-1-

eIDAS 1
eIDAS 2
&
AMLR

A new landscape on the horizon for CDD Data

eIDAS 1.0 (2014)

Digital Identity schemes

- Discretionary notification process (State-controlled)
- Public-sector focus
- High level LoA EU guidelines
- Technical specs remain national
- SAML-based interoperability architecture

eTrust Services

- E-signature & seals + 3 others
- Fully open to private sector
- Accreditation process
- ETSI standards

eIDAS 2.0 (2022)

Digital Identity schemes

- European Digital Identity Wallets (**EDIWs**) in addition to digital identity schemes
- Public & private-sector use
- Accreditation process
- Common technical specifications
- Fully recognised within EU

eTrust Services

- **e-attested attributes** linked to EDIWs
- e-archiving services
- e-ledgers

AMLR (2022)

Customer Due Diligence (CDD)

- Common Identity attribute requirements (natural & legal persons)
- Regulatory technical standards by future AMLA for simplified and enhanced CDD

- Recognition of EDIWs (on a par with ID documents)

- **CDD Data Portability**
- Common rules for '*third party reliance*'
- Common rules for CDD outsourcing

Significant impact for the Financial Sector

SGM Consulting
In cooperation with
eWALLET NETWORK

-2-

eIDAS 2 defines broad EDIW specifications

But more is to come with the 🧰

MUST HAVE	Must be accredited – complies with common specifications	Common specifications co-constructed with eIDAS Expert Group
	Must be issued or ‘approved’ by a Member-State	Digital equivalent of national ID cards & passports
	Must offer ***High*** Level of Assurance	For remote ID-proofing - will likely imply using biometric-based ID-proofing processes (CIR 2015/15002 & ETSI 119 461)
	Must put EDIW users in full control of EDIWs	(who can disagree with this?)
	Must be accepted for identity-proofing by relying parties offering **financial** and other key services as well as ‘*very large online platforms*’ (GAFAM + BATX)	Private-sector focus. Cannot be refused by key private and public service providers Relying parties will need to be authenticated
	Must accept eAAs (electronically attested attributes)	Range of attributes goes beyond core ID attributes (extends to status, qualifications, **financial data**, etc)
	Must be free of charge for users	(but not necessarily for other participants)
	Must create Qualified Electronic Signatures/seals	**CRITICAL REQUIREMENTS** **WITH STRUCTURAL IMPLICATIONS**
	Must work offline as well as online	
	Must support Strong Customer Authentication requirements (inc. for payment authorisation)	
NICE (OR VERY NICE) TO HAVE	**Strengthen privacy**	… but will need to communicate the ‘Unique identifier’ whenever required (when?)
	Allow several identity profiles	Use for private/professional context
	Support CBDCs	

High LoA Identity + **Offline & SCA/payment initiation** functionalities + **Signing/countersigning** viewed as key steps for CBDC deployment

-3-

What to make out of this?

- (Very) ambitious proposal + tight implementation timeframe

- The EDIW – a near universal digital credential

All key service providers required to accept EDIWs

- ➢ Core ID attributes
- ➢ 'e-attested attributes' (issued by eIDAS TSPs but available on EDIWs)

- A structural impact on the financial sector (AML/CFT 'obliged entities')

1. Data providing side : Financial institutions can provide electronically attested attributes on EDIWs (IBAN, account information, etc)
   - ➢ Not certain whether this implies TSP status

2. For CDD processes : EDIWs clear substitutes for ID documents
   - ➢ EDIWs avoid *Third party reliance* constraints (FATF recommendation 17)
   - ➢ Key tool for CDD Data portability/reusability but economic model + liability allocation provisions need addressing

3. EDIWs will authorize payments online and offline
   - ➢ Structural impact on PSD2 SCA processes
   - ➢ 'Redirection' no longer needed (inconsistent with offline mode)

The Toolbox process

2nd meeting

eIDAS Expert Group meeting,

27 October 2021

Agenda

- Opening of meeting
- Constitute working groups for the architecture and reference framework
- Use cases: discuss feedback and approach
- Present and discuss feedback on the architecture and reference framework non-paper

