logically associated with other data in electronic form **to ensure the latter's origin and integrity**;"* (Article 3 (25) eIDAS)

- Certificate for electronic **seal**: *"an electronic attestation that links electronic seal validation data to a **legal person** and confirms the name of that person;"* (Article 3 (29) eIDAS)

e-signature
used by a natural person to ***sign***

	Certificates for eSignatures	Certificates for eSeals
Can be issued to	Natural persons	Legal persons
Usage	Sign data	Ensure integrity and authenticity of data
Use case	Contracts	Invoices



Signed and all signatures are valid.

Signatures

Validate All

Rev. 1: Signed by Ministère d'Etat

Signature is valid:

Source of Trust obtained from European Union Trust

Document has not been modified since this signa

Signer's identity is valid

The signature includes an embedded timestamp.

Signature is not LTV enabled and will expire after

Signature Details

Last Checked: 2018.06.18 11:40:28 +02'00'

Field: Signature1 (invisible signature)

Click to view this version

JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 563 du 14 juin 2017

Règlement grand-ducal du 22 mai 2017 modifiant le règlement grand-ducal du 25 juillet 2015 portant exécution de l'article 4, paragraphe 1er, de la loi du 25 juillet 2015 relative à l'archivage électronique.

Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau,

Vu la loi du 25 juillet 2015 relative à l'archivage électronique et notamment son article 4, paragraphe 1er;

Vu les avis de la Chambre de commerce et de la Chambre des métiers;

Notre Conseil d'État entendu;

Sur le rapport de Notre Ministre de l'Économie et après délibération du Gouvernement en conseil;

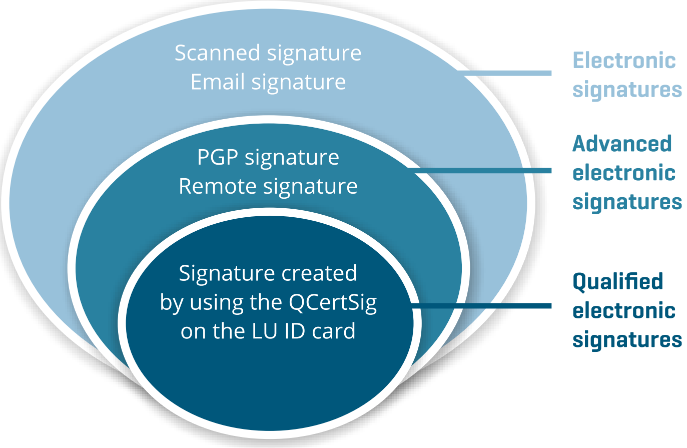
Source: https://legilux.public.lu/eli/etat/leg/rgd/2017/05/22/a563/jo

I. eIDAS REGULATION

Electronic signatures

- Different categories of electronic signatures
  - **Electronic signature**
  - **Advanced electronic signature:**
    - ✓ **uniquely** linked to the signatory;
    - ✓ capable of **identifying** the signatory;
    - ✓ created using electronic signature creation data that the signatory can, *with a high level of confidence*, use under his **sole control**; and
    - ✓ it is linked to the data signed therewith in such a way that any subsequent **change in the data is detectable**.
  - **Qualified electronic signature:** an **advanced electronic signature** that is
    - ✓ created by a **qualified signature creation device** (QSigCD)
    - ✓ based on a **qualified certificate for electronic signatures** (QCertSig)

signatures (QCertSig) which contains: **Name of the user,** Name of the QTSP, Validity period, **Public key ,** Indication of "**qualified**" certificate, Advanced electronic signature of the **QTSP**



Scanned signature
Email signature

PGP signature
Remote signature

Signature created
by using the QCertSig
on the LU ID card

Electronic signatures

Advanced electronic signatures

Qualified electronic signatures

I. eIDAS REGULATION

Electronic time stamps, time-stamp protocol and qualified electronic time stamps

- Electronic time stamp: “*data in electronic form which* ***binds*** *other* ***data*** *in electronic form* ***to*** *a particular* ***time*** *establishing evidence that the latter data existed at that time;*” (Article 3 (33) eIDAS)
- **Qualified** electronic time stamp (Art. 41(1) eIDAS):
  - time stamped **data cannot be changed** undetectably,
  - based on an **accurate time source** linked to Coordinated Universal Time (UTC), and
  - **signed** or **sealed** with an advanced electronic signature resp. an advanced electronic seal of the QTSP

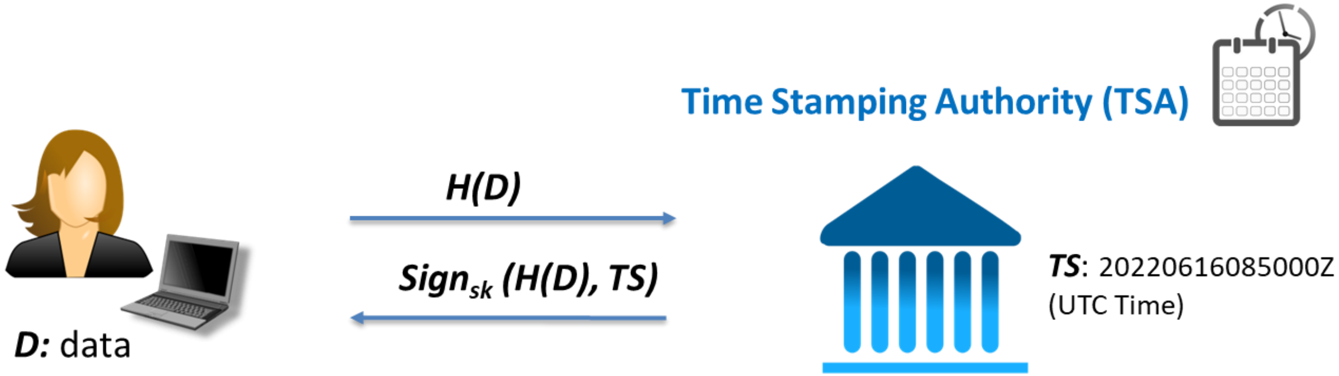
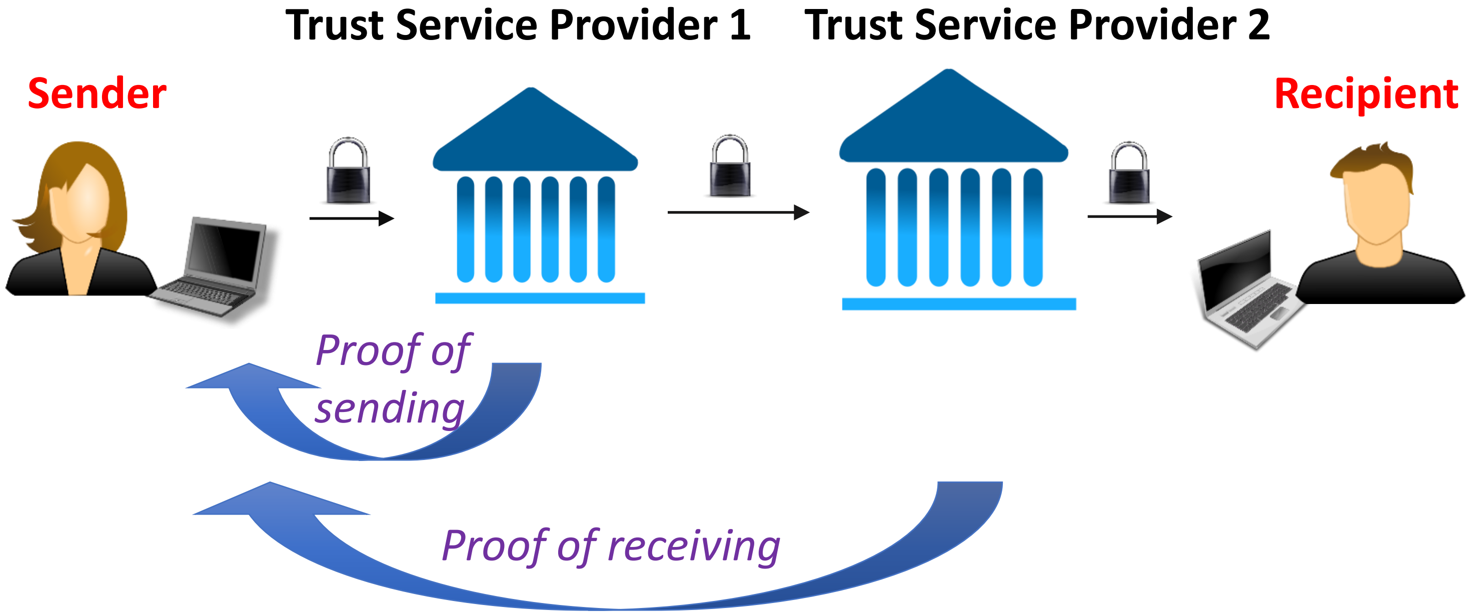


Figure: Time-stamp protocol (IETF RFC 3161)

I. eIDAS REGULATION

eRegistered Delivery Services



- Requirements for **all** trust service providers (TSPs):
  - Notification of security breaches to ILNAS (Art. 19(2))
- Requirements for **qualified** trust service providers (**QTSPs**) (Art. 24):
  - **Verify the identity** of the natural or legal person who requests a **qualified** certificate,
  - Employ staff who possess the necessary qualifications,
  - **Use trustworthy systems and products**
  - Take appropriate measures against forgery and theft of data,
  - Have an up-to-date **termination plan**,
  - Ensure lawful processing of personal data in accordance with the GDPR,…
- **QTSPs: Supervision by ILNAS**
  - Initial audit, notification and conformity assessment report
  - Surveillance audit (after 1 year)
  - Reassessment audit (after 2 years)

I. eIDAS REGULATION

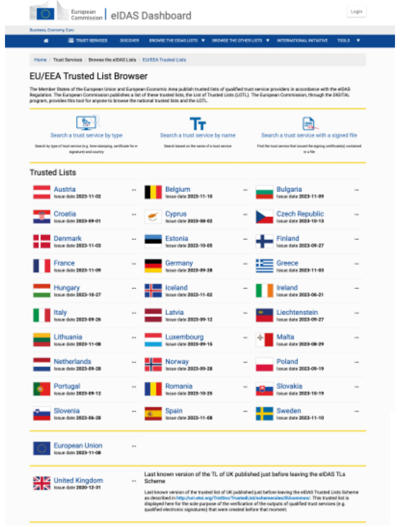
Legal effects (eSignatures, eSeals, eTimeStamps and eRegistered Delivery Services)

	eSignatures	eSeals	eTimeStamp
Non-discrimination	Yes	Yes	Yes
Legal effect of **qualified** type	**Equivalent legal effect of handwritten signatures**	Presumption of **integrity** and of **correctness of the origin** of the data	▪ Presumption of **accuracy of the date and the time** it indicates ▪ Presumption of the **integrity of the data** to which the date and time are bound
Cross-border recognition within EU	Yes, for **qualified** eSignatures	Yes, for **qualified** eSeals	Yes, for **qualified** eTimeStamps

	eRegistered Delivery Services	Qualified eRegistered Delivery Services
Non-discrimination	Yes (for sent and received data)	Yes (for sent and received data)
Legal effect	No	▪ Presumptions of the **integrity of the data**, the sending of that data by the **identified sender**, the receipt of the data by the **identified addressee** and the **accuracy of the date and time** of the data. ▪ **Equivalent legal effect of registered postal mail** 🇱🇺
Cross-border recognition within EU	No	Yes

I. eIDAS REGULATION

Role of ILNAS



Home / Trust Services / Browse the eIDAS Lists / EU/EEA Trusted Lists

EU/EEA Trusted List Browser

The Member States of the European Union and European Economic Area publish trusted lists of qualified trust service providers in accordance with the eIDAS Regulation. The European Commission publishes a list of these trusted lists, the List of Trusted Lists (LOTL). The European Commission, through the DIGITAL program, provides this tool for anyone to browse the national trusted lists and the LOTL.

