Electronic identities and electronic signatures

Björn Scharin and Anna Amundberg

PTS

Presentation

- Introduction and presentation of The Swedish Post and Telecom Authority (PTS)
- Background of the eIDAS regulation
- Regulation vs Directive
- Electronic ID
- Trust services and service providers
- European Digital Identity Wallet
- Implementing legal acts
- About the trust services
- Questions

The Swedish Post and Telecom Authority (PTS)

Our vision

Secure and accessible communication for Sweden.

Our operating concept

Through cooperation, promotional efforts, regulation and supervision, we contribute to a safe, digital transition.

Section for Digital and Trust Services

- eIDAS regulation
  - Trusted services
- The NIS act
  - Digital infrastructure and digital services
- Data retention in the Electronic Communications act

PTS is guided by the following

- EU primarily through directives and regulations.
- The Swedish Parliament (Riksdagen) and the Swedish Government:
  - Laws and Ordinances
  - Committee Terms of Reference and Instructions
  - Government Assignments
- PTS reports to the Ministry of Finance

Background

History

- 1999/93/EC signature directive harmonized legislation in EU
- Evaluation of the directive - market and legal aspects of electronic signatures
  - Harmonization in theory but not in practice
- Service directive
  - Commission decision that every member state shall recognize qualified electronic signatures and advanced electronic signatures based on a qualified certificate
- Studies and Mandate to CEN and ETSI to standardize
- eIDAS regulation 2016
- Revised eIDAS regulation 21 May 2024

eIDAS regulation

- Regulation vs directive
- Purpose of the eIDAS regulation

Why is the difference between an EU regulation and an EU directive important?

It has relevance for the understanding of the legal effect that the eIDAS regulation has on national legislation.

Regulation

Regulations are legal acts that **apply automatically and uniformly** to all EU countries as soon as they enter into force, without needing to be transposed into national law. They are binding in their entirety on all EU countries.

Directive

Directives **lay down certain results that must be achieved**, but each Member State is free to implement the directive into national law in a way that suits them. Implementation must take place within a certain deadline or the Commission may initiate infringement proceedings.

Purpose of the eIDAS regulation

- Create a European internal market for trust services.
- Ensure an adequate level of security.
- Increase trust in electronic transactions in the single market through a common level of security.
- Ensure access to public services in other MSs, where electronic identification are available.
- Non-discrimination (legal status).
- Provide and recognise European Digital Identity Wallets.

The eIDAS regulation regulates

- eID, European Digital Identity Wallets, trust services and trust service providers
- Internal Market Principle: Recognition of trust services from other Member States
- Legal recognition of trust services (non-discrimination)
- General requirements. (Detailed requirements can be issued by the European Commission in cooperation with the Member States through implementing acts.)

Exceptions from eIDAS regarding trust services

- Closed systems.
- Aspects related to the conclusion and validity of contracts or other legal obligations where there are national or Union requirements in regards to form.

Implementing acts

- Legally binding acts set by the Commission to ensure that EU law is applied uniformly.
- The implementing acts more detailed than the eIDAS regulation.
- Implementing acts will refer to standards from ETSI and CEN.
- If Commission refer to a standard – complying with the standard leads to a presumption of compliance with the regulation.

eID AS

Cross boarder recognition of electronic identification

Trust services for electronic transactions in the internal market

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

EU regulation 910/2014

PTS

PTS current mandate

- Supervisory body for trust services and trust service providers.
- Verify conformity assessment reports once a QTSP notifies their intention to start providing qualified trust services.
- Supervise trust service providers and trust services.
- Receive incident reports.
- Publish the national trusted list.
- Issue secondary legislation.
- Cooperation with other responsible national authorities.

Electronic identification

Electronic identification (eID)

- Mutual recognition of national systems for electronic identification
- Mandatory for a Member State to notify at least one eID system
- To be recognized, a system should be notified to the European Commission
- If a system is notified it means obligations and liability for the notifying member states
- System that could be notified should meet the security level substantial or high
- Security cheked through a peer review process or cybersecurtiy certification
- Notifying an eID system means that it could be used cross border in EU

eID cooperation network

- A cooperation network is setup to coordinate
- National eID-system checked through a peer review process
- Incident reporting through the cooperation network
- The responsible authority in Sweden for eID and the cooperation network is The Agency for Digital Government (DIGG)

Sweden

EU MS EU

Online service

National eID

eIDAS node

EU agreed SAML

eIDAS node

EU agreed SAML

National eID

Online service

National eID

National eID

Technically simple

Difficult to get attribute to ambiguously identifying a person

Trustlevels for eID

eIDAS	Sweden	Content	Gap eIDAS and Sweden
High	4	• High trust level • Face to face registration at a meeting • Hardware credential • Strong authentication	• Similar but 4 requires face to face meeting every five year
Substantial	3	• High trust • Based on face to face • Strong authentication	• No difference
Low	2	• Some trust	• No difference

Personal identity minimum dataset

Mandatory minimum dataset
First name
Surname
Date of birth
Voluntary minmum dataset
Name at birth, first and sur name
Place of birth
Current address
Sex
Other (attributes)
”Bilateral agreements”

”Minimum dataset”

There is also a table for organizations minimum dataset

What will the Swedish public sector do as a minimum

1. Lägga till ”Foreign eID”

3. Visa välkomstmeddelande

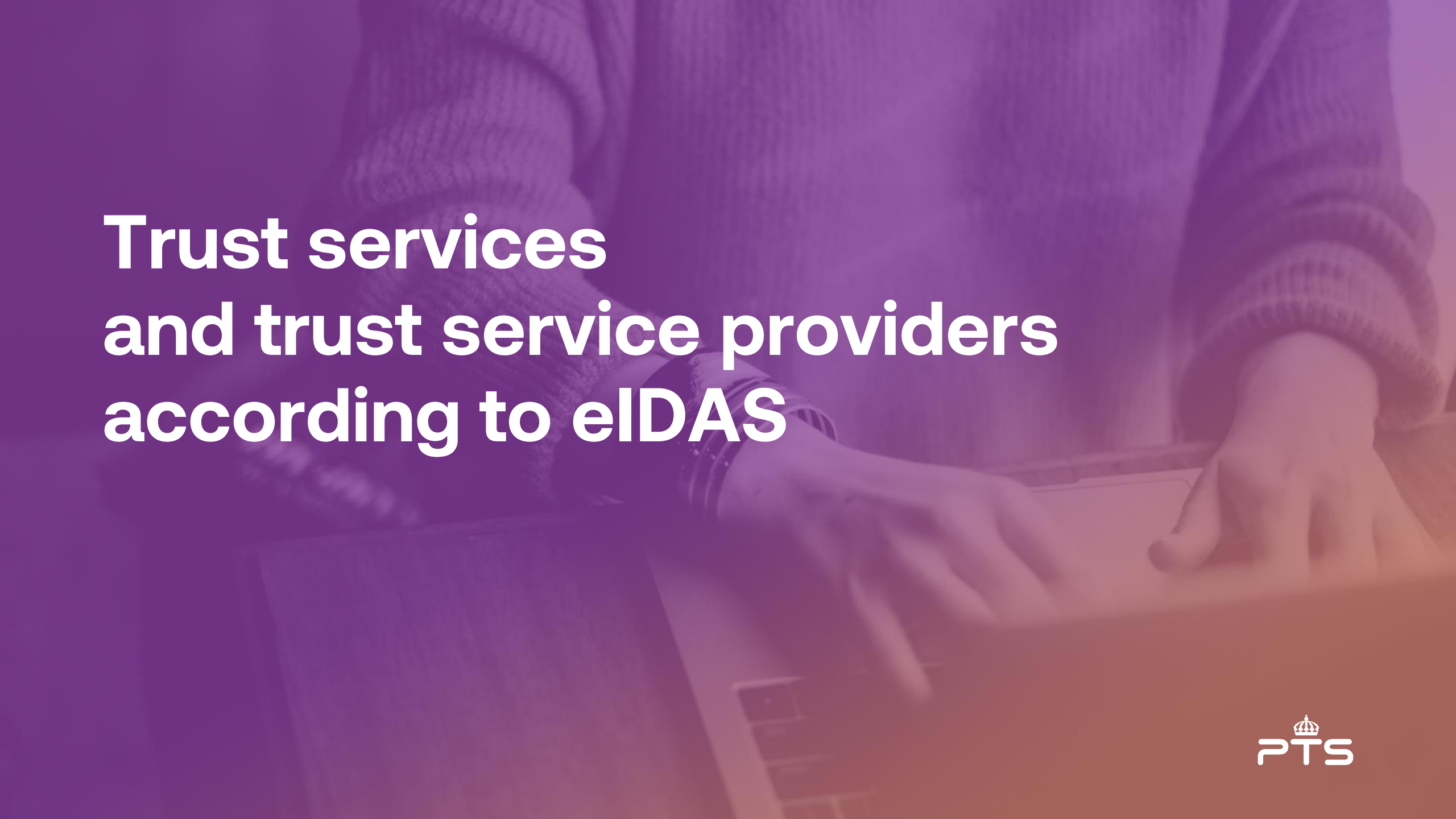
Welcome!
Your eID is recognised

What can be done could be depending on authorization

Sweden –notified eID schemes

- BankID,
- Freja eID+
- EFOS (for public sector employees)

- BankID and Freja are peer reviewed and can be used cross boarder



Trust services and trust service providers according to eIDAS

What’s a trust service?

