Welcome

Bienvenue

Willkommen

ILNAS

National Digital Trust Body -

Trust Services, eArchiving, Cybersecurity Certification, Cyber Resilience & AI

Alain Wahl

27/11/2025

ILNAS

AGENDA

- Introduction – Digital Trust Body
- eIDAS Regulation
- eArchiving Regulation
- Cybersecurity Act
- Cyber Resilience Act
- AI Act

AGENDA

- Introduction – Digital Trust Body
- eIDAS Regulation
- eArchiving Regulation
- Cybersecurity Act
- Cyber Resilience Act
- AI Act

NATIONAL DIGITAL TRUST BODY

- **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')**
  - EUCC: Common Criteria;
  - EUDIW: Digital Identity Wallet;
  - EUCS: Cloud Scheme;
  - EU5G.
- **Promotion of good practices**
- **NIS CG WS PQC cooperation group on post-quantum cryptography**
- **New missions to come: AI Act, Cyber Resilience Act, …**

- ❑ News and newsletters
- ❑ INAP Training on e-signatures and trust services
- ❑ DLH trainings, Master in Technopreneurship
- ❑ https://portail-qualite.public.lu

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)

eArchiving 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, ICT processes and managed security services

AGENDA

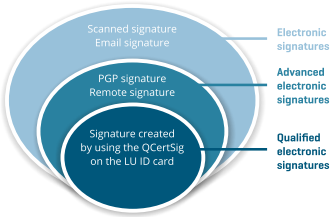
- Introduction – Digital Trust Body
- eIDAS Regulation
- eArchiving Regulation
- Cybersecurity Act
- Cyber Resilience Act
- AI Act

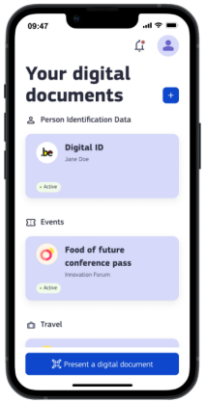
II eIDAS REGULATION

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

Trust Services

- Website authentication
- eID
- eSignature / eSeal with time stamp
- Electronic registered delivery service
- Electronic archiving
  Electronic ledger





Identification & authentication

Store & present attestations of attributes

Sign & seal electronically

LUXTRUST beys INCERT NEXT-GEN SHIELD FOR DIGITAL WORLD

Trust services under the EUDI Framework

General Trust Services

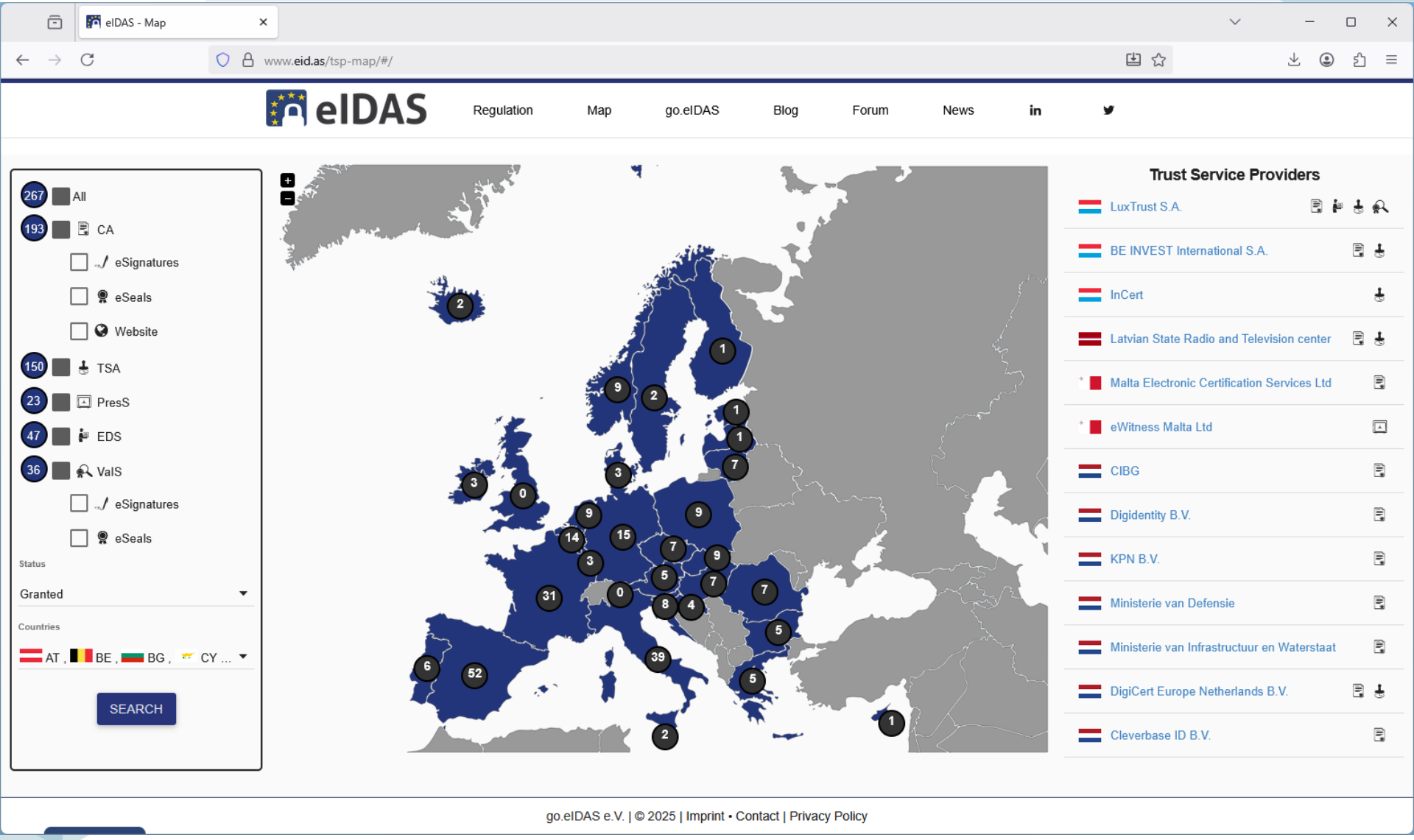
- electronic signatures
- electronic seals
- electronic time stamps
- electronic documents
- electronic registered delivery services
- certificate services for website authentication
- electronic signature and seal creation devices