Search a trust service by type
Search by type of trust service (e.g. time-stamping, certificate for e-signature) and country

Search a trust service by name
Search based on the name of a trust service

Search a trust service with a signed file
Find the trust service that issued the signing certificate(s) contained in a file

Trusted Lists

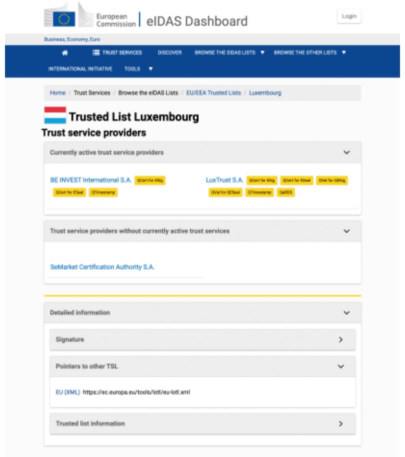
Austria Issue date 2023-11-02	Belgium Issue date 2023-11-10	Bulgaria Issue date 2023-11-09
Croatia Issue date 2023-09-01	Cyprus Issue date 2023-08-02	Czech Republic Issue date 2023-10-13
Denmark Issue date 2023-11-03	Estonia Issue date 2023-10-05	Finland Issue date 2023-09-27
France Issue date 2023-11-09	Germany Issue date 2023-09-28	Greece Issue date 2023-11-03
Hungary Issue date 2023-10-27	Iceland Issue date 2023-11-02	Ireland Issue date 2023-06-21
Italy Issue date 2023-09-26	Latvia Issue date 2023-09-12	Liechtenstein Issue date 2023-09-27
Lithuania Issue date 2023-11-08	Luxembourg Issue date 2023-09-15	Malta Issue date 2023-08-29
Netherlands Issue date 2023-09-28	Norway Issue date 2023-09-28	Poland Issue date 2023-09-19
Portugal Issue date 2023-09-12	Romania Issue date 2023-10-25	Slovakia Issue date 2023-10-19
Slovenia Issue date 2023-06-28	Spain Issue date 2023-11-08	Sweden Issue date 2023-11-10

European Union
Issue date 2023-11-08

United Kingdom
Issue date 2020-12-31

Last known version of the TL of UK published just before leaving the eIDAS TLs Scheme

Last known version of the trusted list of UK published just before leaving the eIDAS Trusted Lists Scheme as described in http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon/. This trusted list is displayed here for the sole purpose of the verification of the outputs of qualified trust services (e.g. qualified electronic signatures) that were created before that moment.



Home / Trust Services / Browse the eIDAS Lists / EU/EEA Trusted Lists / Luxembourg

Trusted List Luxembourg

Trust service providers

Currently active trust service providers

BE INVEST International S.A. QCert for ESig QCert for ESeal QTimestamp

LuxTrust S.A. QCert for ESig QCert for ESeal QVal for QESig QVal for QESeal QTimestamp QeRDS

Trust service providers without currently active trust services

SeMarket Certification Authority S.A.

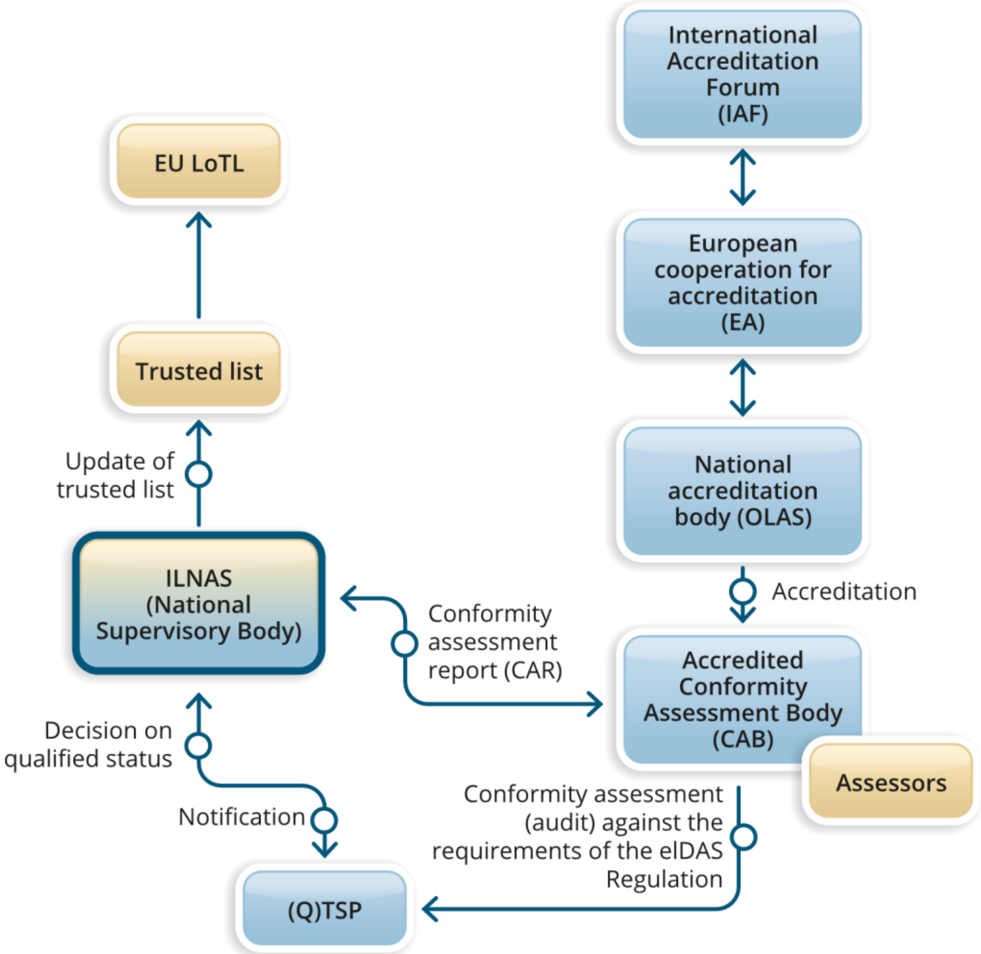
Detailed information

Signature

Pointers to other TSL

EU (XML) https://ec.europa.eu/tools/lotl/eu-lotl.xml

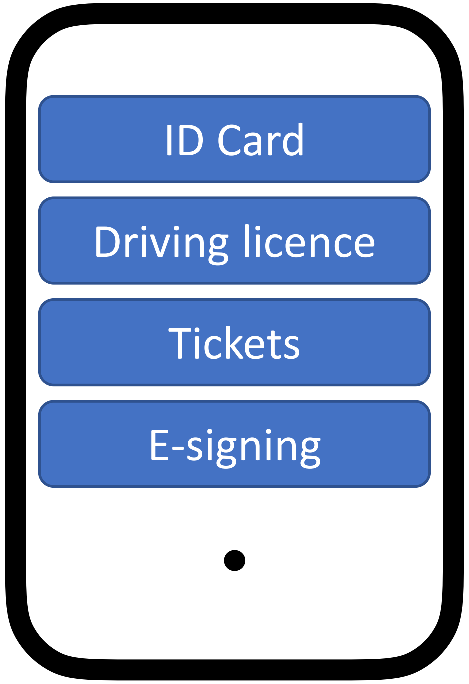
Trusted list information


International Accreditation Forum (IAF)
European cooperation for accreditation (EA)
National accreditation body (OLAS)
Accreditation
Accredited Conformity Assessment Body (CAB)
Assessors
EU LoTL
Trusted list
Update of trusted list
ILNAS (National Supervisory Body)
Conformity assessment report (CAR)
Decision on qualified status
Notification
Conformity assessment (audit) against the requirements of the eIDAS Regulation
(Q)TSP

I. eIDAS REGULATION

The revision of the eIDAS Regulation (eIDAS2)

- **eIDAS 2.0 (Regulation) (2023):**
  - Further trust services:
    - ✓ (qualified) electronic archiving,
    - ✓ (qualified) electronic attestation of attributes,
    - ✓ the management of remote qualified electronic signature and seal creation devices,
    - ✓ (qualified) electronic ledgers.
  - “EU Digital Identity Wallet”



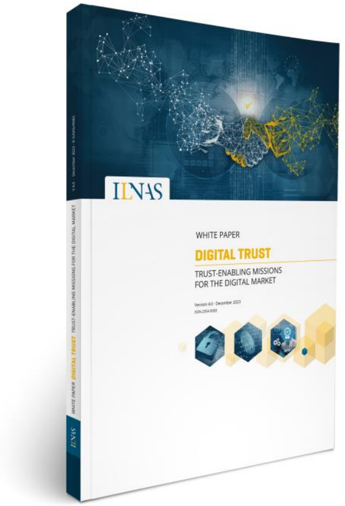
ID Card

Driving licence

Tickets

E-signing

For more details



Chapter 2 of the Digital Trust White Paper 4.0

ILNAS

Digital Trust White Paper 4.0

TRUST-ENABLING MISSIONS FOR THE DIGITAL MARKET

E-archiving and Dematerialization

14th December 2023

Dr. Michel Ludwig

PSDC Supervision Manager - ILNAS

Electronic archiving

- Goal:

  preserve **integrity**, **confidentiality**, **availability** of digital documents over extended periods of time

- Legal value of archived electronic documents:

  Law of 25 July 2015 on electronic archiving

- Revolutionary aspect of the e-archiving framework in Luxembourg:

  digitization of analog documents, preserving their probative value

INTRODUCTION

Digitization

- Goal: **transform analog documents** into **digital documents**
- Typically: scanning of paper documents
- Reduce operational costs & provide additional services:
  - large, physical archives not needed anymore
  - mitigation of threats: e.g. theft / destruction of analog documents that possess legal value
  - Easy access to digital documents, even from remote locations
  - Searching through documents possible