Trust services are services that are meant to increase trust in electronic correspondence – such as the exchange of electronic documents – for example through electronic signatures or seals, which are linked to certificates issued by trusted issuers.

Definition of trust service

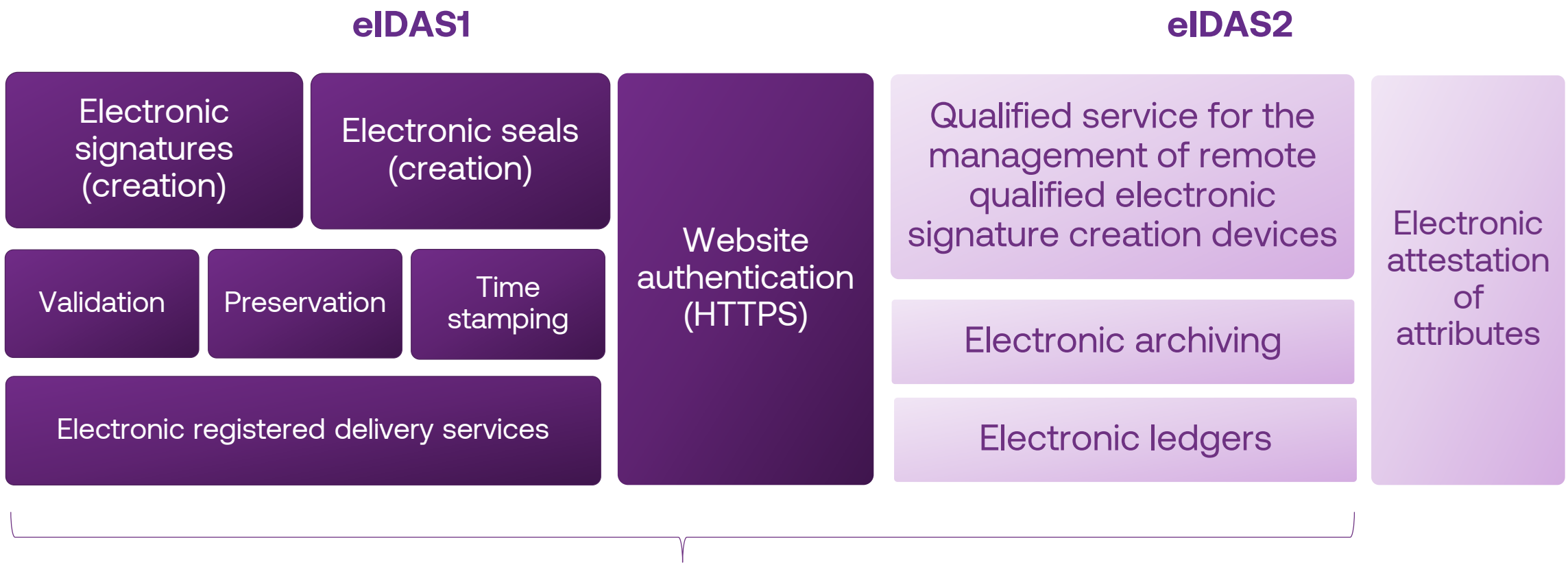
Trust service means an electronic service normally provided for remuneration which consists of:

(a) the *creation*, *verification*, and *validation* of **electronic signatures**, **electronic seals** or **electronic time stamps**, **electronic registered delivery services** and **certificates** related to those services, or

(b) the *creation*, *verification* and *validation* of **certificates for website authentication**; or

(c) the *preservation of* **electronic signatures**, **seals** or **certificates** related to those services.

Trust services



Two levels of trust:

Trust Service provider (TSP) & Qualified Trust Service provider (QTSP)

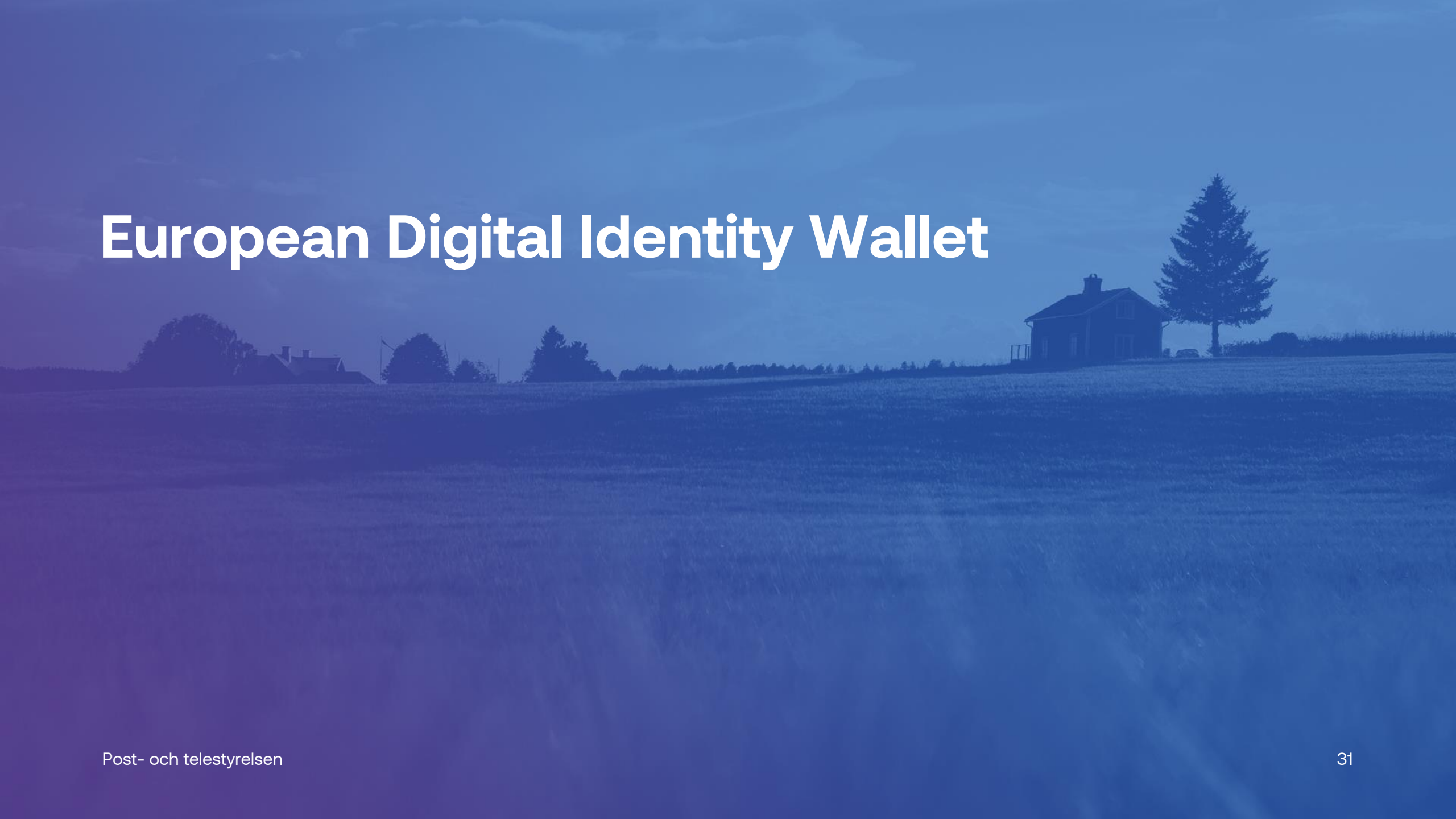
Obligations for TSPs according to eIDAS

- Security requirements: Have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or indirect risks to the provision of the non-qualified trust service, which shall, notwithstanding Article 21 of NIS2, include at least measures relating to:
  - (i) registration and onboarding procedures for a trust service;
  - (ii) procedural or administrative checks needed to provide trust services;
  - (iii) the management and implementation of trust services.
- Liable for damage – normal burden of proof.
- Obligation to report security incident Post incident supervision.