2. Working groups

WG participation

WG lead volunteers

- WG 1 (attributes)
  - Netherlands, Denmark
- WG 2 (wallet functionality)
  - Germany, Poland, Sweden, (Austria)
- WG 3 (reliance on wallet)
  - (Austria), (Poland), (Netherlands)
- WG 4 (governance)
  - Italy

WG participants

- Large majority of Member States expressed intent to participate in all four working groups
- Feedback from 24 MS

European Commission

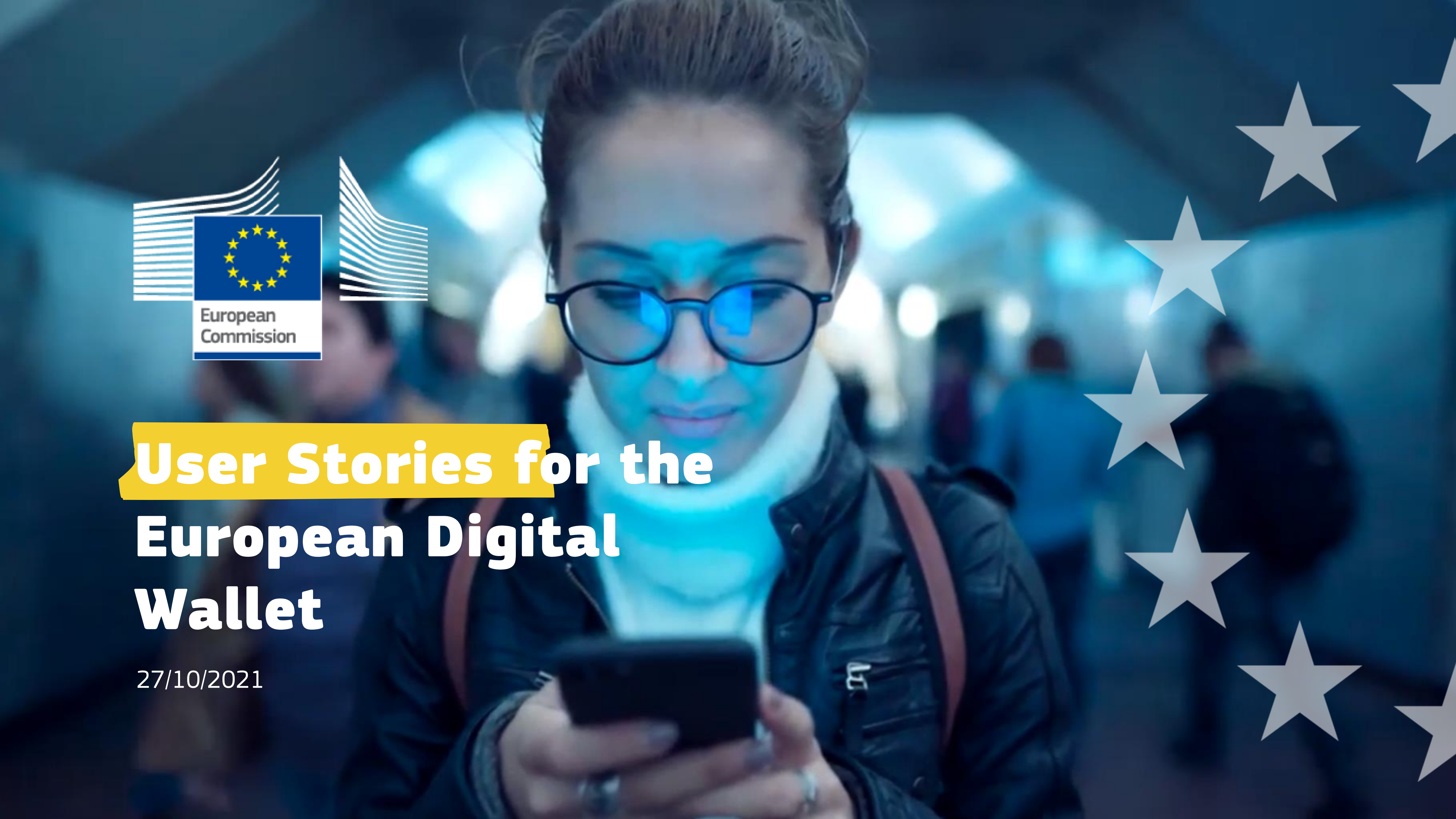
Suggestions on work organisation

“Start with use cases”

- “wallet must support use cases and not vice versa” (EE)
- “advance with use cases before activating working groups” (IT)
- “collect requirements and continue with staged approach” (AT)
- “start with pilot use cases” (PL)

Management

- Based on experience with DCC, “work must be clearly scoped, done in increments, with a clear decision making process for each step” (SE)
- Main principles are derived from eIDAS proposal
- Overall architecture owner is eIDAS expert group (ARF non-paper)
- WG-s reshuffled taking into account basic use cases
- Commission provides Technical Secretariat (?)