+ New - Relevant to EUDI Framework

- **electronic archiving**
- **electronic attestation of attributes**
- **electronic ledgers**
- **management of remote qualified signature creation device**
- **management of remote qualified seal creation device**

European Commission | EU Digital Identity Wallet

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



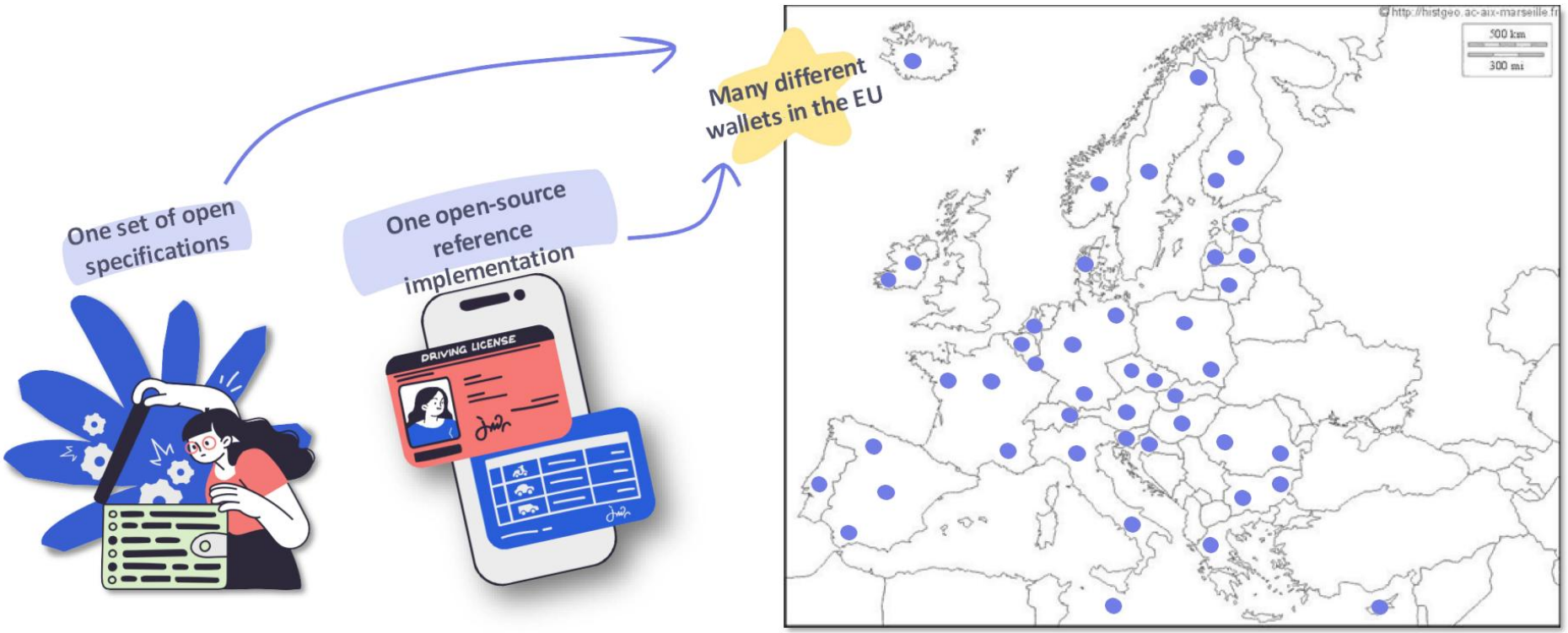
Legal effects (eSignatures, eSeals, eTimeStamps and eRegistered Delivery Services)

	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

Open

There will be multiple EU Digital Identity Wallets, all built to a common set of open specifications by the European Commission and Member States. They will be **interoperable**, and both the reference implementation and all European Wallet Apps for consumer devices will be open source.