Obligations for QTSPs according to eIDAS

- Obligation to notify supervisory body, together with a conformity assessment report issued by a Conformity Assessment Body (CAB).
- Mandatory conformity assessments and audits.
- Security requirements:
  - same as TSPs
  - additional requirements regarding identification methods, sufficient financial resources, trustworthy systems, termination plans, record keeping, etc.
- Liable for damage – reversed burden of proof
- Obligation to report security incident.
- Planned and post incident supervision.

European Digital Identity Wallet



All member states shall ensure that

- ✓ All natural and legal persons in the union shall have a secure and trusted and seamless cross boarder access to public and private services
- ✓ The issuance, usage and revocation of wallets shall be free of charge for natural persons
- ✓ The usage of the wallet shall be voluntary for the user and the user shall have full control of their data

The EU Digital Identity Wallet

Free use for all citizens

Provided by Member States, all EU citizens may use it for free on a voluntary basis

Accepted throughout the Union

Recognised by private and public service providers (relying parties) for all transactions that require authentication

Secure and privacy oriented

Citizens can control and protect their identity, personal data and digital assets

European Digital Identity Wallets shall be provided by Member States

a) Directly by a Member State

b) Under a mandate from a Member State

c) Independently of a Member State but recognised by that Member State

Core functionalities of the EU Digital Identity Wallet

Identification/ Authentication

Disclose identity data required for accessing public and private services (relying parties)

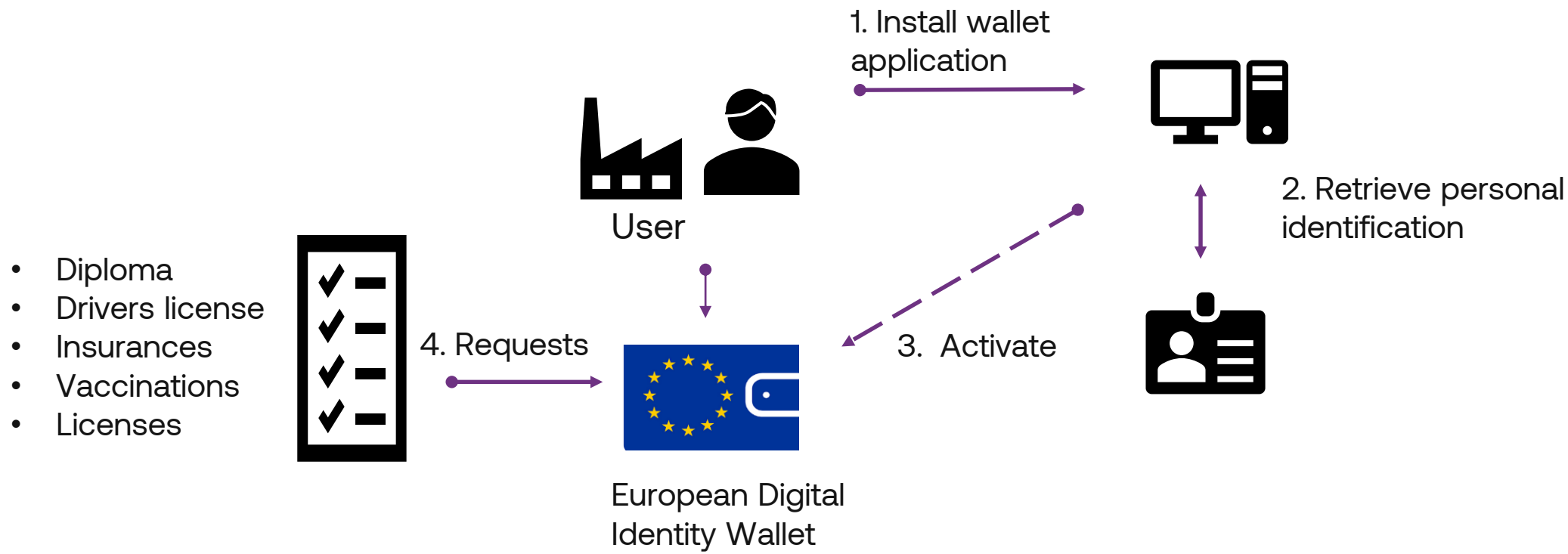
Store and present attestations of attributes

E.g. present educational diplomas/reports for enrolling at university; present your driving license for renting a car

Sign/seal electronically

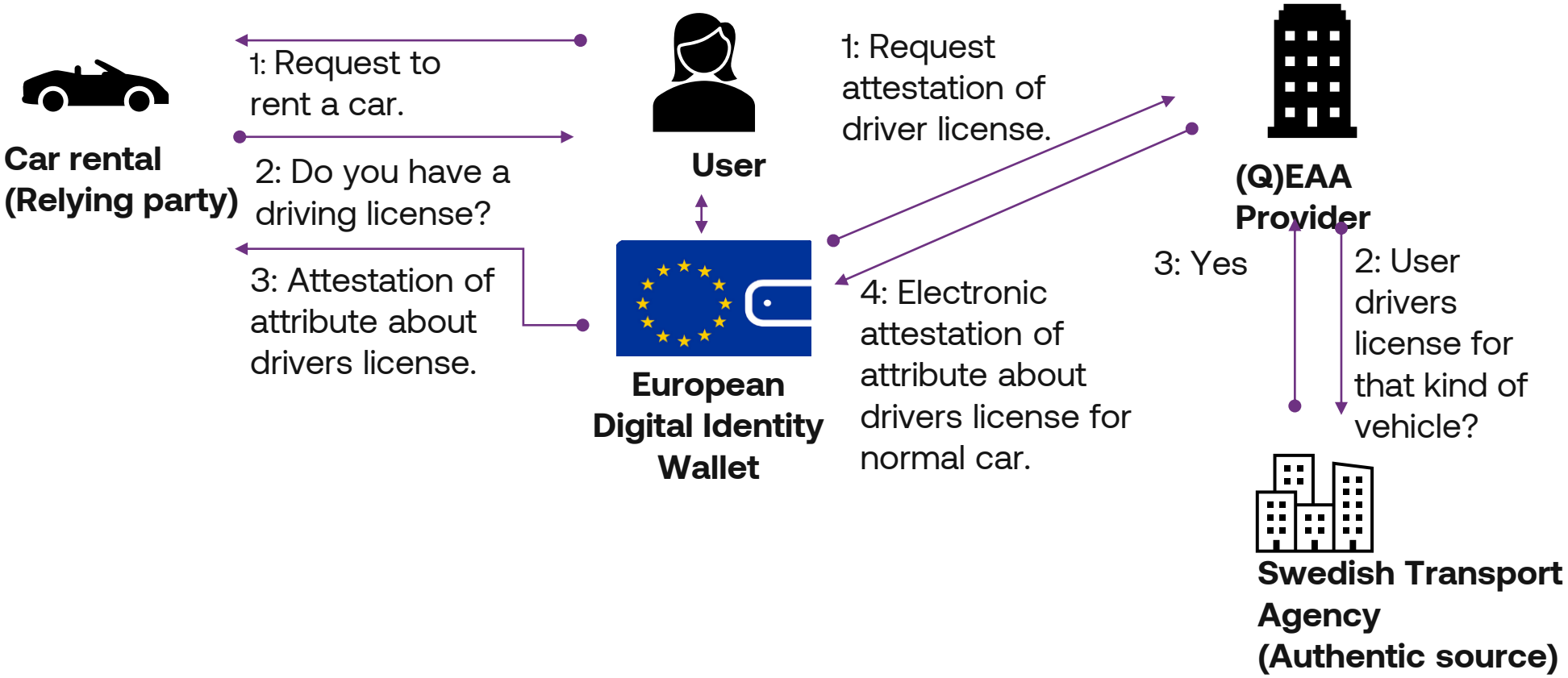
E.g. sign an employment contract to start a new job; authorise a payment