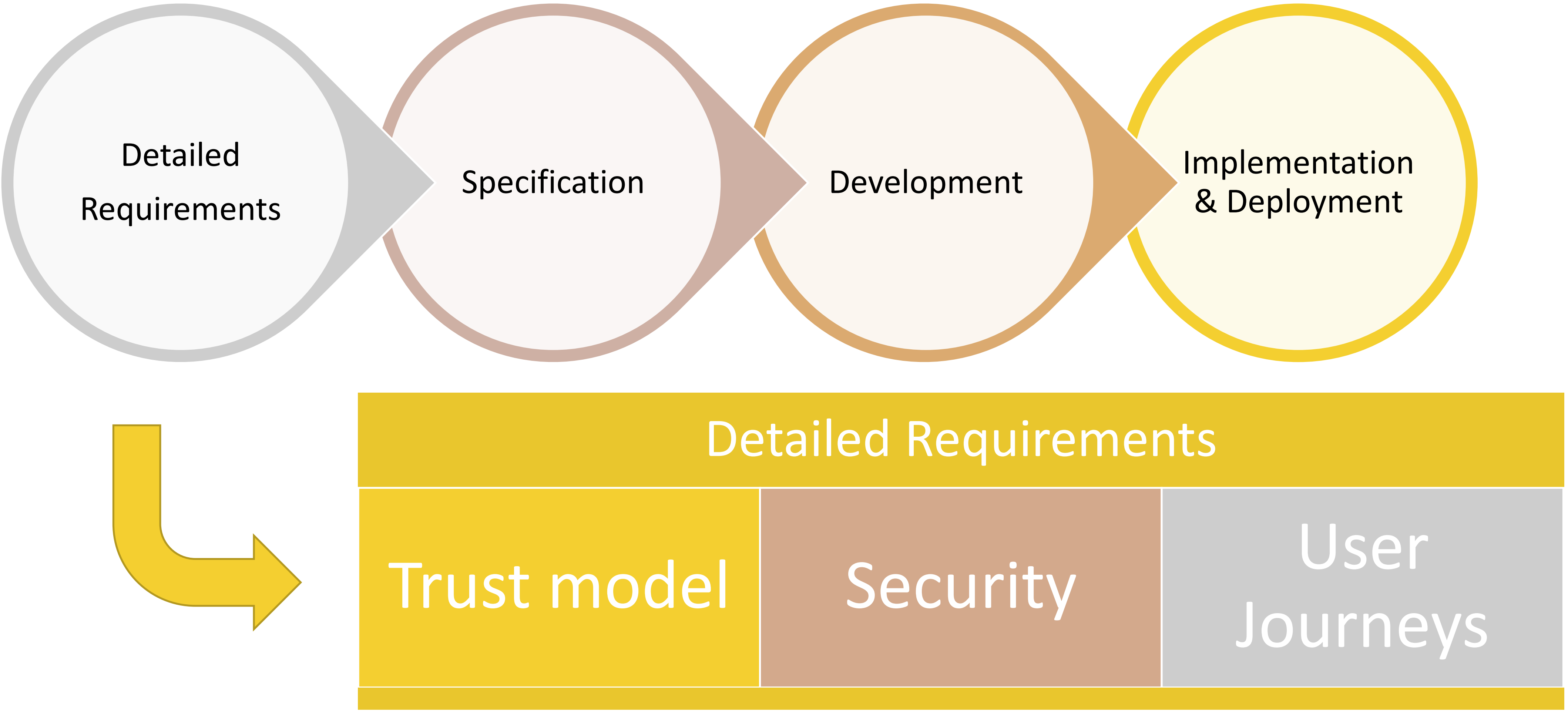


European Commission

User Stories for the European Digital Wallet

27/10/2021

Next Steps towards implementation



Detailed Requirements

Specification

Development

Implementation & Deployment

Detailed Requirements

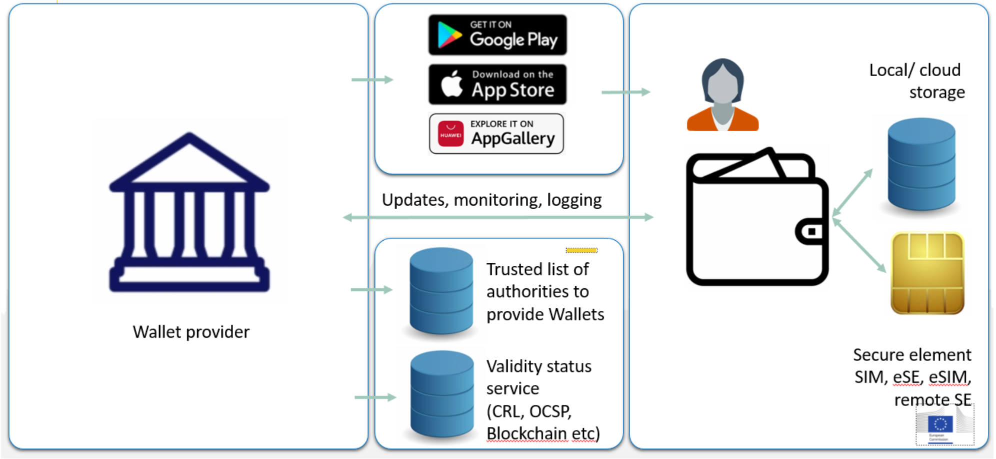
Trust model

Security