II LAW OF 25 JULY 2015 ON ELECTRONIC ARCHIVING

Law of 25 July 2015 on electronic archiving

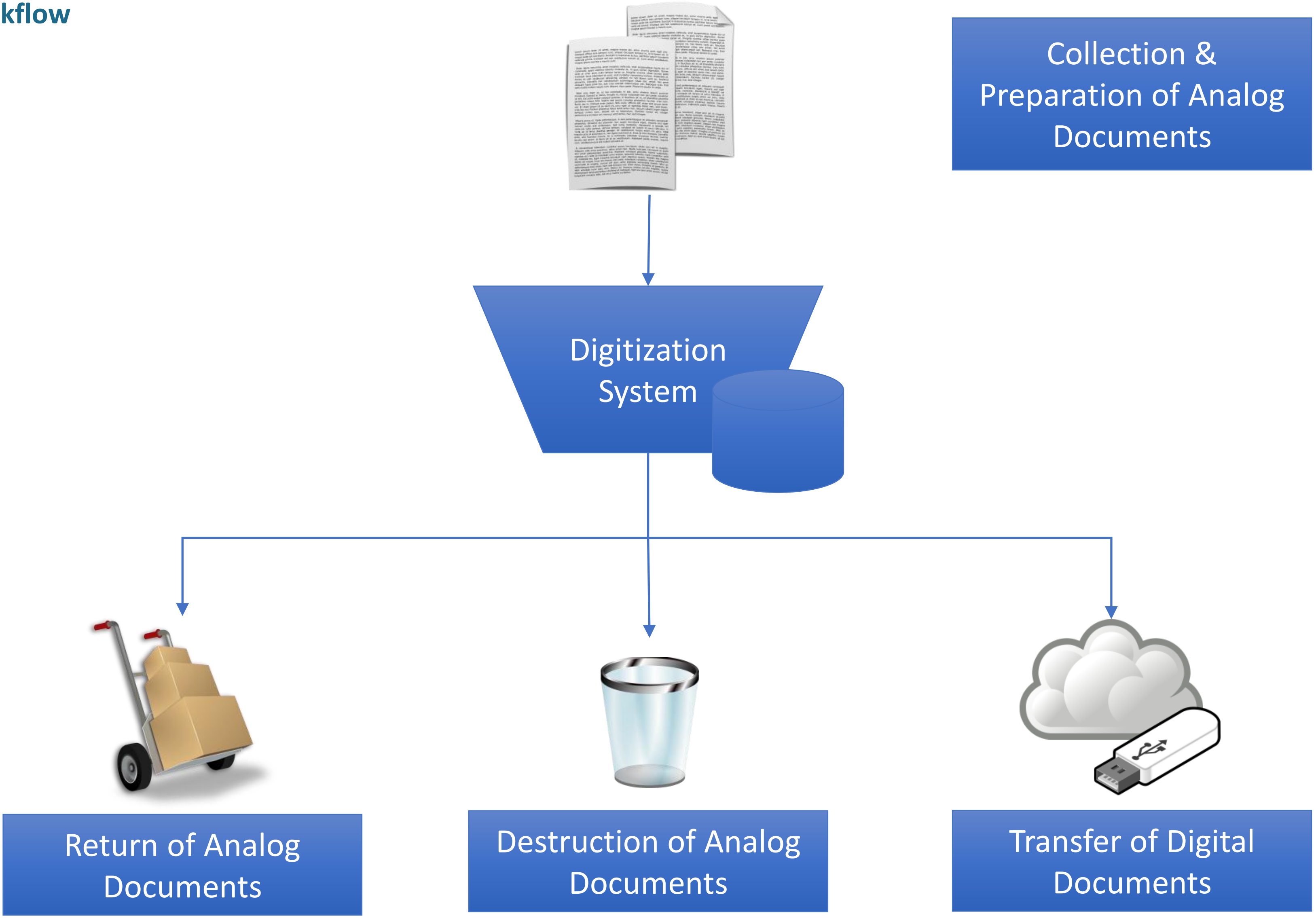
- introduces the **main legal context** concerning electronic archiving in Luxembourg, covering
  - digitization of analog documents
  - archiving of digital documents

- Defines conditions under which digital documents **benefit from a presumption of conformity** w.r.t. originals:
  - analog document ⟷ digitized version
  - digital document to be archived ⟷ digital archive

- Technical requirements regarding digitization / electronic archiving defined in the national standard

ILNAS 106:2022 - Archivage électronique - Référentiel d’exigences pour la certification des prestataires de services de dématérialisation ou de conservation (PSDC)

Digitization Workflow



Collection & Preparation of Analog Documents

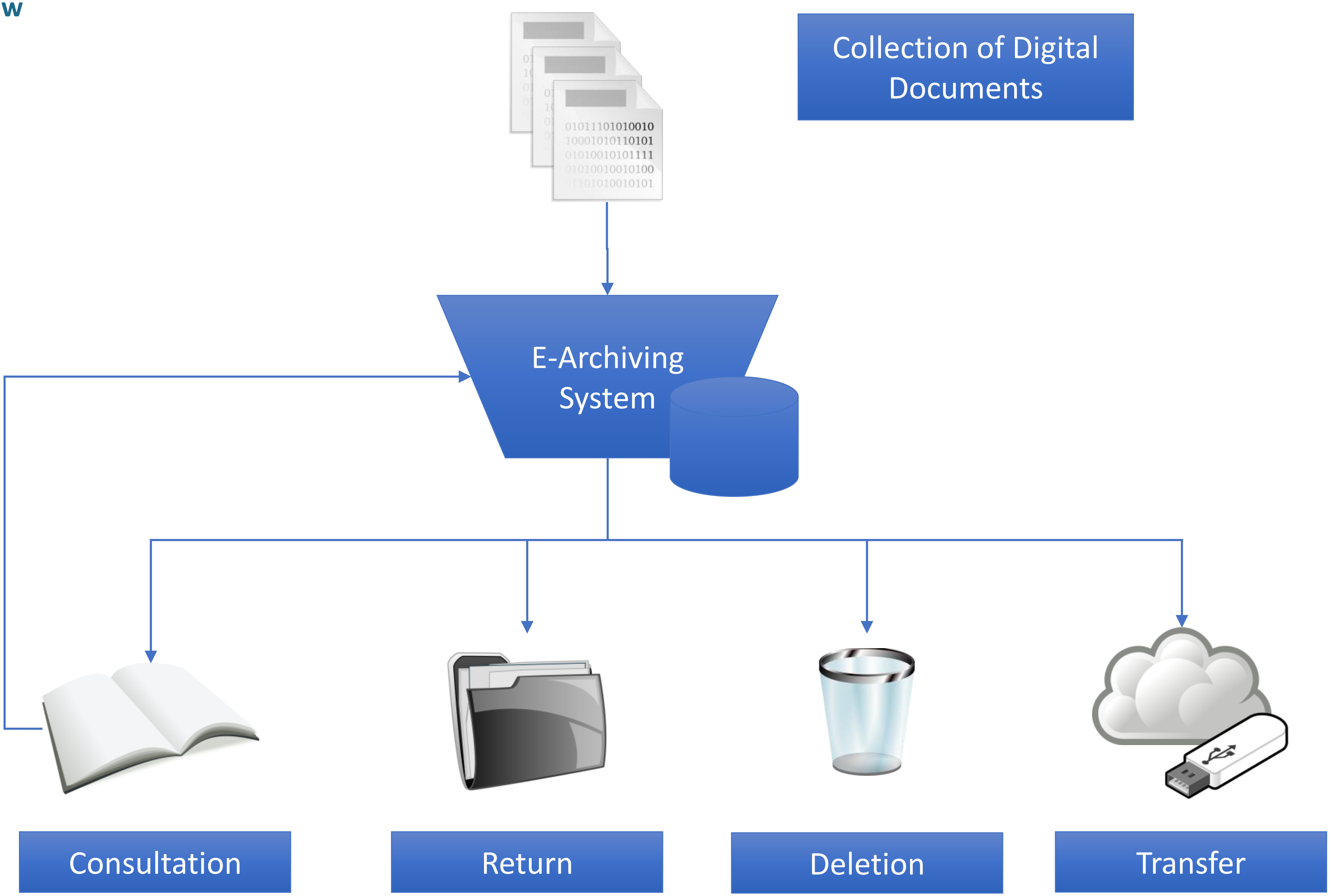
Digitization System

Return of Analog Documents

Destruction of Analog Documents

Transfer of Digital Documents

E-archiving Workflow



Law of 25 July 2015 on electronic archiving

- Introduces the legal status of

prestataire de services de dématérialisation ou de conservation (PSDC)

- i.e. “provider of digitization or e-archiving services” in English
- PSDC status granted by ILNAS only
- Organizations with PSDC status supervised by ILNAS

Documents digitized or archived by PSDCs will have the same legal value as the corresponding original documents (presumption of conformity w.r.t. the originals)!

List of PSDCs

Organization	Notification ID	PSDC Status Since	Scope
Lab Luxembourg S.A. 3, rue Dr. Elvire Engel L-8346 Grass	2016/9/001	01/02/2017	Digitization & E-archiving
Numen Europe S.A. 2, rue Edmond Reuter L-5326 Contern	2016/9/002	26/09/2017	Digitization & E-archiving
Syndicat Intercommunal de Gestion Informatique 11, rue Edmond Reuter L-5326 Contern	2017/9/005	26/02/2018	E-archiving
KPMG Services S.à.r.l. 39, avenue John F. Kennedy L-1855 Luxembourg	2017/9/004	20/08/2018	Digitization & E-archiving
Centre des technologies de l'information de l'Etat 560, rue de Neudorf L-2220 Luxembourg	2017/9/006	23/08/2018	E-archiving

(as of 14 December 2023)

https://portail-qualite.public.lu/fr/confiance-numerique/archivage-electronique/liste-psdc.html

Law of 25 July 2015 on electronic archiving

Prerequisite for PSDC status: **certification** by a conformity assessment body (CAB)

Aims of certification:

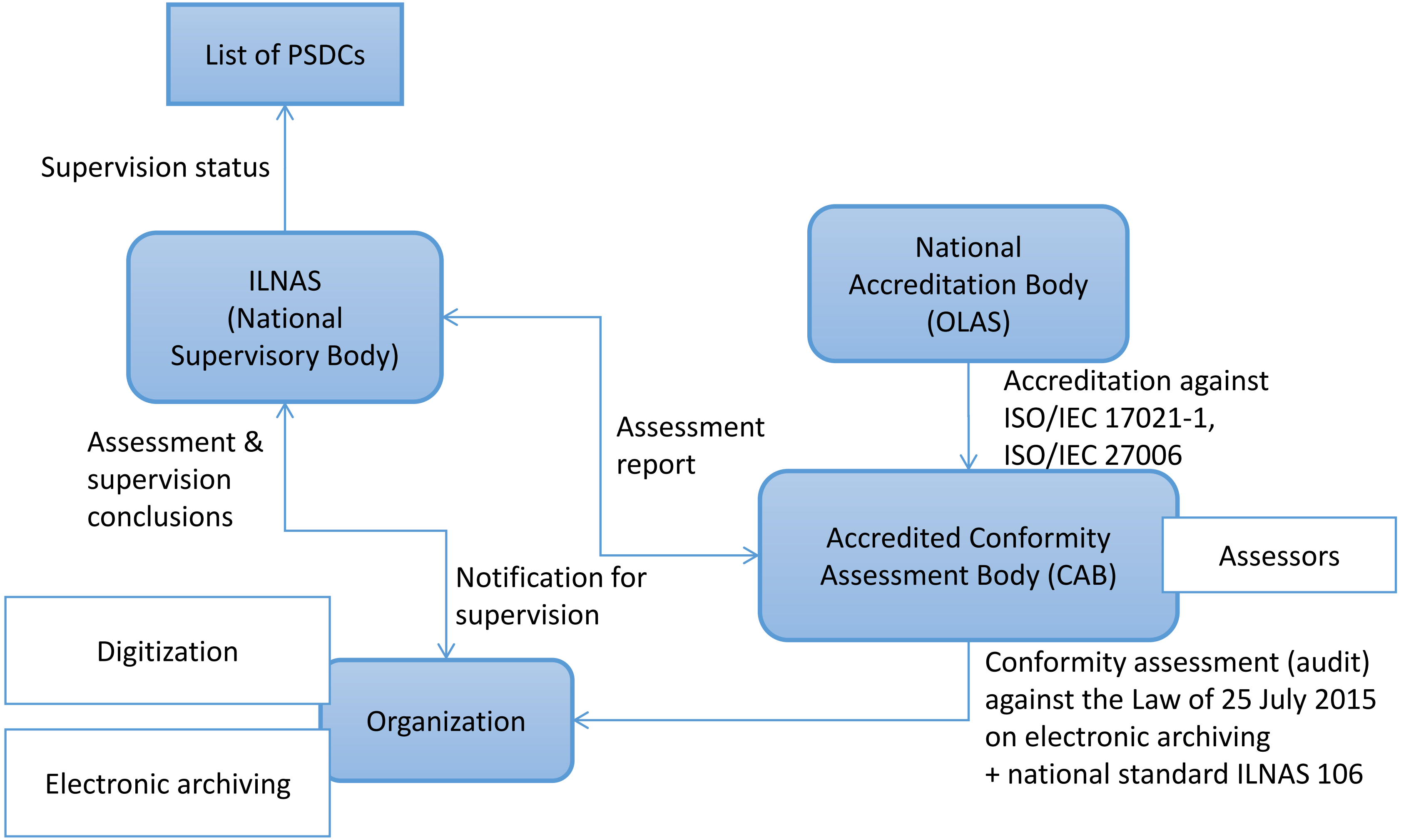
- Verify that digitization / e-archiving follows predetermined procedures
- Procedures have to respect the Law of 25 July 2015 on e-archiving + national standard ILNAS 106