European Commission | EU Digital Identity Wallet

EU Digital Identity Wallets

Wallets for Businesses

Business-to-business and business-to-government scenarios including regulatory compliance, company registration, and power of attorney

Wallets for Travel

National and Cross-border travel scenarios including local public transport, long-distance travel, shared mobility border control, hotel check-in

Wallets for Payments & Banking

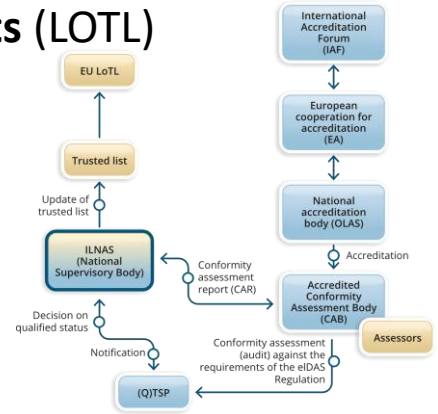
Payment and banking scenarios including a standardised process for Know-Your-Customer, Strong Customer Authentication, and offline transactions and processes

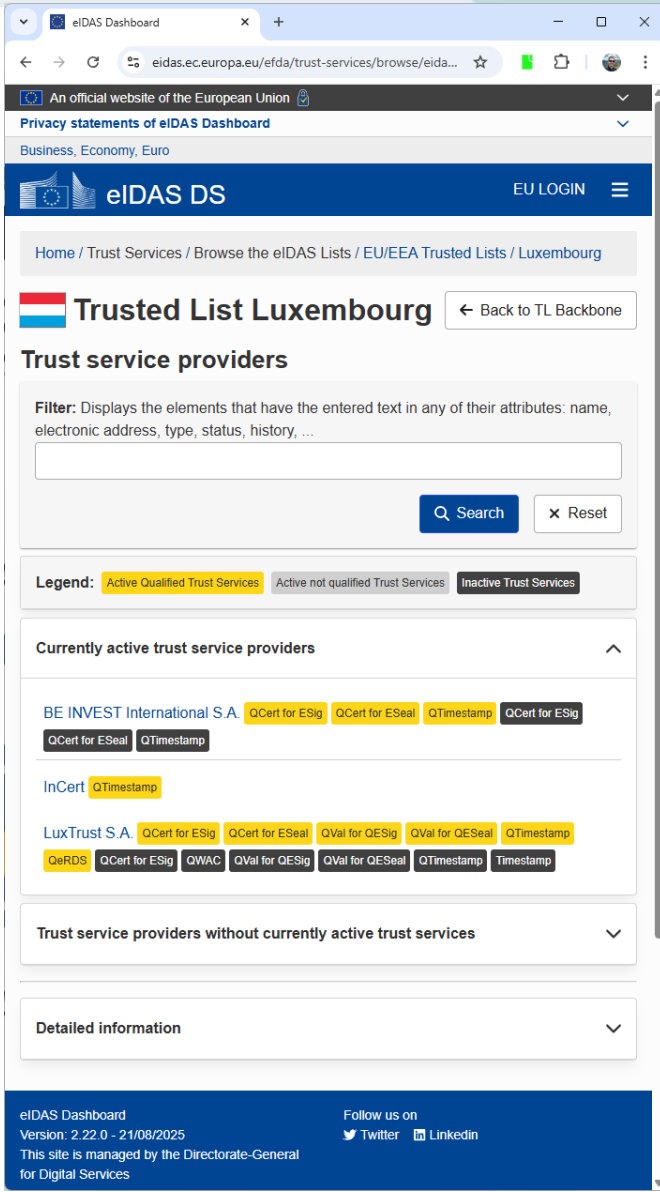
Wallets for Age Verification

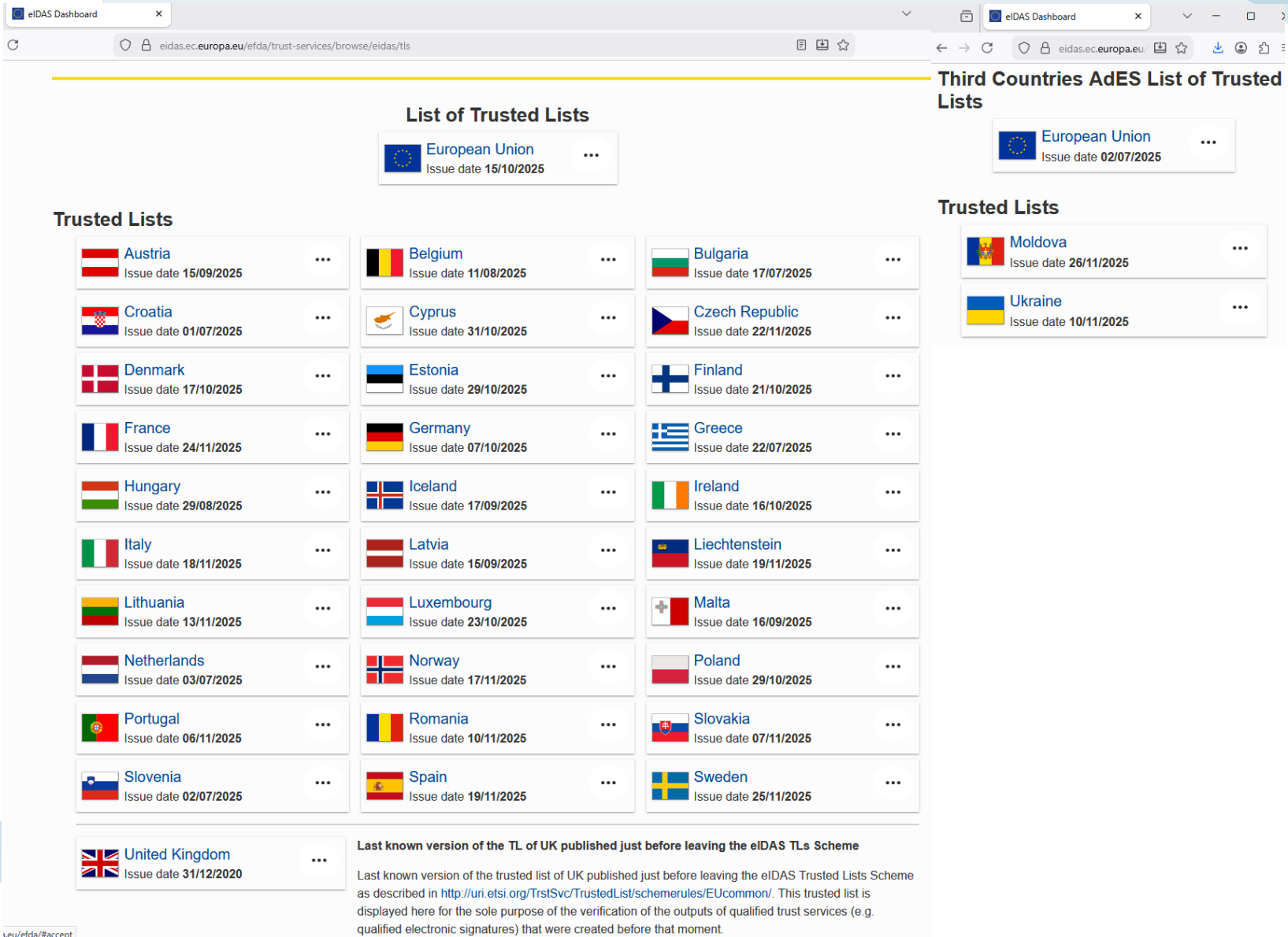
Age verification scenarios including the issuance of a pseudonymous attestation containing only age information by a trusted third party

European Commission | EU Digital Identity Wallet

- Each EU Member State maintains a **national trusted list**
- The Trusted List Luxembourg contains the **qualified trust service providers** established in Luxembourg as well as the **qualified trust services** they provide
- National trusted lists have a **constitutive effect**
- The trusted list also contains a link to the **European List of Trusted Lists** (LOTL)