User Journeys

User Stories

User story 1: issuing Wallets



Wallet provider

GET IT ON Google Play

Download on the App Store

EXPLORE IT ON AppGallery

Updates, monitoring, logging

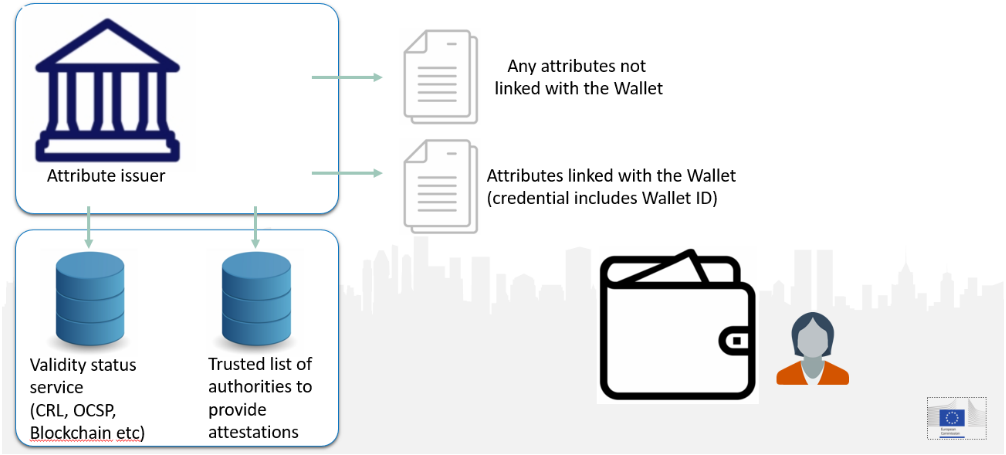
Trusted list of authorities to provide Wallets

Validity status service (CRL, OCSP, Blockchain etc)