Establish a trust relationship:

- External verification
- Return / transfer of digital documents or archives if a PSDC ceases its activities

Concerning analog documents, the legal context only applies to “private deeds” or to the documents referred to in Article 16 of the “Code de commerce” (accounting and supporting documents)

III ILNAS SUPERVISION SCHEME FOR PSDCS


List of PSDCs
Supervision status
ILNAS (National Supervisory Body)
National Accreditation Body (OLAS)
Accreditation against ISO/IEC 17021-1, ISO/IEC 27006
Assessment report
Assessment & supervision conclusions
Accredited Conformity Assessment Body (CAB)
Assessors
Notification for supervision
Digitization
Organization
Electronic archiving
Conformity assessment (audit) against the Law of 25 July 2015 on electronic archiving + national standard ILNAS 106

IV OVERVIEW OF THE NATIONAL STANDARD ILNAS 106:2022

National Standard ILNAS 106:2022

- developed by the technical committee ILNAS/TC 106 (founded in 2018)
- Aim: develop a national standard on digitization and e-archiving that can serve as the basis for the certification of PSDCs
- published as a national standard in July 2022
- national standard ILNAS 106:2022 is based on the international standards
  - ISO/IEC 27001:2013: Information Technology — Security Techniques — Information Security Management Systems — Requirements
  - ISO/IEC 27002:2013: Information Technology — Security Techniques — Code of Practice for Information Security Controls
  - ISO 14641: Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications
- a few additional security controls (e.g., on cryptography, regular verifications of the integrity of archived documents, etc.)

ILNAS

Institut luxembourgeois de la normalisation de l'accréditation, de la sécurité et qualité des produits et services

ILNAS 106:2022

ARCHIVAGE ÉLECTRONIQUE - RÉFÉRENTIEL D'EXIGENCES POUR LA CERTIFICATION DES PRESTATAIRES DE SERVICES DE DÉMATÉRIALISATION OU DE CONSERVATION (PSDC)

© ILNAS 2022

07/2022

Available free of charge at

https://portail-qualite.public.lu/fr/documentations/confiance-numerique/

Welcome

ILNAS

Digital Trust White Paper 4.0

TRUST-ENABLING MISSIONS FOR THE DIGITAL MARKET

Cybersecurity Certification

14th December 2023

Dr. Jean Lancrenon
Chargé de mission – *Département Confiance Numérique - ILNAS*

ILNAS

I. 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

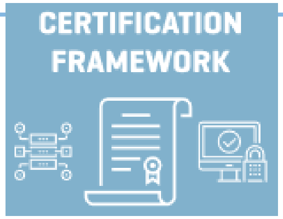
Fully entered into force on 28 June 2021

Two major parts

enisa

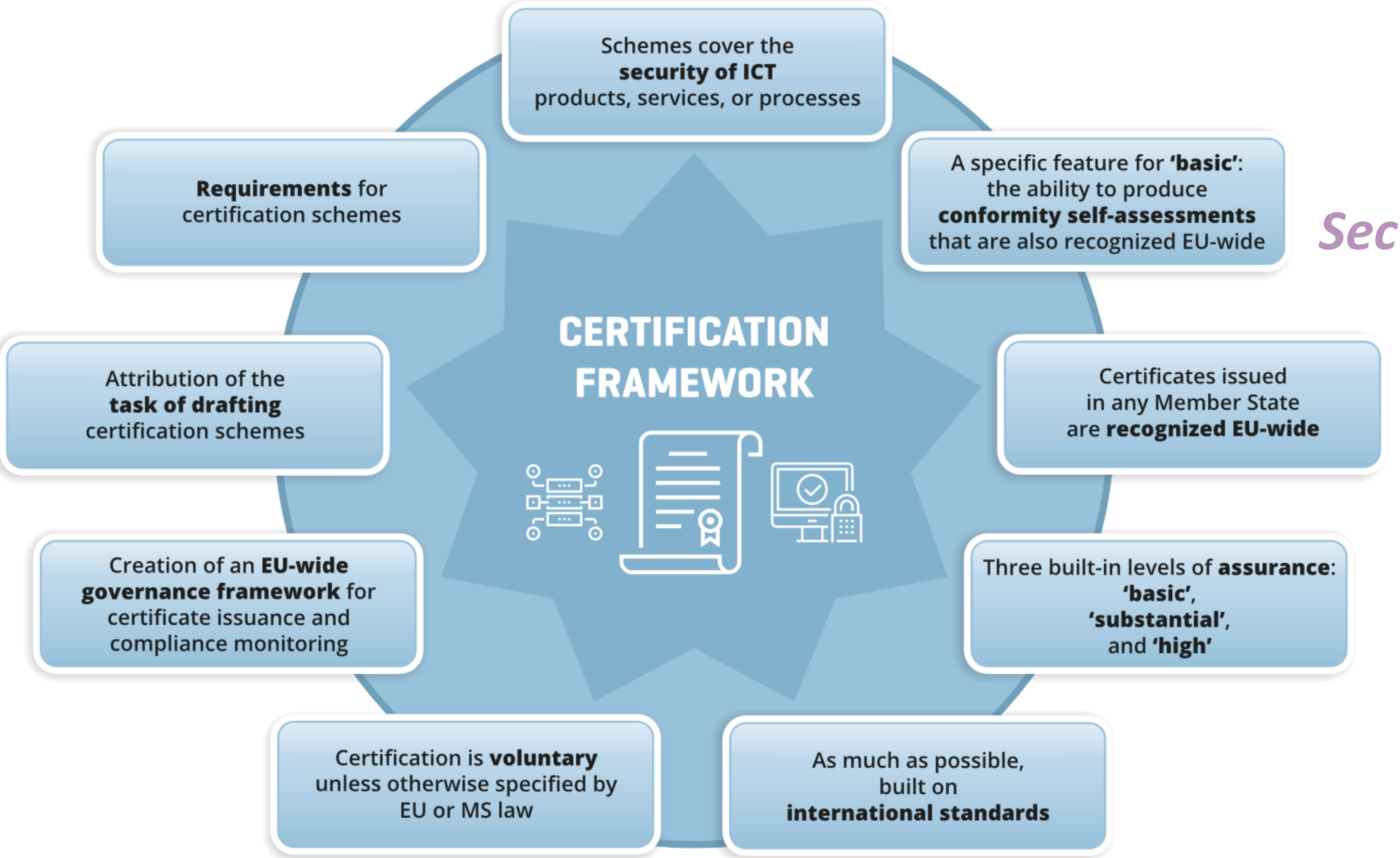
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

EU-wide cybersecurity



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

II. CSA major features



CERTIFICATION FRAMEWORK

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

A specific 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**

Certification is **voluntary** unless otherwise specified by EU or MS law

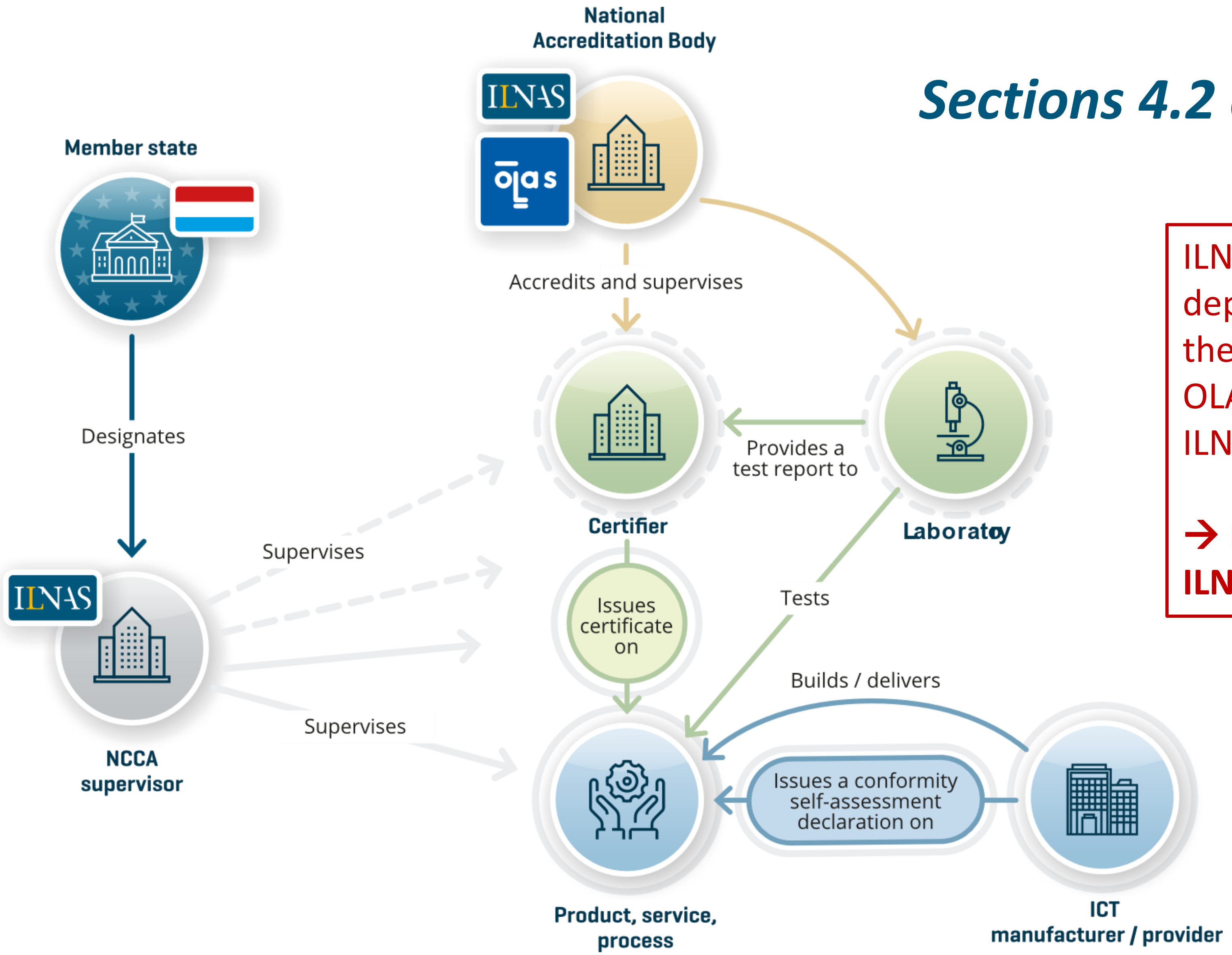
Creation of an **EU-wide governance framework** for certificate issuance and compliance monitoring