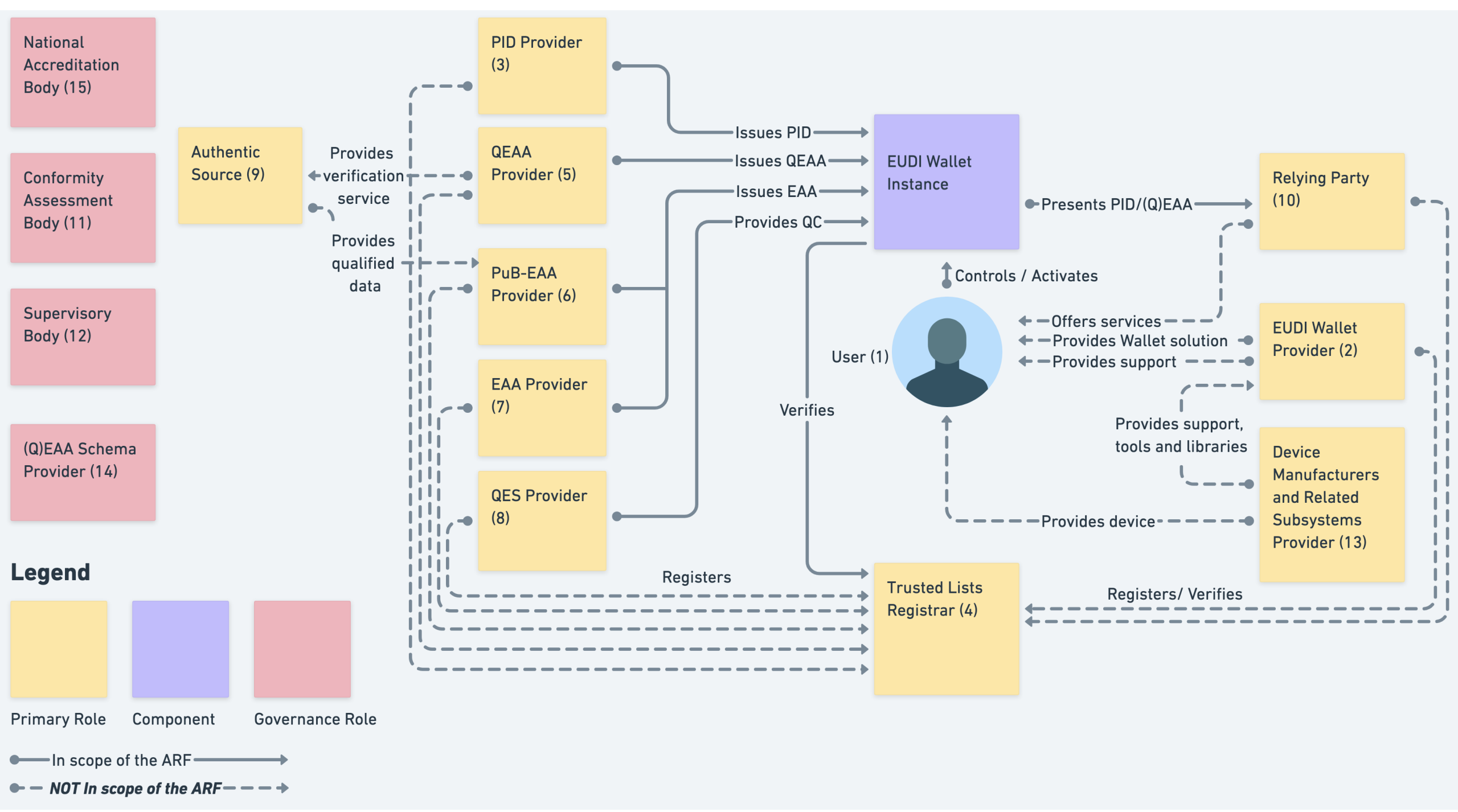
A European Digital Identity Wallet

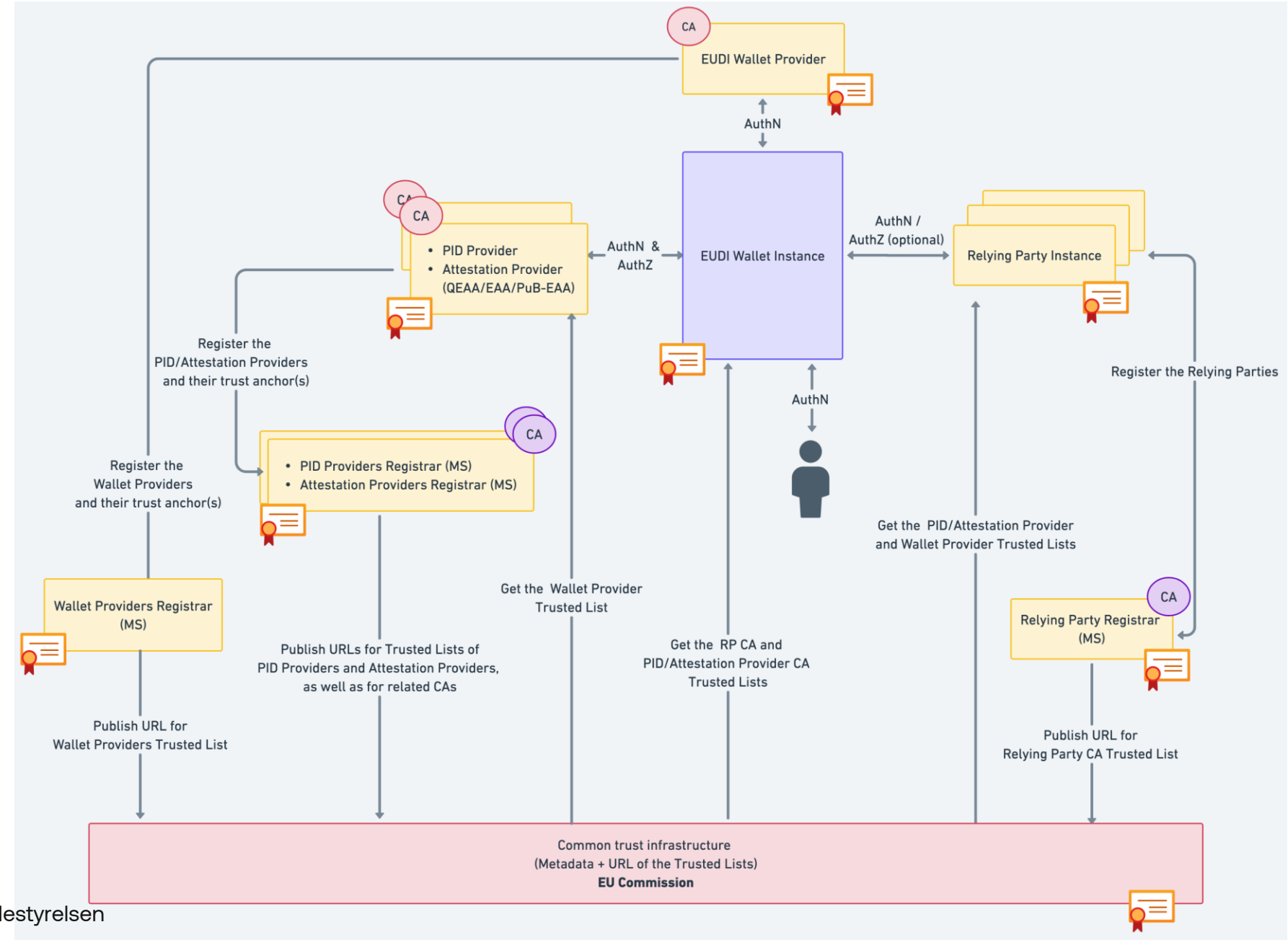


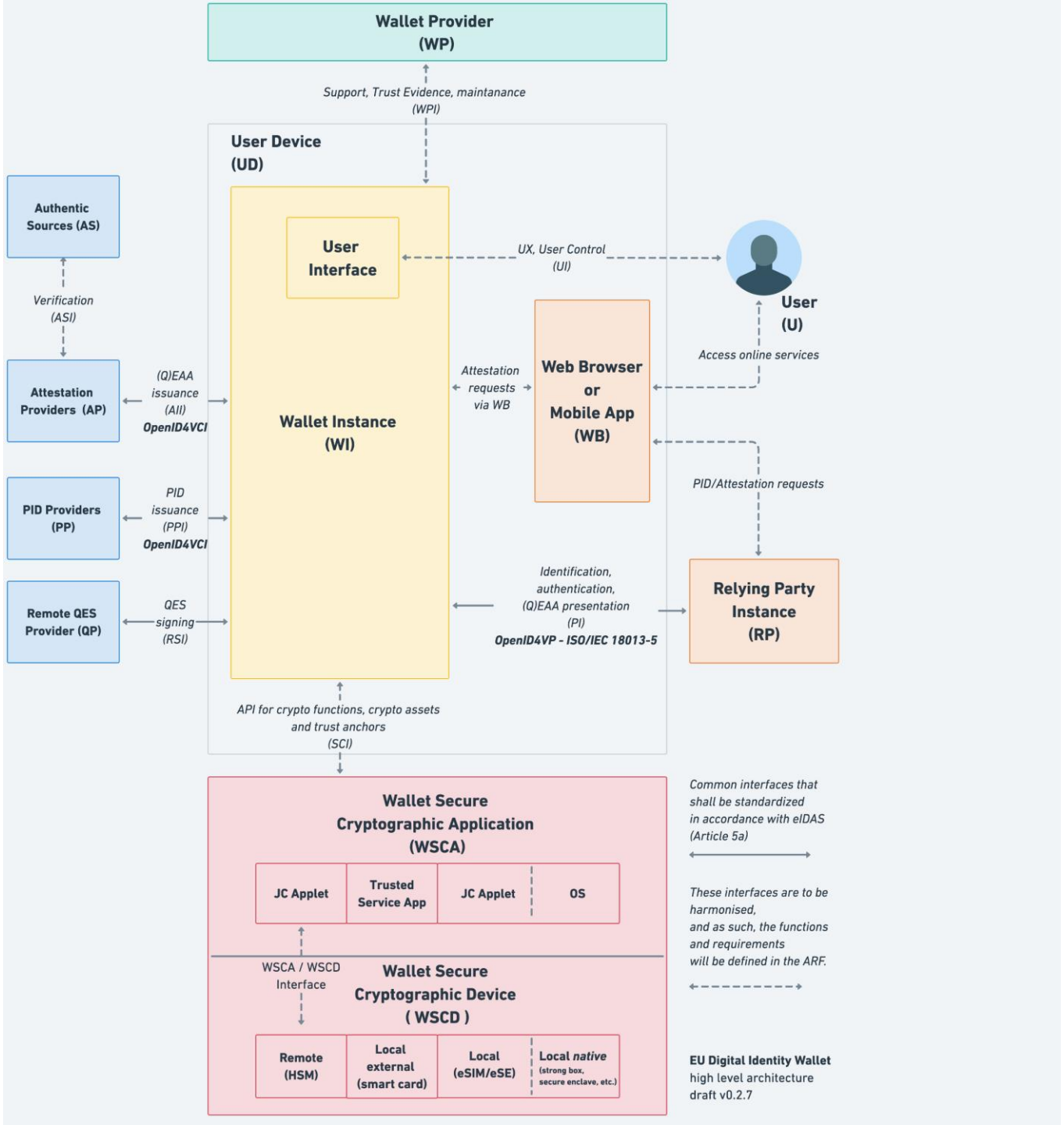
- Diploma
- Drivers license
- Insurances
- Vaccinations
- Licenses

Using a European Digital Identity Wallet




National Accreditation Body (15)
Conformity Assessment Body (11)
Supervisory Body (12)
(Q)EAA Schema Provider (14)
Authentic Source (9)
Provides verification service
Provides qualified data
PID Provider (3)
QEAA Provider (5)
PuB-EAA Provider (6)
EAA Provider (7)
QES Provider (8)
Issues PID
Issues QEAA
Issues EAA
Provides QC
EUDI Wallet Instance
Presents PID/(Q)EAA
Relying Party (10)
Controls / Activates
User (1)
Offers services
Provides Wallet solution
Provides support
EUDI Wallet Provider (2)
Verifies
Provides support, tools and libraries
Device Manufacturers and Related Subsystems Provider (13)
Provides device
Registers
Trusted Lists Registrar (4)
Registers/ Verifies
Legend
Primary Role
Component
Governance Role
In scope of the ARF
NOT In scope of the ARF


CA
EUDI Wallet Provider
AuthN
CA
CA
• PID Provider
• Attestation Provider
(QEAA/EAA/PuB-EAA)
AuthN &
AuthZ
EUDI Wallet Instance
AuthN /
AuthZ (optional)
Relying Party Instance
Register the
PID/Attestation Providers
and their trust anchor(s)
AuthN
Register the Relying Parties
CA
• PID Providers Registrar (MS)
• Attestation Providers Registrar (MS)
Register the
Wallet Providers
and their trust anchor(s)
Get the PID/Attestation Provider
and Wallet Provider Trusted Lists
Wallet Providers Registrar
(MS)
Get the Wallet Provider
Trusted List
CA
Relying Party Registrar
(MS)
Publish URLs for Trusted Lists of
PID Providers and Attestation Providers,
as well as for related CAs
Get the RP CA and
PID/Attestation Provider CA
Trusted Lists
Publish URL for
Wallet Providers Trusted List
Publish URL for
Relying Party CA Trusted List
Common trust infrastructure
(Metadata + URL of the Trusted Lists)
EU Commission


Wallet Provider
(WP)
Support, Trust Evidence, maintanance
(WPI)
User Device
(UD)
Authentic
Sources (AS)
Verification
(ASI)
Attestation
Providers (AP)
(Q)EAA
issuance
(AII)
OpenID4VCI
PID Providers
(PP)
PID
issuance
(PPI)
OpenID4VCI
Remote QES
Provider (QP)
QES
signing
(RSI)
User
Interface
Wallet Instance
(WI)
UX, User Control
(UI)
User
(U)
Access online services
Attestation
requests
via WB