Local/ cloud storage

Secure element SIM, eSE, eSIM, remote SE

User story 2: issuing attributes



Attribute issuer

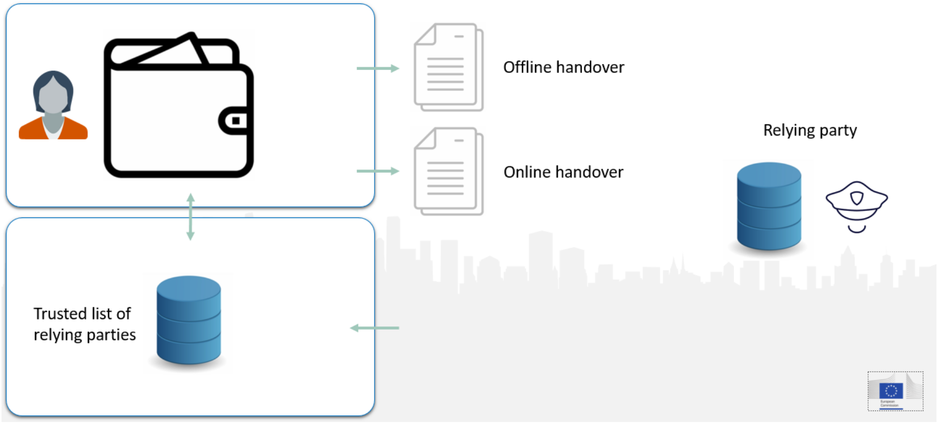
Any attributes not linked with the Wallet

Attributes linked with the Wallet (credential includes Wallet ID)

Validity status service (CRL, OCSP, Blockchain etc)

Trusted list of authorities to provide attestations

User story 3: providing/ presenting credentials



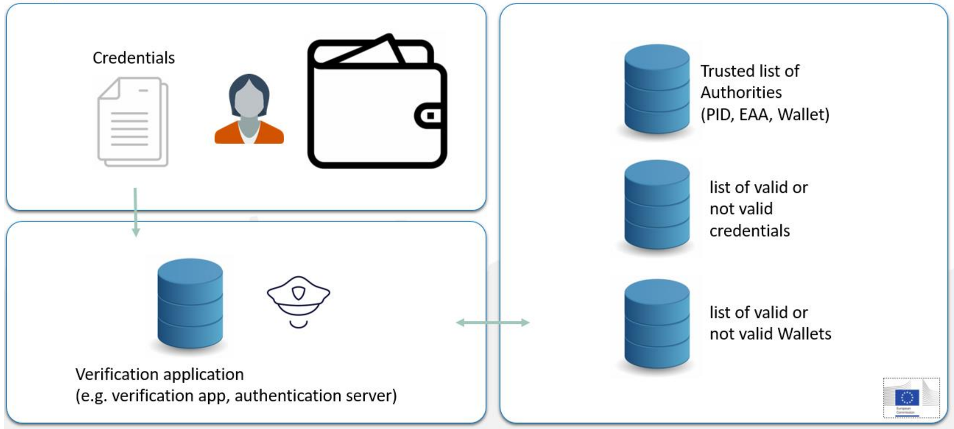
Offline handover

Online handover

Relying party

Trusted list of relying parties

User story 4: authentication of credentials



Credentials

Verification application (e.g. verification app, authentication server)

Trusted list of Authorities (PID, EAA, Wallet)

list of valid or not valid credentials

list of valid or not valid Wallets

Detailing the Lifecycle into User journeys

Trusted Accreditation Organisation

Issuer

Support Infrastructure

Holder

Relying Party

1. On-boarding of actors

- Set up wallets and create Identifiers
- Registration of Wallets
- Accreditation of issuers of electronic Attestations

2. Issuing & storage

- Request issuance of electronic Attestations
- Storage of of electronic Attestations

3. Presentation & verification

- Request of electronic Attestations
- Share Presentation
- Verify Claims

Understanding the roles

Distribution of roles per Member State

MS A

Domain List(s) of trusted Issuers

Gov. Entity

Registers issuers of educational credentials in the Trusted Register of Universities

Issuer

University A

Issues educational credential upon the request of the student

Mobile

Holder

Student

Configures the wallet, requests the issuance of educational credentials and share it with university / employer