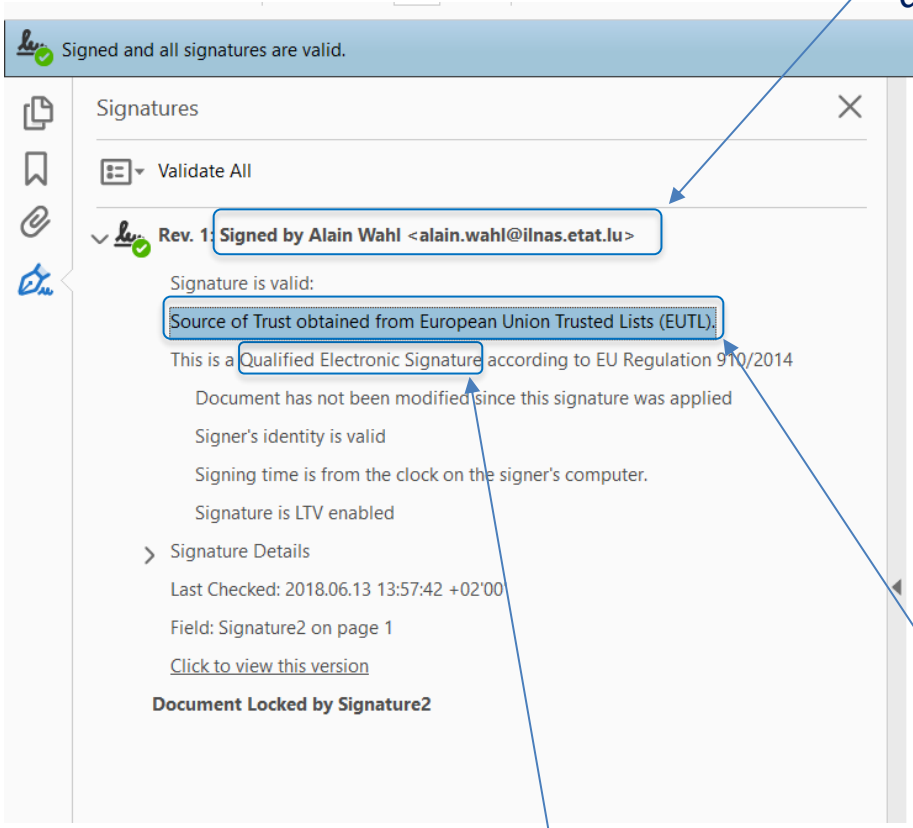





eIDAS Dashboard
eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls
List of Trusted Lists
European Union
Issue date 15/10/2025
Trusted Lists
Austria
Issue date 15/09/2025
Belgium
Issue date 11/08/2025
Bulgaria
Issue date 17/07/2025
Croatia
Issue date 01/07/2025
Cyprus
Issue date 31/10/2025
Czech Republic
Issue date 22/11/2025
Denmark
Issue date 17/10/2025
Estonia
Issue date 29/10/2025
Finland
Issue date 21/10/2025
France
Issue date 24/11/2025
Germany
Issue date 07/10/2025
Greece
Issue date 22/07/2025
Hungary
Issue date 29/08/2025
Iceland
Issue date 17/09/2025
Ireland
Issue date 16/10/2025
Italy
Issue date 18/11/2025
Latvia
Issue date 15/09/2025
Liechtenstein
Issue date 19/11/2025
Lithuania
Issue date 13/11/2025
Luxembourg
Issue date 23/10/2025
Malta
Issue date 16/09/2025
Netherlands
Issue date 03/07/2025
Norway
Issue date 17/11/2025
Poland
Issue date 29/10/2025
Portugal
Issue date 06/11/2025
Romania
Issue date 10/11/2025
Slovakia
Issue date 07/11/2025
Slovenia
Issue date 02/07/2025
Spain
Issue date 19/11/2025
Sweden
Issue date 25/11/2025
United Kingdom
Issue date 31/12/2020
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.
eIDAS Dashboard
eidas.ec.europa.eu
Third Countries AdES List of Trusted Lists
European Union
Issue date 02/07/2025
Trusted Lists
Moldova
Issue date 26/11/2025
Ukraine
Issue date 10/11/2025

Demo

Information on the signatory (as contained in the qualified certificate for electronic signatures)



Type of signature: **Qualified electronic signature** (based on a QCertSig on a QSigCD)

Signature verification used the **European List of Trusted Lists**

AGENDA

- Introduction – Digital Trust Body
- eIDAS Regulation
- eArchiving Regulation
- Cybersecurity Act
- Cyber Resilience Act
- AI Act

Electronic archiving

- Goal

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

- Legal value of electronic documents:

  Law of 25 July 2015 on electronic archiving

- Revolutionary aspect of the e-archiving framework in Luxembourg

  digitization of analog documents, preserving the probative value

- New **eIDAS trust service**: electronic archiving service

Objectives of the law

- Legal framework for digitization and e-archiving services;
- Rules for service providers who request the **"PSDC" status** (digitization and e-archiving service provider)

About the legal value of electronic copies

- Electronic copies **digitised by a PSDC ⇨ Presumption of conformity** with the original document
- An electronic copy cannot be rejected by a judge
  - because of its electronic format (cf. eIDAS)
  - because it has not been created by a PSDC

Nom et adresse actuels de la personne morale	Numéro d'identification	Périmètre actuel
Lab Luxembourg S.A. 3, rue Dr. Elvire Engel L-8346 Grass	2016/9/001 (Historique)	Dématérialisation & Conservation
Numen Europe S.A. 2, rue Edmond Reuter L-5326 Contern	2016/9/002 (Historique)	Dématérialisation & Conservation
KPMG Services S.à.r.l. 39, avenue John F. Kennedy L-1855 Luxembourg	2017/9/004 (Historique)	Dématérialisation & Conservation
Centre des technologies de l'information de l'Etat 560, rue de Neudorf L-2220 Luxembourg	2017/9/006 (Historique)	Conservation
LuxTrust S.A. 13-15, Parc d'activités L-8308 Capellen	2024/9/008 (Historique)	Conservation

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

National Standard ILNAS 106:2024

- 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, updated in Mars 2024
- National standard ILNAS 106:2024 is based on the international standards
  - ISO/IEC 27001:2022: Information Technology — Security Techniques — Information Security Management Systems — Requirements
  - ISO/IEC 27002:2022: Information Technology — Security Techniques — Code of Practice for Information Security Controls
  - ISO 14641:2018: 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.)