Web Browser
or
Mobile App
(WB)
PID/Attestation requests
Identification,
authentication,
(Q)EAA presentation
(PI)
OpenID4VP - ISO/IEC 18013-5
Relying Party
Instance
(RP)
API for crypto functions, crypto assets
and trust anchors
(SCI)
Wallet Secure
Cryptographic Application
(WSCA)
JC Applet
Trusted
Service App
JC Applet
OS
WSCA / WSCD
Interface
Wallet Secure
Cryptographic Device
(WSCD)
Remote
(HSM)
Local
external
(smart card)
Local
(eSIM/eSE)
Local native
(strong box,
secure enclave, etc.)
Common interfaces that
shall be standardized
in accordance with eIDAS
(Article 5a)
These interfaces are to be
harmonised,
and as such, the functions
and requirements
will be defined in the ARF.
EU Digital Identity Wallet
high level architecture
draft v0.2.7

Responsibilities within Sweden for the EUDI

- Agency for digital government (Digg), provide and recognise wallets
- Digg provide personal identification data for natural persons
- Swedish Companies Registration office provide personal identification data for legal persons
- The Swedish Defence Material Administration cybersecurity certification of wallets
- Swedish Post and Telecom Authority, supervision of wallets and register of relying parties to the wallet

Timeline for the European Digital Identity Wallet

Once the first implementing acts enters in to force the MS have 24 month to provide wallets.

20 May 2024
eIDAS2 entered in to force

21 November 2024
First set of implementing acts for the wallets

Nov/dec 2026
Start of usage of wallets

EU Digital Identity Wallet Milestones

Legislative Process
Adoption - Ongoing work on Implementing Acts (IAs)

Publication of the Regulation in the Official Journal on April 30 and entry into force on 20 May 2024

Wallet technical specification
Published ARF 1.3, pending ARF 1.4

Published the Architecture Reference Framework (ARF) 1.3, on **GitHub** for public feedback - to be followed by version 1.4. in May

Wallet Prototype (Template)
Released first libraries and software components

Published first release of libraries and software components on GitHub, to be followed by regular releases based on feedback from pilots and updates to the ARF

Large-Scale Pilots
Approaching 1-year milestones and deliverables

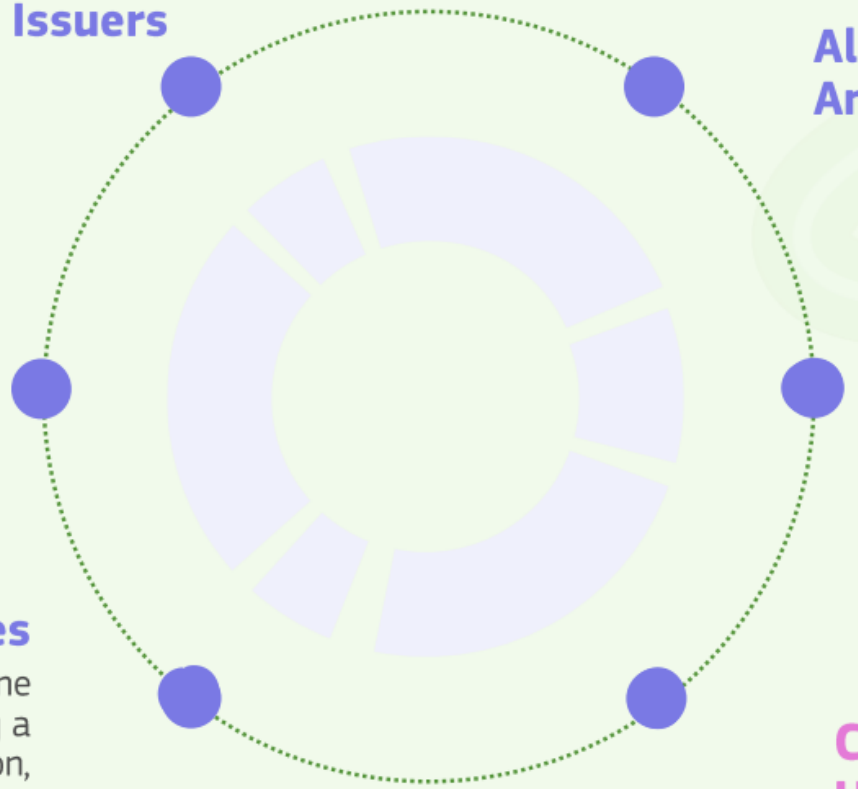
The 4 LSPs are **working towards 1-year milestones and deliverables**