Attribution of the **task of drafting** certification schemes

Requirements for certification schemes

Section 4.1

III. The CSA Luxembourg ecosystem



Sections 4.2 and 4.4

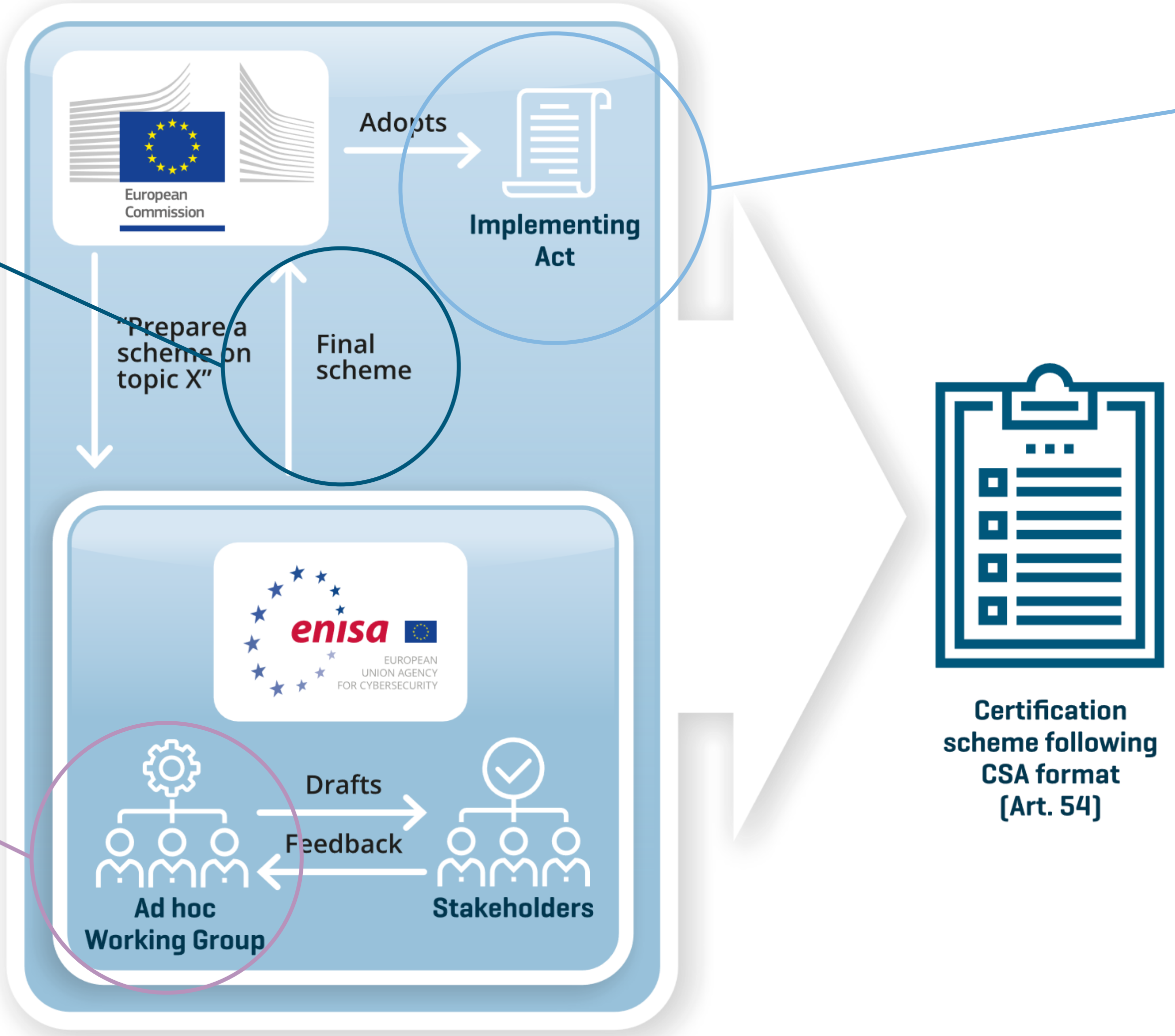
ILNAS' Digital Trust department is taking the NCCA tasks, and OLAS is also a part of ILNAS

→ Hence no plans for ILNAS to be a certifier

IV. Scheme status

EUCS is somewhere here: ongoing negotiations between COM and AHWG

EU5G is here: AHWG formed, and preparing first draft

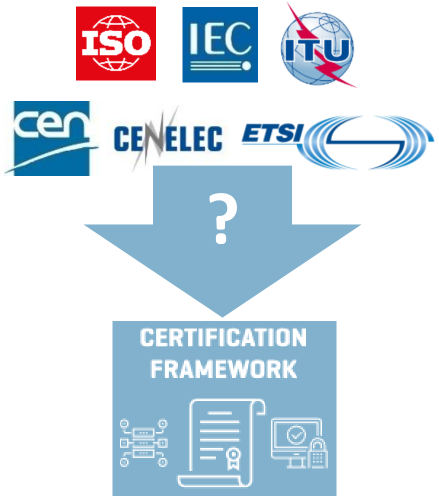

European Commission
Adopts
Implementing Act
"Prepare a scheme on topic X"
Final scheme
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
Drafts
Feedback
Ad hoc Working Group
Stakeholders
Certification scheme following CSA format (Art. 54)

EUCC is around here: Implementing Act almost ready

Section 4.2

V. Pointers to main technical standards

Which standards and for what?



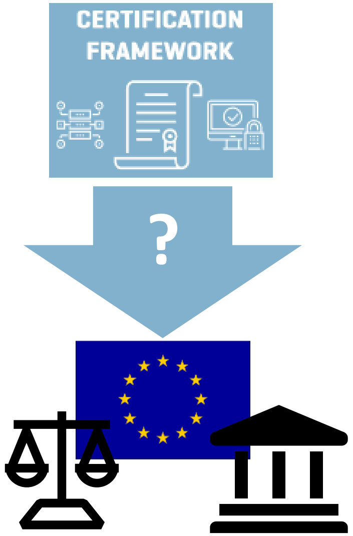
Technical requirements for the schemes themselves

All throughout, but mostly Section 4.2

Technical requirements for evaluation against the schemes

Technical requirements for evaluating laboratories/certifiers

Potential applications of the CSA elsewhere in European legislation



Section 4.3

The NIS2 Directive

The eIDAS2 Regulation

The list is certainly not exhaustive

ILNAS

DIGITAL TRUST

Section 4.4

WORK 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

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

Other activities

- Participating in the European project CORAL*

Contact info

- Jean-François GILLET and Jean LANCRENON
- CSA-matters email supervision-cybersecurite@ilnas.etat.lu
- https://portail-qualite.public.lu/fr/cybersecurity-act.html

*cybersecurity **C**ertification based **O**n **R**isk ev**AL**uation and treatment

Co-financed by the Connecting Europe Facility of the European Union

ILNAS

Digital Trust White Paper 4.0

TRUST-ENABLING MISSIONS FOR THE DIGITAL MARKET

Technical Standardization

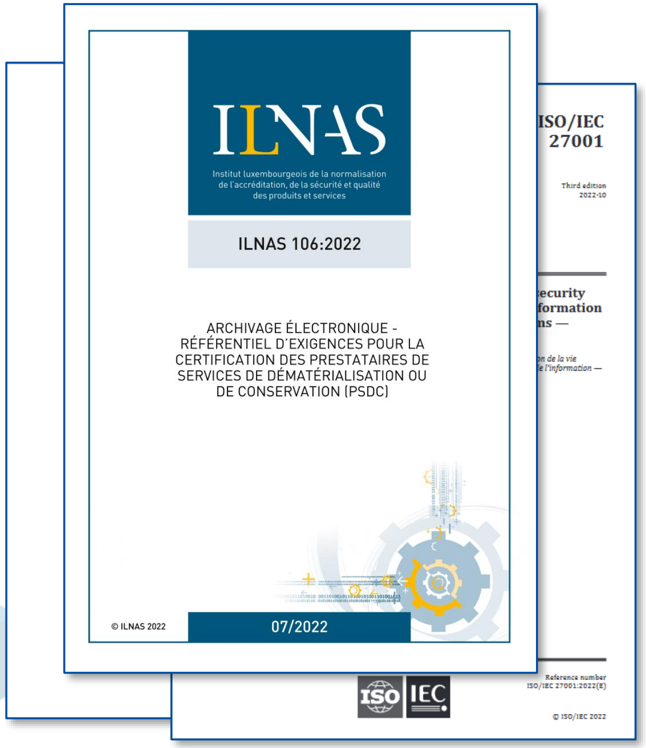
14th December 2023

Mr. Nicolas Domenjoud

Responsible "ICT & Technical Standardization" – ILNAS/OLN

I. Digital Trust and Technical Standards

E-archiving



ILNAS

Institut luxembourgeois de la normalisation de l'accréditation, de la sécurité et qualité des produits et services

ILNAS 106:2022

ARCHIVAGE ÉLECTRONIQUE - RÉFÉRENTIEL D'EXIGENCES POUR LA CERTIFICATION DES PRESTATAIRES DE SERVICES DE DÉMATÉRIALISATION OU DE CONSERVATION (PSDC)

© ILNAS 2022

07/2022

ISO/IEC 27001

Third edition 2022-10

Reference number ISO/IEC 27001:2022(E)

© ISO/IEC 2022

eIDAS

ETSI TS 119 612 V2.1.1 (2015-07)

TECHNICAL SPECIFICATION

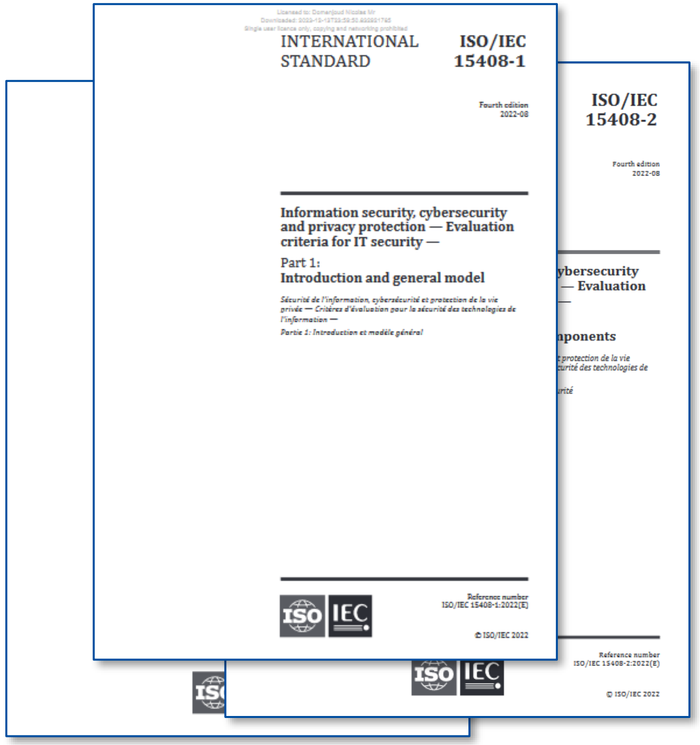
Electronic Signatures and Infrastructures (ESI); Trusted Lists