Available free of charge at

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

AGENDA

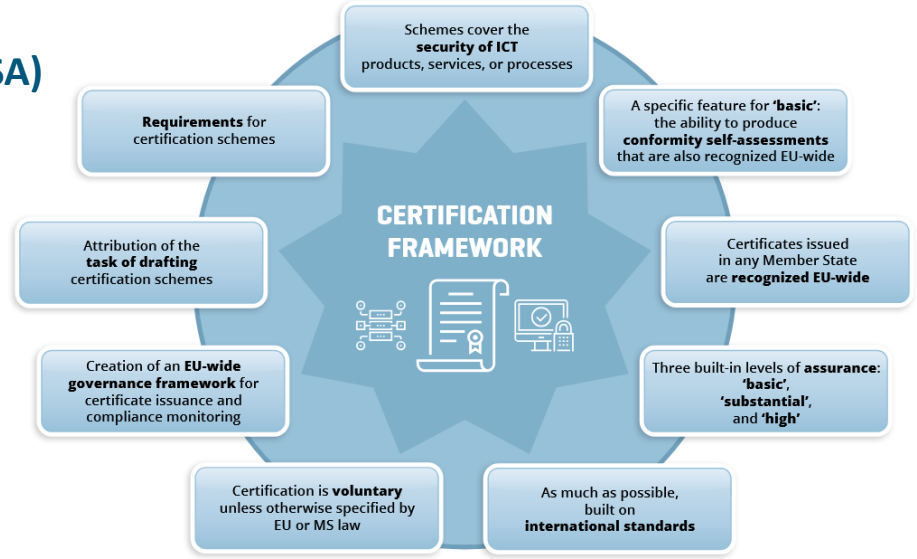
- Introduction – Digital Trust Body
- eIDAS Regulation
- eArchiving Regulation
- Cybersecurity Act
- Cyber Resilience Act
- AI Act

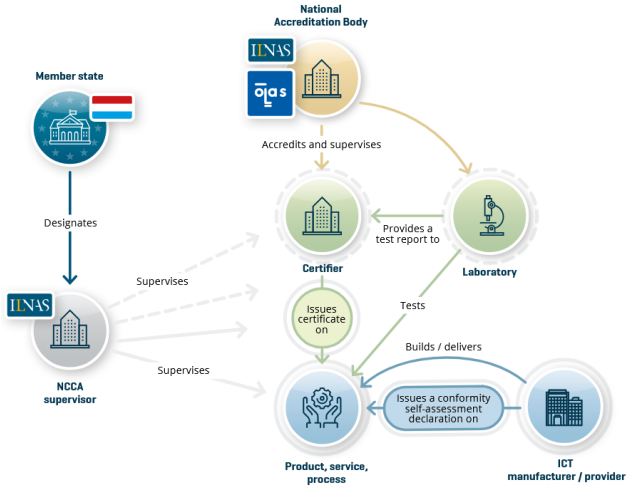
Cybersecurity Act (CSA) – Regulation 2019/881

- **European Framework for Cybersecurity Certification Schemes (Cybersecurity Act, or CSA)**

- **Topics of Cybersecurity Certification Schemes**
  - *IT products with security functions (active)*
    EUCC – Based on "Common Criteria" standards
  - *EUCS – Cloud Scheme*
  - *EU5G equipment (in preparation)*
  - *Digital ID wallet (in preparation)*
  - *Managed security services (in preparation, new)*

- **ILNAS – National Cybersecurity Certification Authority (NCCA)**
  - *Supervision of certificates issued within the national territory*
  - *Certification at the assurance level "high"*
    Certification can be delegated by general delegation





AGENDA

- Introduction – Digital Trust Body
- eIDAS Regulation
- eArchiving Regulation
- Cybersecurity Act
- Cyber Resilience Act
- AI Act

Legislative Act

Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (hereinafter referred to as “CRA”).

Applicable from 11 December 2027 (with exceptions for some articles)

Objective

The CRA aims to strengthen the cybersecurity of digital products by imposing security requirements from the design stage and throughout the entire lifecycle.

The goal is to reduce vulnerabilities and the impact of cyberattacks on consumers and businesses.

The regulation defines a risk-based approach and sets minimum requirements for products and manufacturers.