Wallet Prototype Codes published 7 March (GitHub)

Main Functionalities

APPs for Verifiers and Issuers

All Mobile Platforms – Android & iOS



Identification and Authentication

Proximity and Remote

Support for Pilot Use Cases

Mobile Driving License, accessing online public and private services, opening a bank account, SIM registration, payments authorization, authenticating a third-party service to sign documents ..

Continuous Feedback and Updates

Use-cases

- **Mobile Driving Licences (mDL) –** for online and physical interactions
- **Opening a Bank Account –** to verify a user's identity when opening a bank.
- **SIM Registration –** Wallet to prove their identity in pre- and post-paid SIM card contract registration
- **eSignatures** - provide a secure digital signature when signing contracts online
- **Accessing government services – to** file taxes or apply for supports
- **ePrescription –** identifying **and** providing details of prescription to a pharmacies
- **Payments -** store credentials and facilitate payments in account-to-account and card-based transactions
- **Travelling –** quick airplane boarding and quick border crossings (e.g. by a storing Digital Travel Credentials)
- **Organisational Digital -** business-to-government or business-to-business interactions
- **Freedom of Movement –**social security documents such as European Health Insurance Card
- **Education/Professional Qualification –** educational qualification or professional

Piloted

Piloted by Large Scale Pilots

NOBID CONSORTIUM

A set of Nordic and Baltic countries who, together with Italy and Germany, who are developing a large-scale pilot for the payment use case in the EU Digital Wallet.

 # PAYMENTS

Potential
For European Digital Identity

Potential is a secure digital ID that will allow citizens to quickly and securely prove their identity as part of their online citizenship procedures.

 # MOBILE DRIVING LICENSE

 # ACCESS GOV SERVICES

 # OPEN BANK ACCOUNT

 # HEALTH

 # CONTRACTS

 # SIM REGISTRATION

EWC

The EWC aims to harness EU digital identity benefits for Digital Travel Credentials across Member States, building on the Reference Wallet Application for this specific use case.

 # PAYMENTS

 # TRAVEL

 # ORGANISATION ID

DC4EU

DC4EU supports the education and social security sectors by integrating cutting-edge digital services across Europe within a cross-border trust framework.

 # EDUCATION

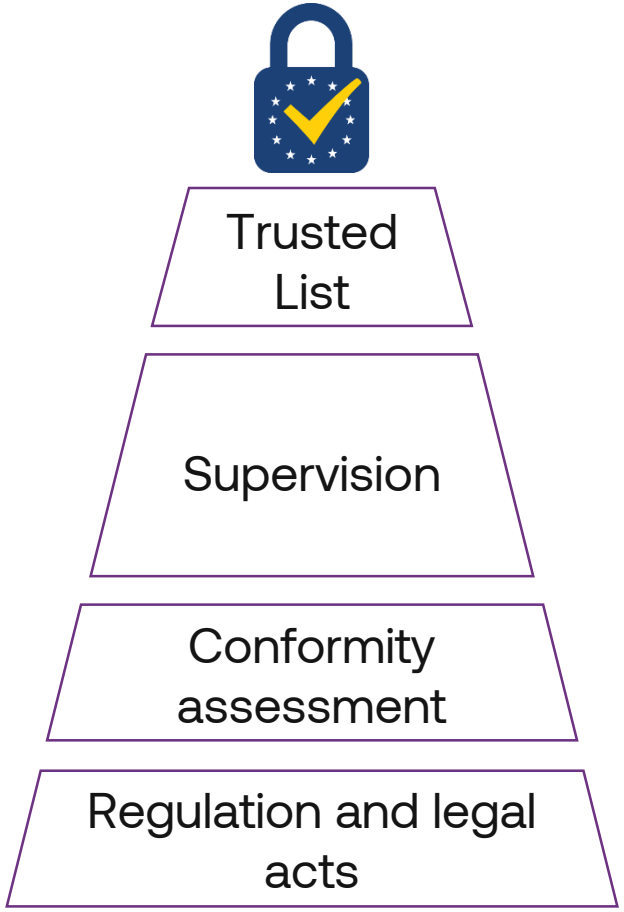
 # SOCIAL SECURITY

Ready ?

Visit our website and discover how the Wallet works.

Regulated trust services and trust model for trust services

Trust model for qualified trust service provider



Trusted List

Current technical and legal status

Supervision

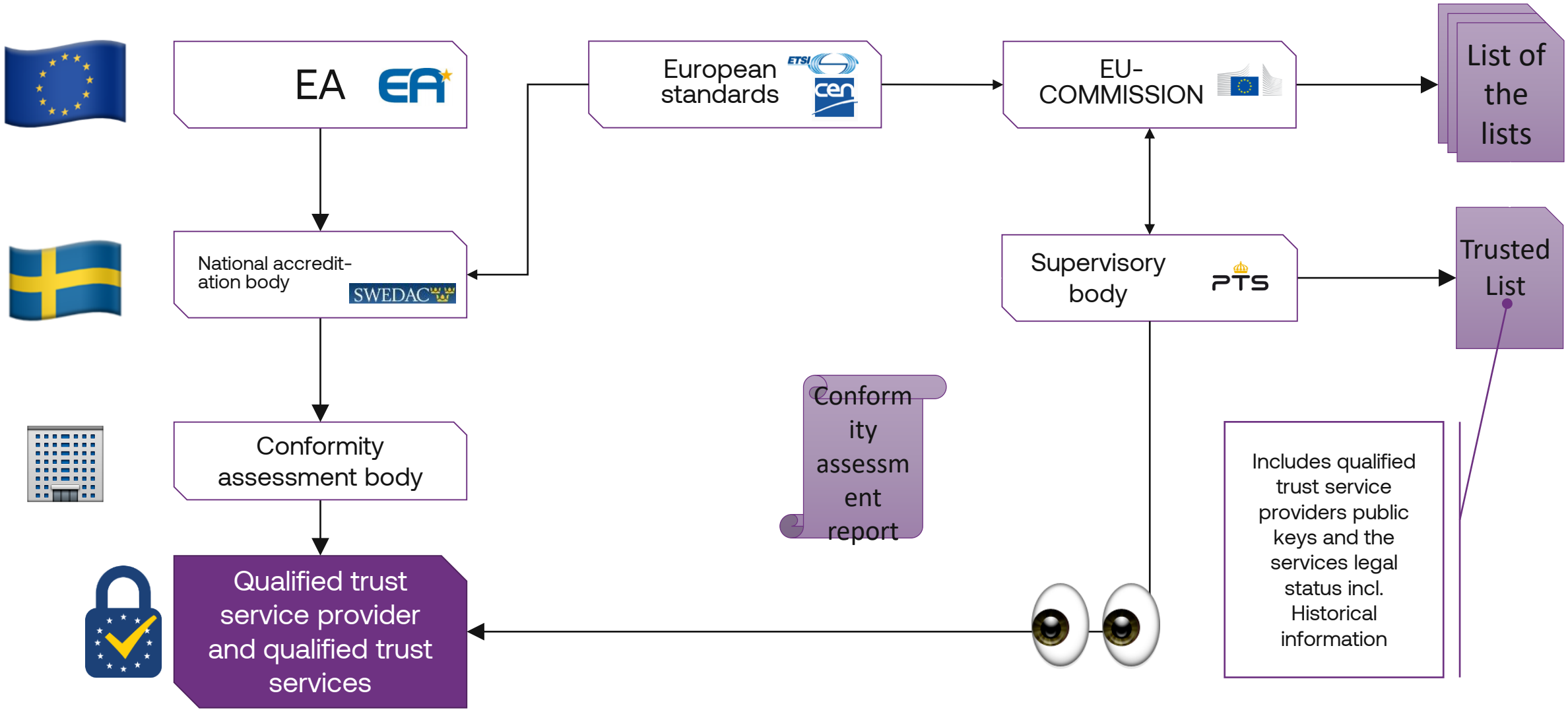
QTSP under post-incident and thematic supervision