CSA

CC EUCC

EUCS

EU5G



INTERNATIONAL STANDARD

ISO/IEC 15408-1

Fourth edition 2022-08

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security —

Part 1: Introduction and general model

Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information —

Partie 1: Introduction et modèle général

Reference number ISO/IEC 15408-1:2022(E)

© ISO/IEC 2022

ISO/IEC 15408-2

Fourth edition 2022-08

Reference number ISO/IEC 15408-2:2022(E)

© ISO/IEC 2022

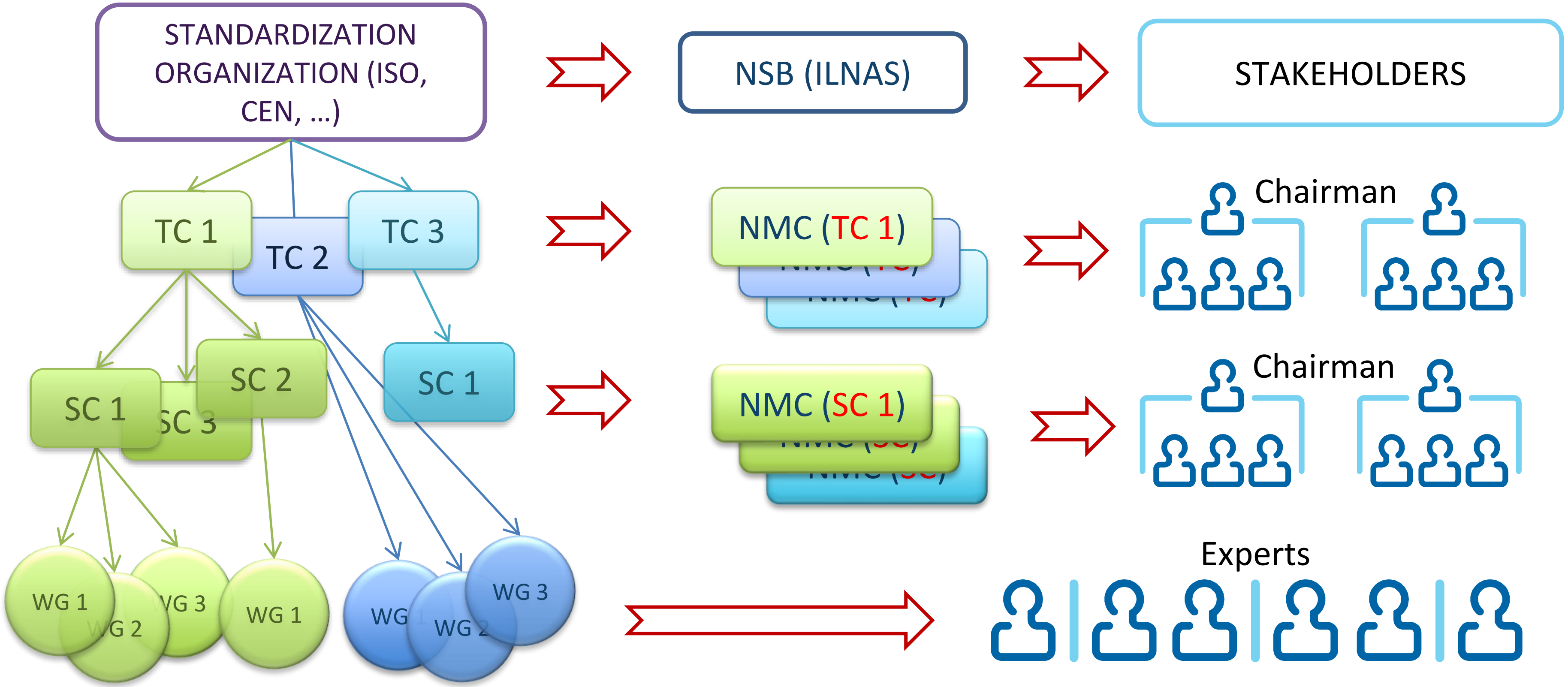
What is a Standard?

> *"[…] A technical specification, adopted by a recognized standardization body, for repeated or continuous application, with which compliance is not compulsory [...]"*

Standardization Organizations

	General Standardization	Electrotechnical Standardization	Telecommunications Standardization
International level	ISO	IEC	ITU ETSI
European level	CEN	CENELEC	
National level	ILNAS	ILNAS	ILNAS

II. What are standards and how are they developed?

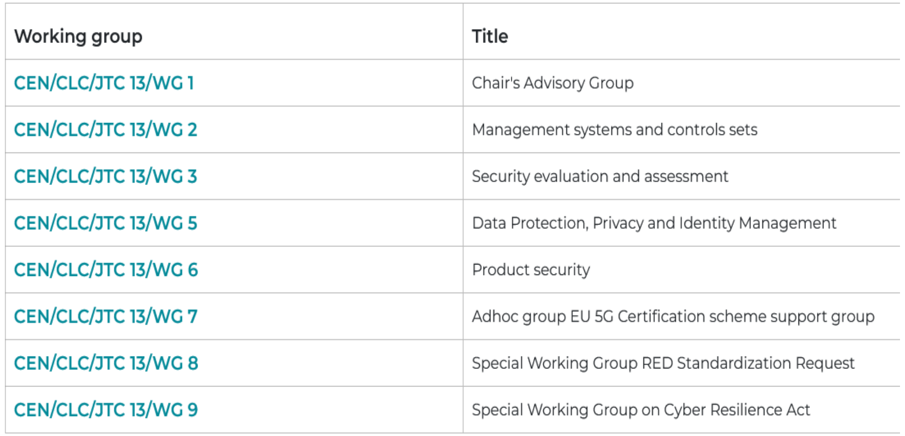


- **NSB**: National Standards Body
- **TC**: Technical Committee
- **SC**: Subcommittee - Entity established within a TC responsible for a large work program (focuses on an area of interest of the TC)
- **WG**: Working Group - Group established by a TC or SC that develops standards project(s) within the scope of activity of the TC/SC
- **NMC**: National Mirror Committee

CEN/CLC JTC 13 “Cybersecurity and Data Protection”

Scope:

- **Development of standards for cybersecurity and data protection** covering all aspects of the evolving information society including but not limited to:
  - **Management systems, frameworks, methodologies**
  - **Data protection and privacy**
  - **Services and products evaluation standards suitable for security assessment for large companies and small and medium enterprises (SMEs)**
  - **Competence requirements for cybersecurity and data protection**
  - **Security requirements, services, techniques and guidelines for ICT systems, services, networks and devices, including smart objects and distributed computing devices**
- Included in the scope is the **identification and possible adoption of documents already published or under development by ISO/IEC JTC 1 and other SDOs and international bodies** such as ISO, IEC, ITU-T, and industrial fora. Where not being developed by other SDO's, the development of cybersecurity and data protection CEN/CENELEC publications for safeguarding information such as organizational frameworks, management systems, techniques, guidelines, and products and services, including those in support of the EU Digital Single Market.

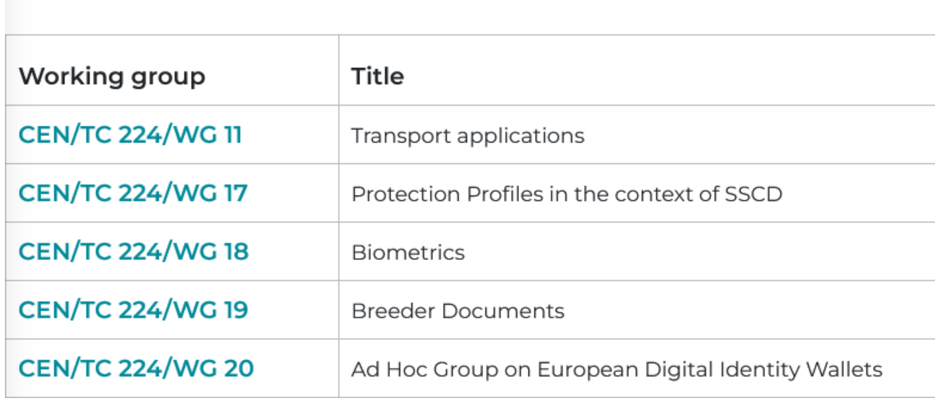


Working group	Title
CEN/CLC/JTC 13/WG 1	Chair's Advisory Group
CEN/CLC/JTC 13/WG 2	Management systems and controls sets
CEN/CLC/JTC 13/WG 3	Security evaluation and assessment
CEN/CLC/JTC 13/WG 5	Data Protection, Privacy and Identity Management
CEN/CLC/JTC 13/WG 6	Product security
CEN/CLC/JTC 13/WG 7	Adhoc group EU 5G Certification scheme support group
CEN/CLC/JTC 13/WG 8	Special Working Group RED Standardization Request
CEN/CLC/JTC 13/WG 9	Special Working Group on Cyber Resilience Act

CEN/TC 224 “Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment”

Scope:

- The **development of standards for strengthening the interoperability and security of personal identification and its related personal devices, systems, operations and privacy in a multi sectorial environment**. It covers:
  - Operations such as applications and services like **electronic identification, electronic signature**, payment and charging, access and border control;
  - Personal devices with secure elements independently of their form factor, such as cards, mobile devices, and their related interfaces;
  - Security services including authentication, confidentiality, integrity, biometrics, protection of personal and sensitive data;
  - System components such as accepting devices, servers, cryptographic modules;
- CEN/TC 224 multi-sectorial environment involves sectors such as Government/Citizen, Transport, Banking, e-Health, as well as Consumers and providers from the supply side such as card manufacturers, security technology, conformity assessment body, software manufacturers.