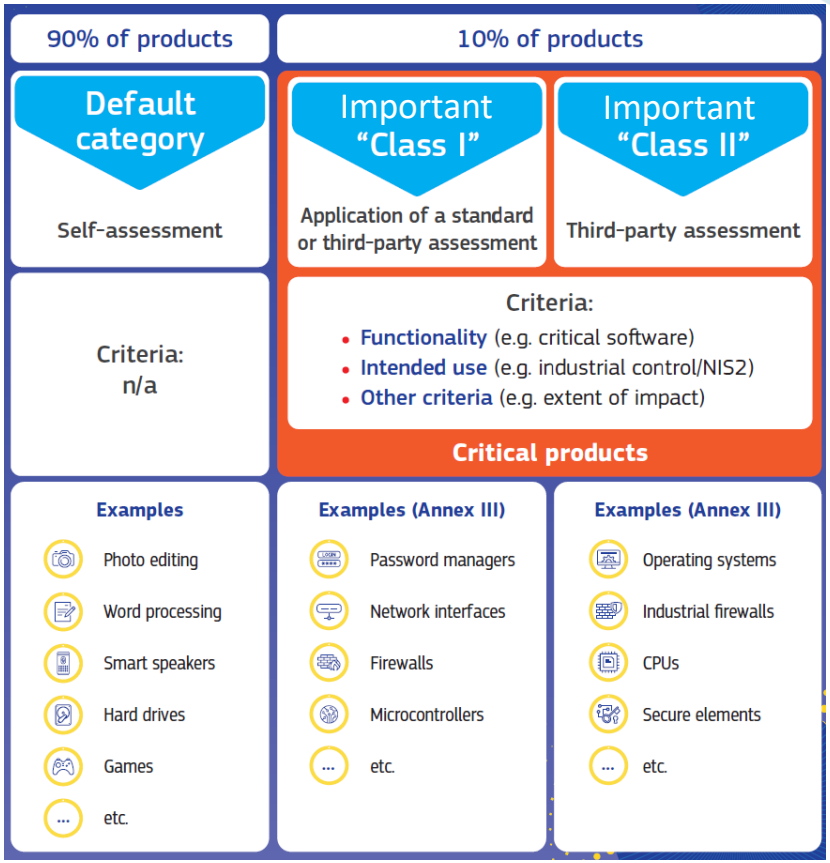
Scope

The CRA applies to products with digital elements made available on the market, where the intended or reasonably foreseeable use includes a direct (e.g., mobile phones) or indirect (e.g., smartwatches), logical or physical connection to a device or a network.

CLASSIFICATION OF PRODUCTS

The CRA defines 4 classes for products with digital elements:

1. Default category
2. Important products – “Class I”
   e.g. password managers, network interfaces, smart home general purpose virtual assistants, …
3. Important products – “Class II”
   e.g. firewalls, intrusion detection and prevention systems, …
4. Critical products
   e.g. smartcards, smart meter gateways, …



The conformity assessment procedure for a product with digital elements depends on its class.

AGENDA

- Introduction – Digital Trust Body
- eIDAS Regulation
- eArchiving Regulation
- Cybersecurity Act
- Cyber Resilience Act
- AI Act

Legislative Act

Regulation (UE) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (hereinafter referred to as “AI Act”)

Objective

The AI Act establishes a common legal framework for the development and use of artificial intelligence systems within the European Union. The AI Act:

- aims to ensure trustworthy AI that respects fundamental rights, health, safety, and the environment;
- prohibits AI uses that pose unacceptable risks and imposes obligations based on risk level;
- promotes innovation while ensuring the free movement of AI-based products and services within the internal market.

Scope

The AI Act applies to all actors involved in placing on the market, using, or distributing AI systems in the EU.

It excludes military uses, non-commercial research activities, and personal uses.

Open-source systems are generally excluded, except when they present high risks.

ARTIFICIAL INTELLIGENCE ACT (AI Act) REGULATION (EU) 2024/1689

PROHIBITED PRACTICES IN THE FIELD OF AI (ARTICLE 5)

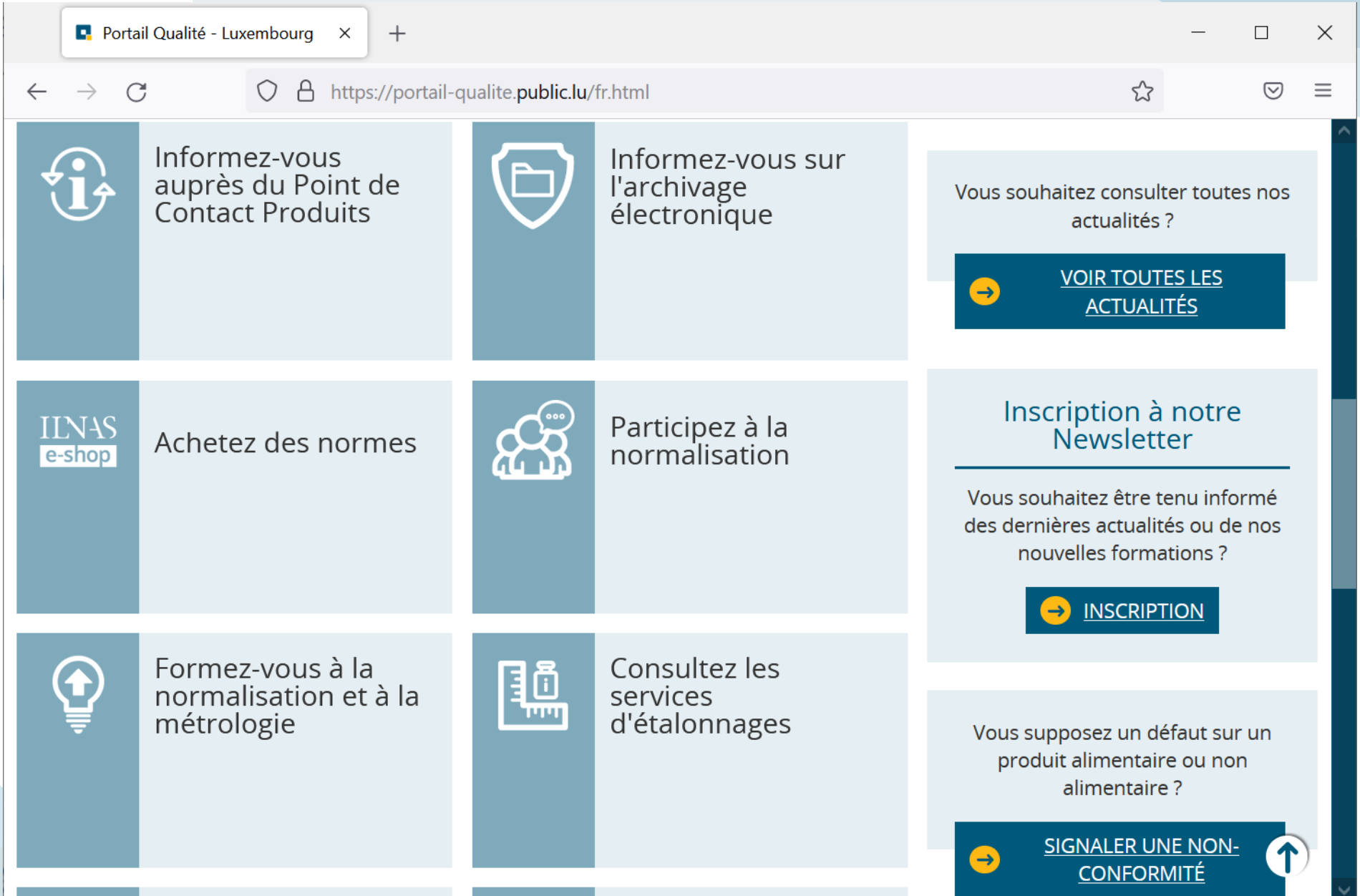
The AI Act prohibits certain uses of artificial intelligence.