Conformity assessment

- IT-products (HSM-module, QSCD etc.)
- Conformity assessment of provider and trust service

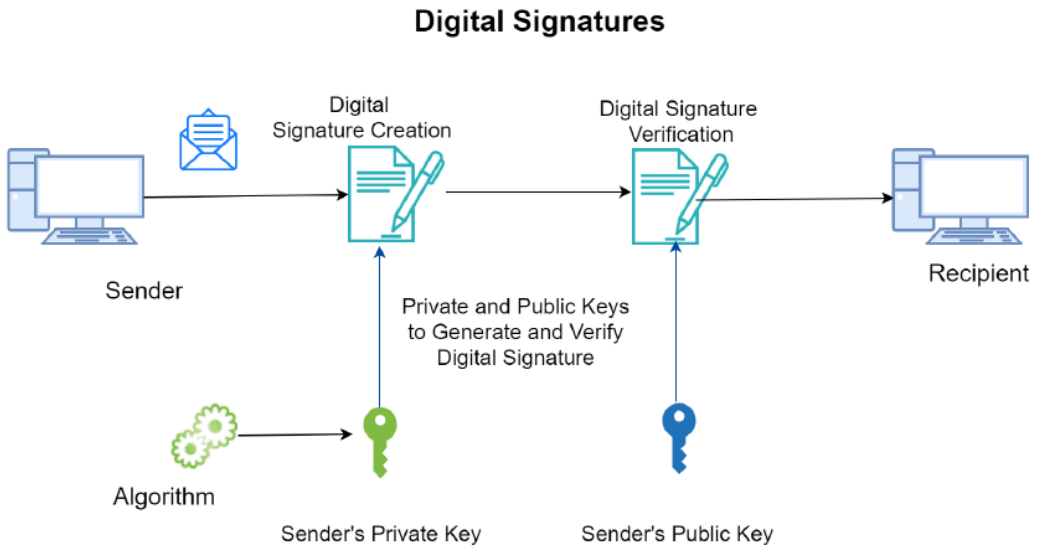
Regulation and legal acts

- eIDAS-regulation
- National eIDAS-law
- PTS guidelines


EA
European standards
EU-COMMISSION
List of the lists
National accredit-ation body
SWEDAC
Supervisory body
PTS
Trusted List
Conformity assessment body
Conformity assessment report
Qualified trust service provider and qualified trust services
Includes qualified trust service providers public keys and the services legal status incl. Historical information

Electronic signatures

- Basic electronic signature
  - A name under an e-mail or fax
- Advanced electronic signature
- Qualified electronic signatures



Advanced electronic signatures

An advanced electronic signature shall meet the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

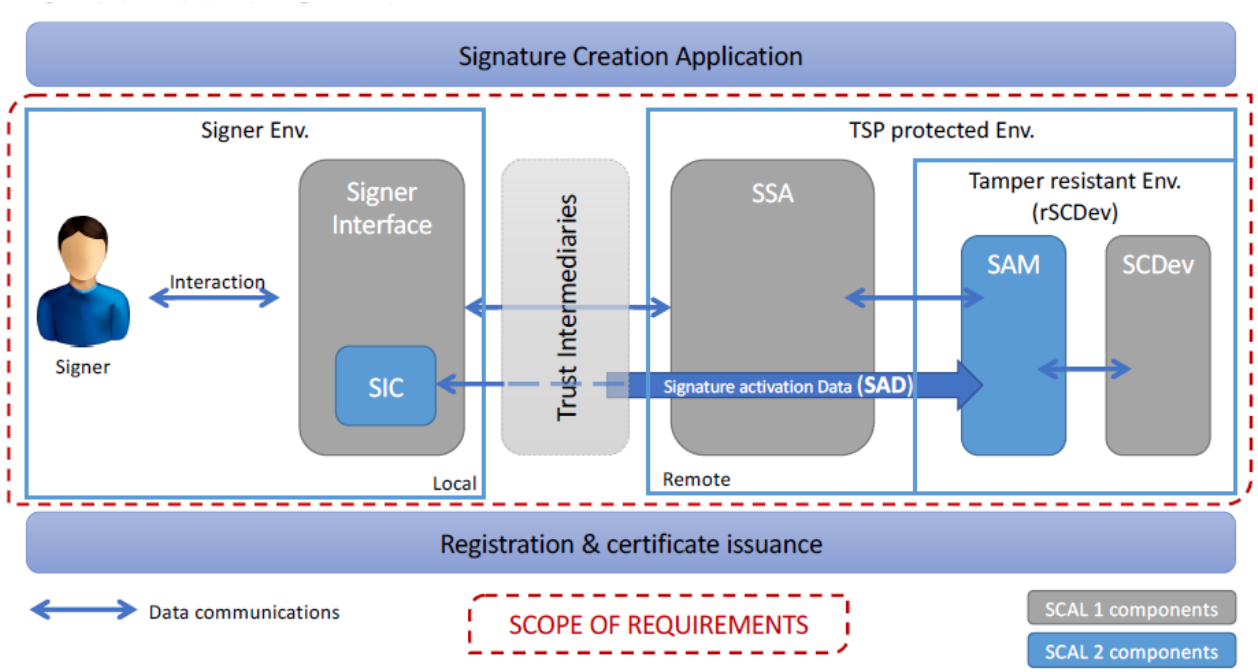
(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Qualified electronic signatures

- A qualified electronic signature is an advanced electronic signature
- Done by a qualified signature creation device based on a qualified certificate for electronic signatures

Qualified signature and seal creation device QSCD

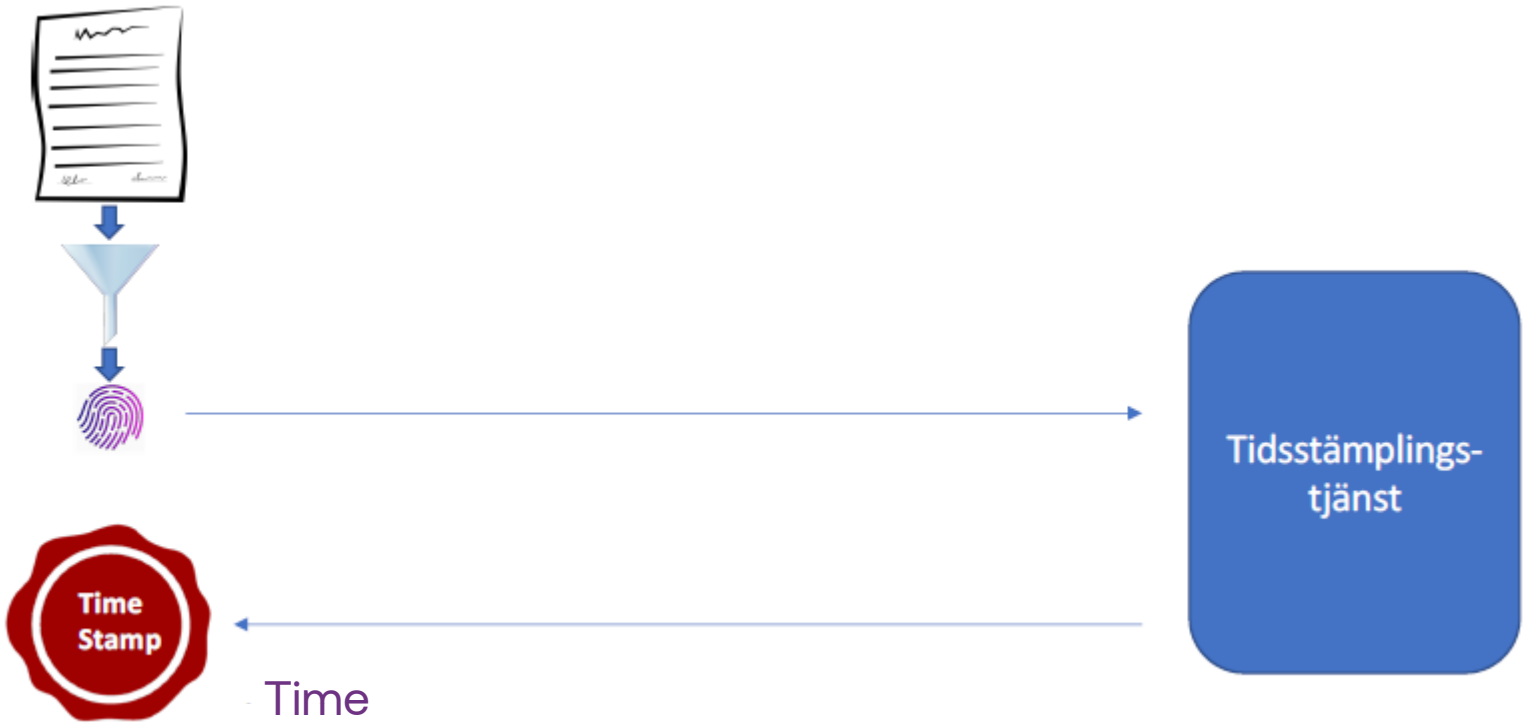
- A device that meets the requirements in the regulation
- A protected storage or generator for cryptographic keys
- A smart card or hardware security module (HSM)
- Evaluated according to standardized common criteria protection profiles
- The profiles that shall be used in an implementing decision on standards for security assessments of QSCD