MS B

Relying Party

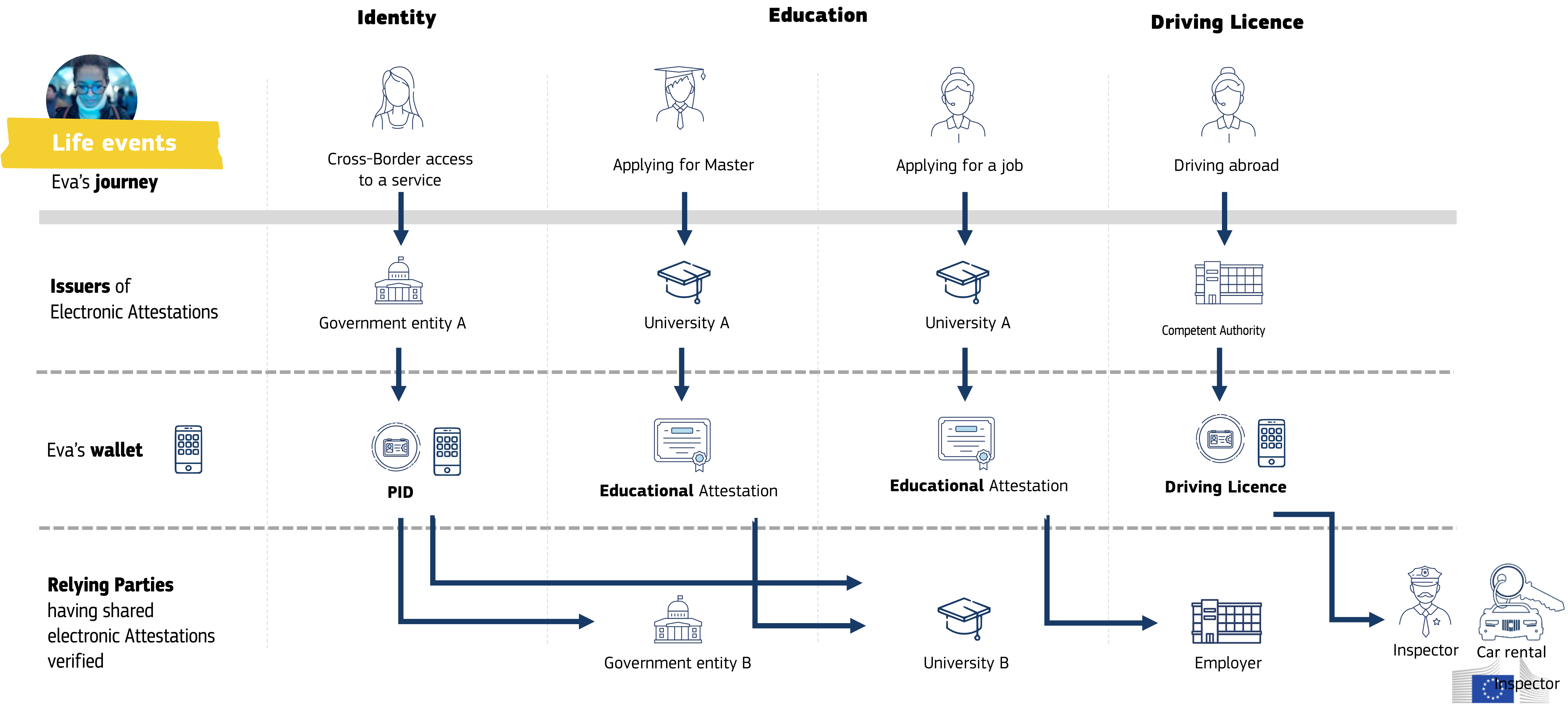
University B

Company

Verifies the educational shared by the student

Electronic Attestation of Attributes applied to use cases

A look at the exchange of electronic Attestations into concrete cases provides further insights