These include AI systems that:

- manipulate people's decisions or exploit their vulnerabilities;
- evaluate or rank individuals based on their social behavior or personal traits;
- predict the likelihood of a person committing a crime;
- collect facial images from the internet or from video surveillance footage;
- infer emotions in the workplace or in educational institutions;
- classify individuals based on their biometric data.

However, certain exceptions are provided for the application of the AI Act, such as searching for missing persons, preventing terrorist attacks.

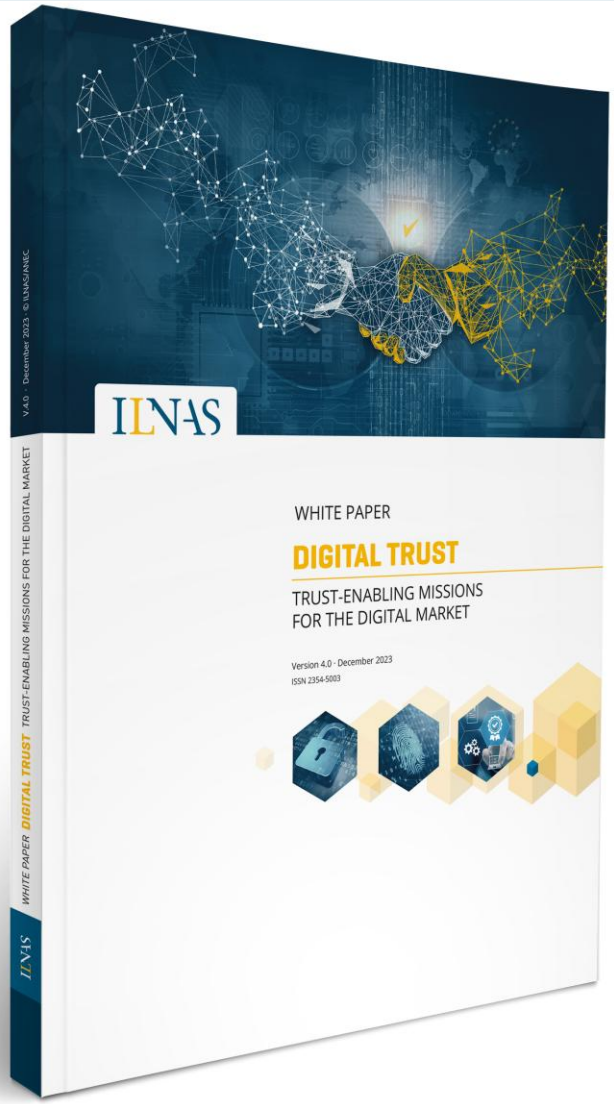
FOR MORE INFORMATION



FOR MORE INFORMATION

- https://portail-qualite.public.lu/fr/publications.html
- News and newsletters

  Register for our newsletters on our website
- DLH trainings
- Master in Technopreneurship
- White Paper



Thank you

Merci

Danke

- News and newsletters
- DLH, INAP trainings, Master in Technopreneurship
- https://portail-qualite.public.lu

ILNAS

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

Tel. : (+352) 24 77 43 53 · Fax : (+352) 24 79 43 - 50

E-mail : confiance-numerique@ilnas.etat.lu

www.portail-qualite.lu