Electronic seals

- It is basically the same as signatures but for organisations
- The regulation includes advanced and qualified electronic seals
- The difference between the advanced electronic signature and seal is that the certificate used for the signature is issued to a physical person and for seals to an organisation

Timestamping



Time
Issuer
Hash
Timestamp policy

Validation services

- The issuer of the certificate for seal or signature is trusted
- Is the certificate valid or was it valid when signed or sealed
- Is the certificate revoced or was it revoced when the signature or seal was created
- Is the signed content unchanged since the seal or signature

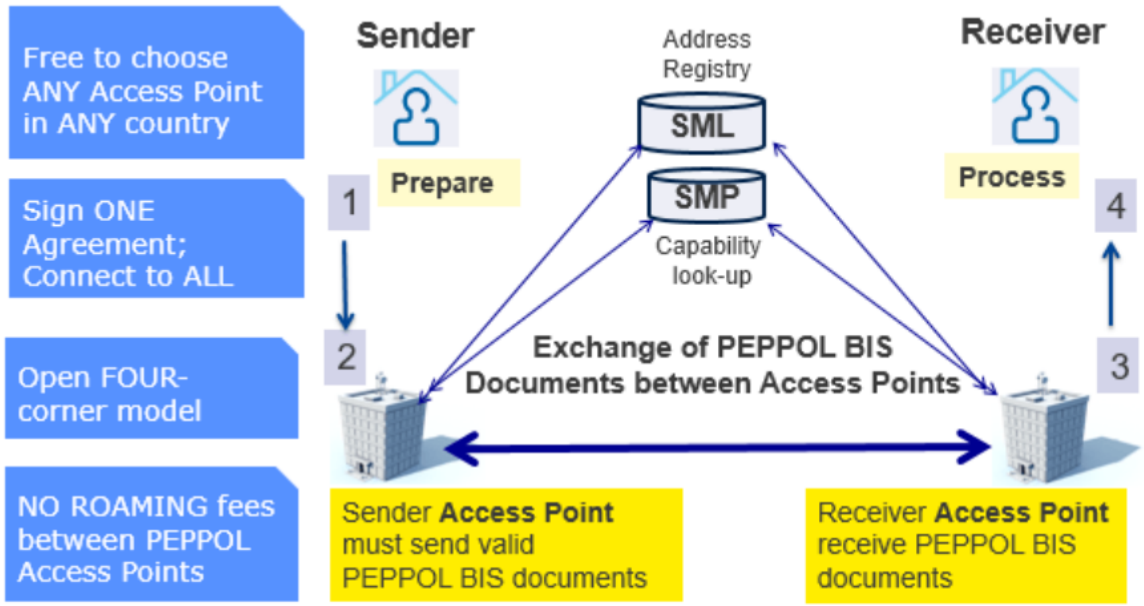
- Deliver the result in a trusted way, signed or sealed by the validation service

Preservation services

- When algorithms are no longer trusted
- Use different technology to keep a signature or seal secured long time
- procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period

Electronic registred delivery services

- a service to transmit data between third parties by electronic means
- provides evidence relating to
  - the handling of the transmitted data,
  - proof of sending and receiving the data,
  - protection of transmitted data against the risk of loss, theft, damage or any unauthorised alterations



Certificate for website authentication

- QWAC - means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued
- eIDAS regulation as complementary to CA-browser forum
- Problem to show that a QWAC are used

Electronic archiving

- Securing electronic documents
- Ensuring the data are preserved that they are safeguarded against loss and alteration
- Changes to medium and form are accepted

Electronic ledgers

- Secure origin of data
- Unique sequential chronological ordering of data records in the ledger
- Record data so any subsequent change to the data is detectabale and ensuring the integrity over time

Electronic attestation of attributes

- Issues attestation of attributes to a wallet at the request of the user
- Make it possible to validate the attestations of attribute
- Make it possible to revoce attestations of attributes
- Could be done by the auhtority responsible for the authentic source or other trusted third parties

Electronic attestation of attributes

Same legal effect as lawfully issued attestations in paper format and recognized by member states

1. Address;

2. Age;

3. Gender;

4. Civil status;

5. Family composition;

6. Nationality or citizenship;

7. Educational qualifications, titles and licenses;

8. Professional qualifications, titles and licenses;

8a. Powers and mandates to represent natural or legal persons

9. Public permits and licenses;

10. For legal persons, financial and company data.

Qualified service for the management of remote qualified electronic signature creation devices

- A service where a qualified trust service provider generates, manages or duplicates the electronic signature or seal creation data, on behalf of a signatory or seal creator.
- Managing QSCD:s for users or other QTSP:s
- Holding a secure environment for HSM:s where users can authenticate to reach their private keys
- Could be used together with the wallet to enable qualified electronic signatures

eIDAS2 and NIS2

eIDAS and NIS2

- Trust service providers fall within the scope of the NIS2 Directive.
- Provisions regarding security, incidents and supervision are now regulated both by NIS2 and eIDAS2.
- NIS2 was supposed to have been transposed into national law on October 18 at the latest throughout the EU. This has not happened in Sweden.
- The cybersecurity obligations laid down in NIS2 should be considered to be complementary to the requirements imposed on trust service providers under eIDAS.

Why are trusted services covered by NIS?

- NIS2 regulates measures to achieve a high common level of cyber security within the Union, with the aim of improving the functioning of the internal market.
  - Recital 84 NIS2 states that due to the cross-border nature of trusted services, they should be subject to a high degree of harmonisation at Union level.
- Trusted service providers should be able to benefit from the legal framework established by NIS2.
  - Designation of a CSIRT unit responsible for incident handling.
  - Participation of relevant competent authorities in the activities of the cooperation group and the CSIRT network.

  (CSIRT =Computer Security Incident Response Team)

Supervision is carried out by?

- eIDAS = Supervisory body
- NIS = Competent authority

NIS2 and eIDAS security requirements and incident reporting

- Article 19 of eIDAS, which contained security requirements and rules regarding incident reporting, expired on October 18, 2024.
- NIS2 was supposed to replace Article 19 of eIDAS but the Swedish implementation is delayed.
- During the wait for implementation of NIS2 we have:
  - Article 19a eIDAS for non-qualified trust service providers
  - Article 24 (24.2 fa och fb)
  - The Commission Implementing Regulation (EU) 2024/2690. Which is a NIS2 implementing regulation.

NIS2 essential or important entity

- NIS2 divides trust service providers into:
  - Essential entities
  - Important entities
- Essential and important entity have different requirements where essential entities have the hardest requirements.
- Qualified trust service providers are considered essential entities.
- (Non-qualified) Trust service providers can either be essential or important entities depending on there size.
- There is also the possibility to specifically designate an entity as essential.

New obligation for trust service providers

- Under NIS2 entities are required to submit information about themselves to the competent authorities.
- Thanks to this, in the future we will know which companies provide trust services covered by eIDAS.
- Proposal that a penalty fee can be decided in case of non-reporting.

Summary

Summary

- There is a difference between a regulation and a directive (legal force)
- eIDAS is a regulation = **applies automatically and uniformly**
- eIDAS consists of three parts: eID, trust services and EUDIW
- There must be mutual recognition of notified national eID-systems and trust services in the EU.
- Two levels of trust services:
  - eIDAS = Non-qualified trust service provider and qualified trust service provider
  - NIS2 = Essential and important entities
- Qualified trust service providers and essential entities have stricter rules.

Thank you for your attention!

Questions?

bjorn.scharin@pts.se
anna.amundberg@pts.se