Working group	Title
CEN/TC 224/WG 11	Transport applications
CEN/TC 224/WG 17	Protection Profiles in the context of SSCD
CEN/TC 224/WG 18	Biometrics
CEN/TC 224/WG 19	Breeder Documents
CEN/TC 224/WG 20	Ad Hoc Group on European Digital Identity Wallets

ETSI/TC CYBER “Cybersecurity”

Scope:

- To act as the **ETSI centre of expertise in the area of Cyber Security**
- Advise and assist all ETSI Groups with the development of Cyber Security requirements
- To develop and maintain the Standards, Specifications and other deliverables to support the development and implementation of Cyber Security standardization within ETSI
- To collect and specify Cyber Security requirements from relevant stakeholders
- To identify gaps where existing standards do not fulfil the requirements and provide specifications and standards to fill these gaps, without duplication of work in other ETSI committees and partnership projects
- To ensure that appropriate Standards are developed within ETSI in order to meet these requirements
- To perform identified work as sub-contracted from ETSI Projects and ETSI Partnership Projects
- **To coordinate work in ETSI with external groups such as ENISA**
- **To answer to policy requests related to Cyber Security, and security in broad sense in the ICT sector**

ETSI/TC ESI “Electronic Signatures and Infrastructures”

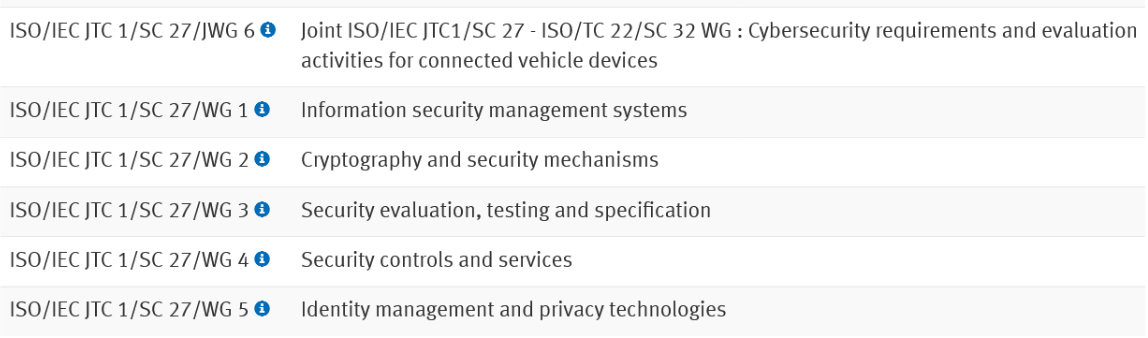
Scope:

- **TC ESI is responsible for standardization within ETSI supporting current and upcoming technology for trust services relating to Electronic Signatures and other trust services such as registered electronic delivery, electronic seals, electronic attestation of attributes and electronic archival.** This includes trust service data formats, Identification procedures and policy and audit requirements for trust infrastructures supporting such trust services. This is aimed at supporting regulatory requirements such as the eIDAS Regulation as well as general international and commercial requirements.
- TC ESI is the lead body within ETSI in relation to electronic signatures, and other trust service Infrastructures, to ensure trust and confidence in electronic transactions by:
  - Developing European Standards and other standardisation deliverables, generic standards, guides and reports
  - Liaising with other ETSI bodies
  - Liaising with bodies external to ETSI
  - Establishing a continuing work plan.
- TC ESI has over 20 years experience in standardisation for Electronic Signatures and Trust Infrastructures. Its standards for signature formats have been recognised under European regulations and adopted by a number of countries around the world. It’s best practices standards for trust service providers and their audit have been adopted across Europe and is recognised by major IT providers.

ISO/IEC JTC 1/SC 27 “Information security, cybersecurity and privacy protection”

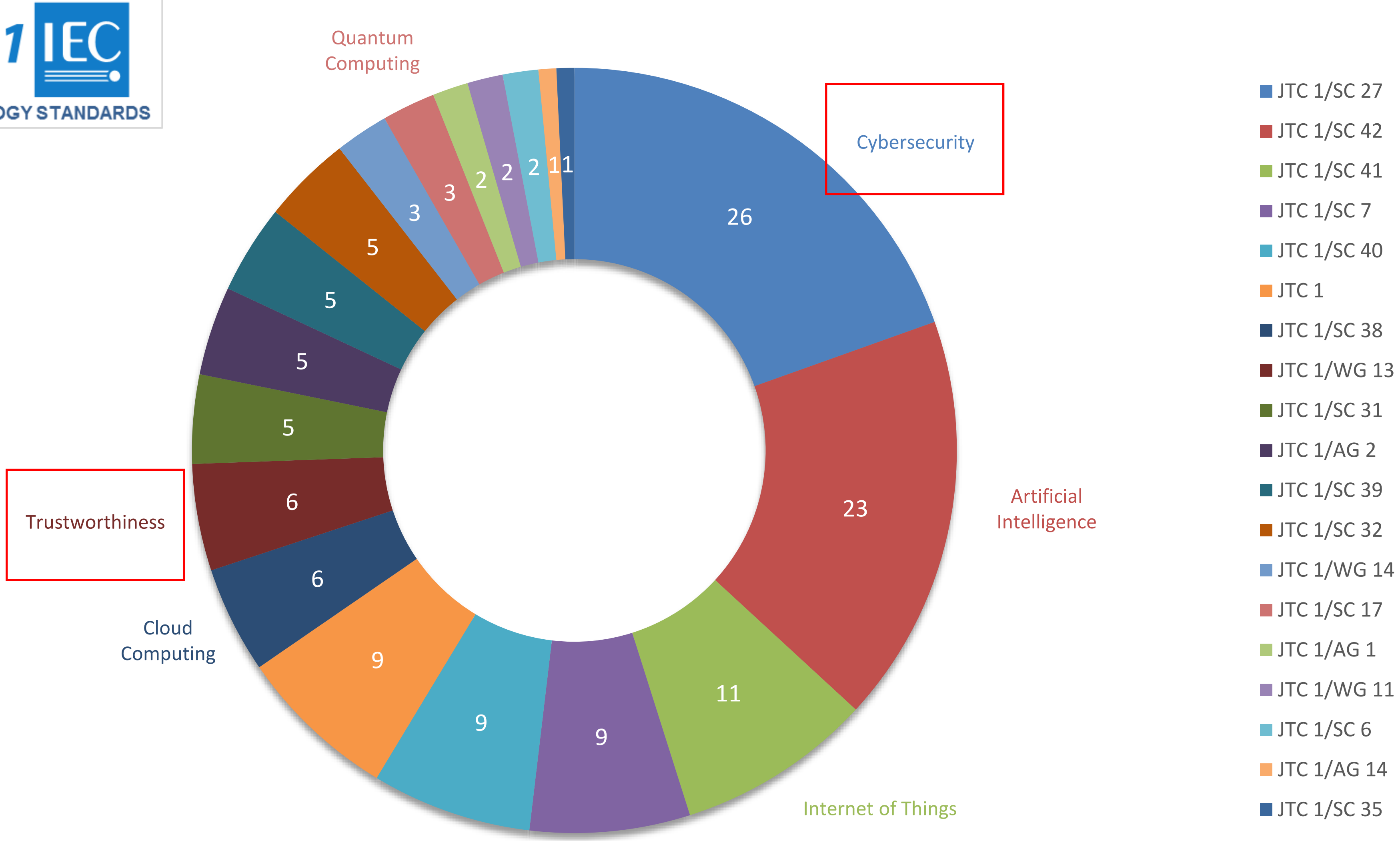
Scope:

- The **development of standards for the protection of information and ICT**. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:
  - Security requirements capture methodology;
  - Management of information and ICT security; in particular information security management systems, security processes, and security controls and services;
  - Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
  - Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
  - Security aspects of identity management, biometrics and privacy;



ISO/IEC JTC 1/SC 27/JWG 6	Joint ISO/IEC JTC1/SC 27 - ISO/TC 22/SC 32 WG : Cybersecurity requirements and evaluation activities for connected vehicle devices
ISO/IEC JTC 1/SC 27/WG 1	Information security management systems
ISO/IEC JTC 1/SC 27/WG 2	Cryptography and security mechanisms
ISO/IEC JTC 1/SC 27/WG 3	Security evaluation, testing and specification
ISO/IEC JTC 1/SC 27/WG 4	Security controls and services
ISO/IEC JTC 1/SC 27/WG 5	Identity management and privacy technologies

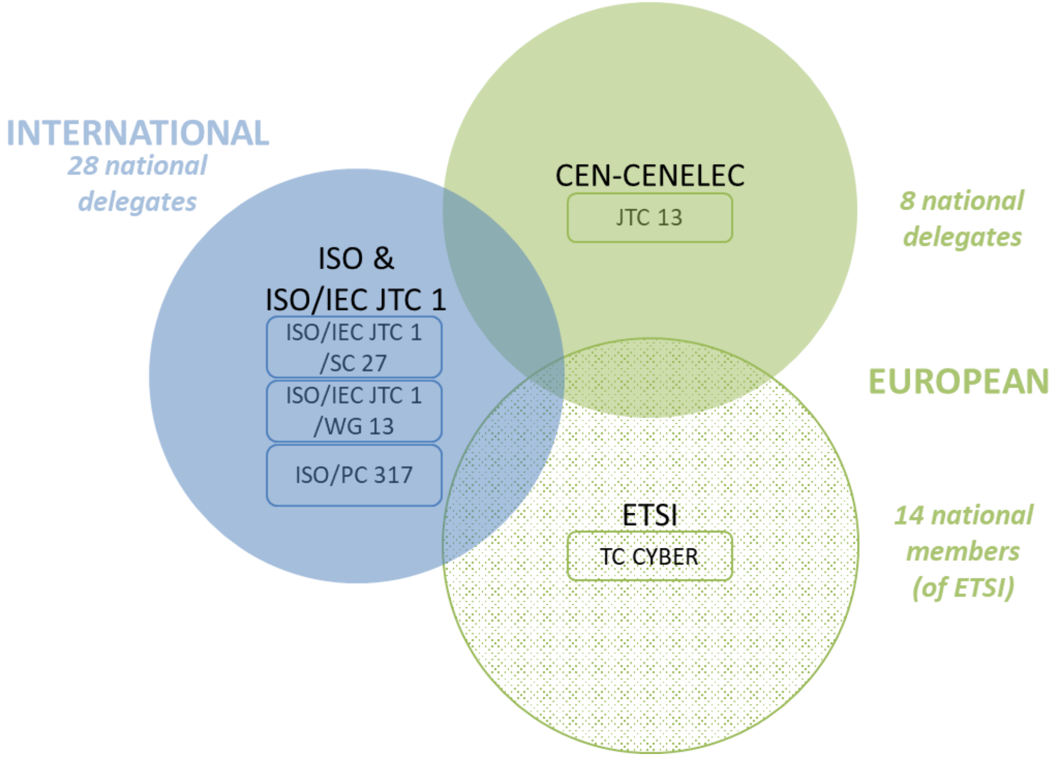
III. Most relevant technical committees in relation with Digital Trust



→ 63 national delegates registered in ISO/IEC JTC 1 (77 in total for the ICT sector)

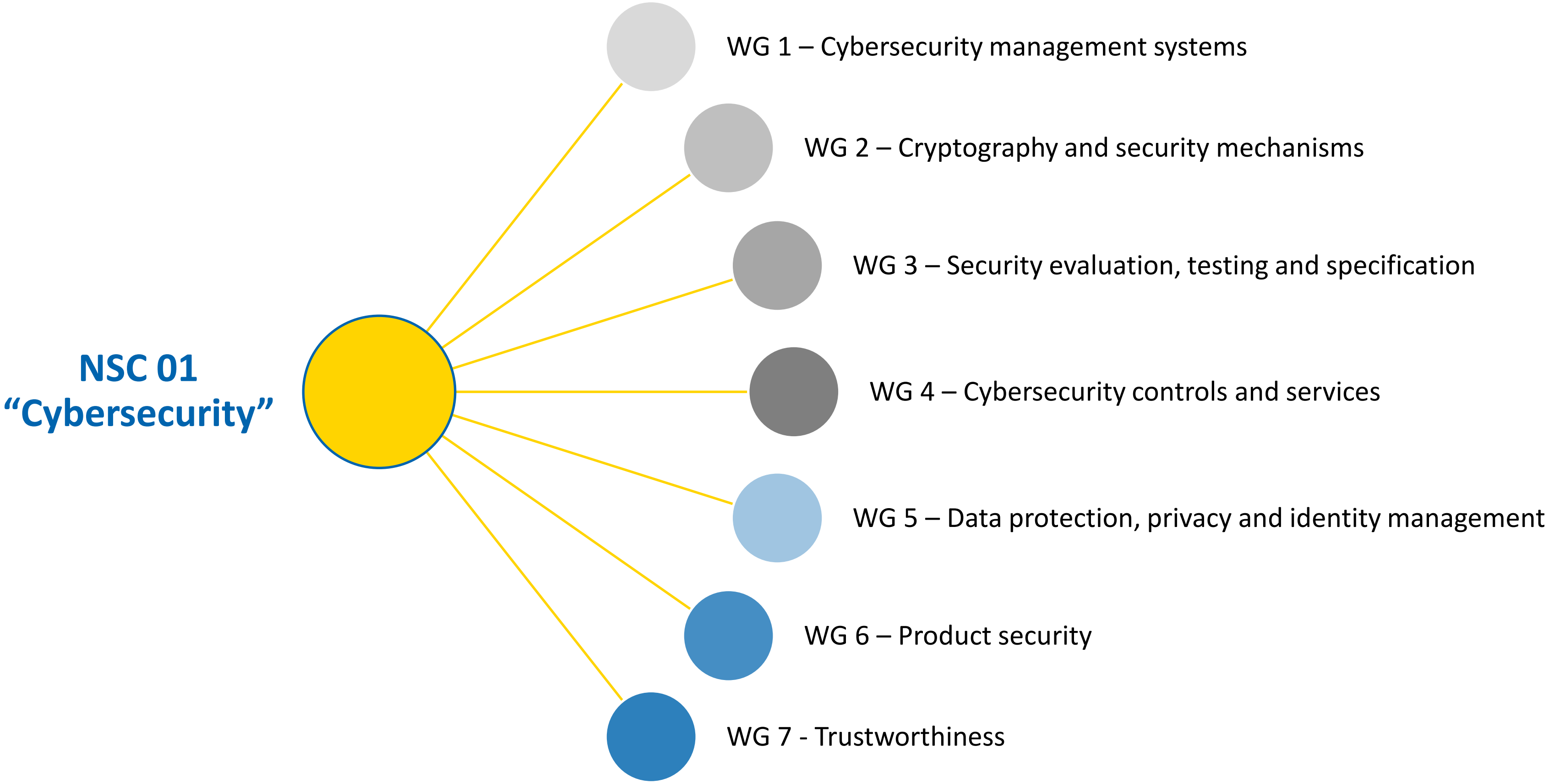
IV. The National Standardization Commission “Cybersecurity” (NSC 01)

Multiple technical committees dealing with similar or complementary projects



- *CEN/CLC/JTC 13 “Cybersecurity and Data Protection”*
- *ETSI/TC CYBER “Cybersecurity”*
- *ISO/IEC JTC 1/SC 27 “Information security, cybersecurity and privacy protection”*
- *ISO/IEC JTC 1/WG 13 “Trustworthiness”*
- *ISO/PC 317 “Consumer protection: privacy by design for consumer goods and services”*

National Standardization Commission (NSC 01) “Cybersecurity”



NSC 01
“Cybersecurity”

- WG 1 – Cybersecurity management systems
- WG 2 – Cryptography and security mechanisms
- WG 3 – Security evaluation, testing and specification
- WG 4 – Cybersecurity controls and services
- WG 5 – Data protection, privacy and identity management
- WG 6 – Product security
- WG 7 - Trustworthiness

→ ***30 national delegates***

Portfolio of more than 80 projects

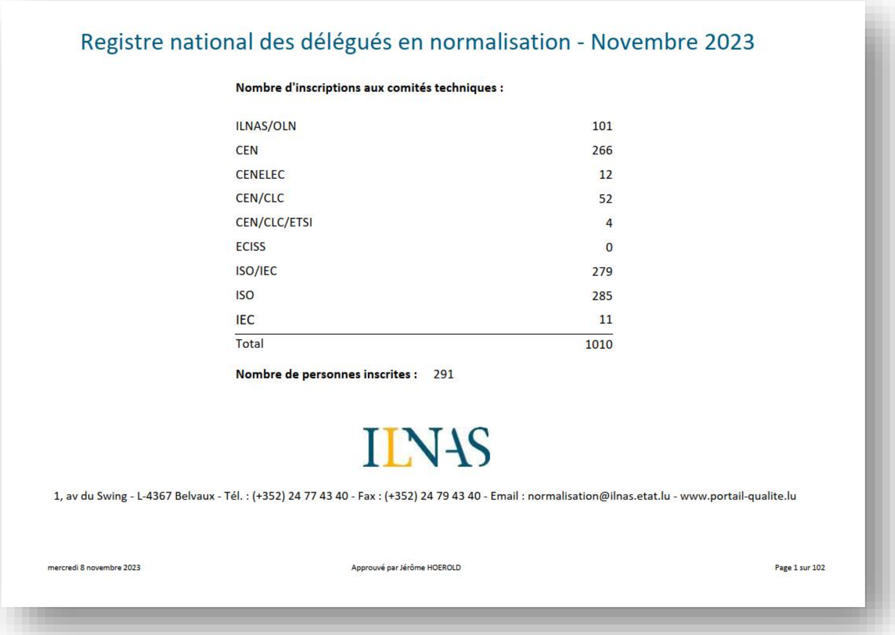
IV. The National Standardization Commission “Cybersecurity” (NSC 01)

- **Why should I participate?**
  - Join a network of experts
  - Anticipate future standards and developments in a specific sector
  - Possibility to vote while representing Luxembourg

- **Who can participate?**
  - Every socio-economic actor in Luxembourg with a certain expertise

- **Costs related to an active participation?**
  - Free of charge

- **National register of standardization delegates (Link)**
  - 291 experts registered
  - 1010 registrations in technical committees



Registre national des délégués en normalisation - Novembre 2023

Nombre d'inscriptions aux comités techniques :

ILNAS/OLN	101
CEN	266
CENELEC	12
CEN/CLC	52
CEN/CLC/ETSI	4
ECISS	0
ISO/IEC	279
ISO	285
IEC	11
Total	1010

Nombre de personnes inscrites : 291

ILNAS

1, av du Swing - L-4367 Belvaux - Tél. : (+352) 24 77 43 40 - Fax : (+352) 24 79 43 40 - Email : normalisation@ilnas.etat.lu - www.portail-qualite.lu

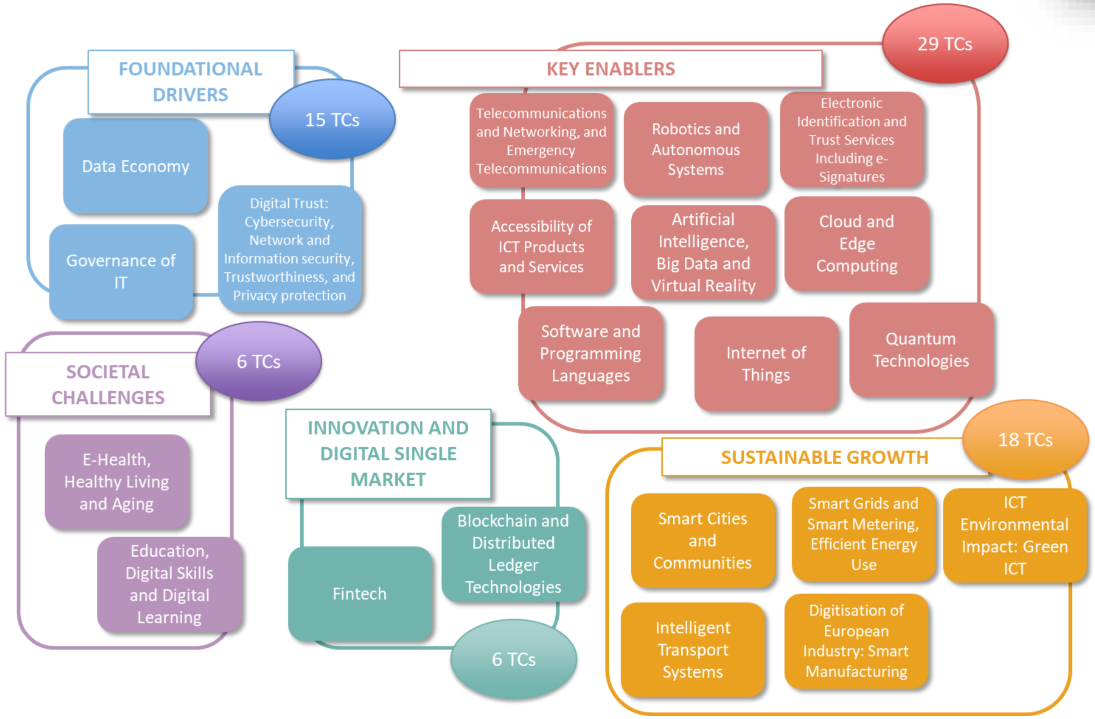
mercredi 8 novembre 2023 Approuvé par Jérôme HOEROLD Page 1 sur 102

V. Products & Services

- **In order to best exploit the advantages linked to technical standardization, ILNAS offers, in collaboration with the GIE ANEC-N, the following products and services to national socio-economic actors:**
  - Diffusion of normative information
  - Continuous training in the field of technical standardization
  - Standards watch
  - National standards analyses (limited to the “priority” sectors defined in the national standardization strategy)

ILNAS
ANEC
2023
CATALOGUE
NORMALISATION TECHNIQUE
TECHNICAL STANDARDIZATION
Formations en ligne
Online trainings
Formations techniques en normalisation
Technical trainings in standardization
Formations personnalisées / Événements de sensibilisation
Customized trainings / Awareness events

DÉVELOPPEZ VOTRE ORGANISATION GRÂCE AUX NORMES
PROFITEZ DE NOS SERVICES GRATUITS !
ILNAS
ANEC



FOUNDATIONAL DRIVERS

15 TCs

Data Economy

Governance of IT

Digital Trust: Cybersecurity, Network and Information security, Trustworthiness, and Privacy protection

KEY ENABLERS

29 TCs

Telecommunications and Networking, and Emergency Telecommunications

Robotics and Autonomous Systems

Electronic Identification and Trust Services Including e-Signatures

Accessibility of ICT Products and Services

Artificial Intelligence, Big Data and Virtual Reality

Cloud and Edge Computing

Software and Programming Languages

Internet of Things

Quantum Technologies

SOCIETAL CHALLENGES

6 TCs

E-Health, Healthy Living and Aging

Education, Digital Skills and Digital Learning

INNOVATION AND DIGITAL SINGLE MARKET

Fintech

Blockchain and Distributed Ledger Technologies

6 TCs

SUSTAINABLE GROWTH

18 TCs

Smart Cities and Communities

Smart Grids and Smart Metering, Efficient Energy Use

ICT Environmental Impact: Green ICT

Intelligent Transport Systems

Digitisation of European Industry: Smart Manufacturing

Thank you

ILNAS

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux
Tel. : (+352) 24 77 43 - 50
E-mail : confiance-numerique@ilnas.etat.lu
www.portail-qualite.lu