Identity

Education

Driving Licence

Life events

Eva's **journey**

Cross-Border access to a service

Applying for Master

Applying for a job

Driving abroad

Issuers of Electronic Attestations

Government entity A

University A

University A

Competent Authority

Eva's **wallet**

PID

Educational Attestation

Educational Attestation

Driving Licence

Relying Parties having shared electronic Attestations verified

Government entity B

University B

Employer

Inspector

Car rental

Inspector

Use cases as journeys

3. Use Cases

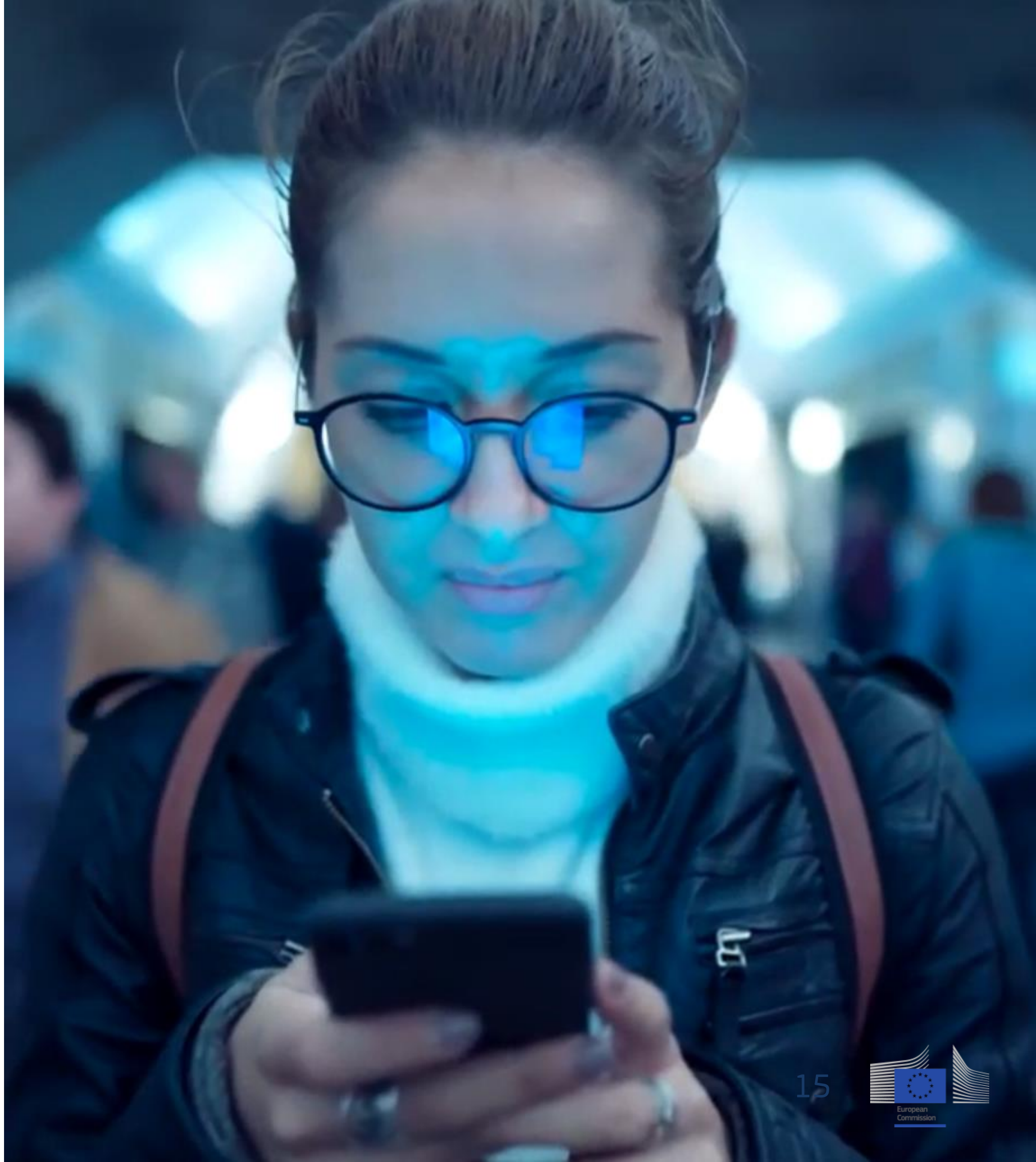
Studying abroad Use Case

What do we want to achieve?

The Diploma Use Case concerns the cross-border verification of educational credentials.

This means that a verifiable attestation (such as a diploma) issued by Member State A can be verified by a university or third party, e.g. an "employer", from Member State B.

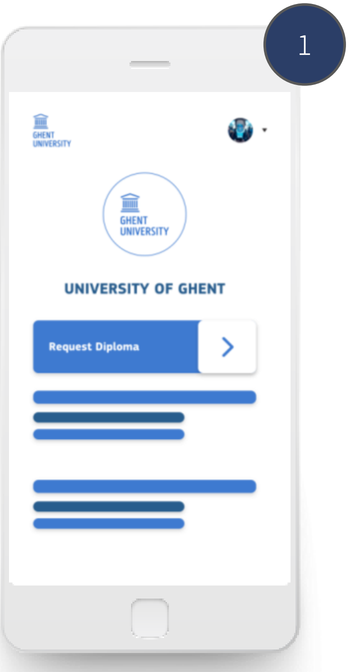
.



Identifying the user journey

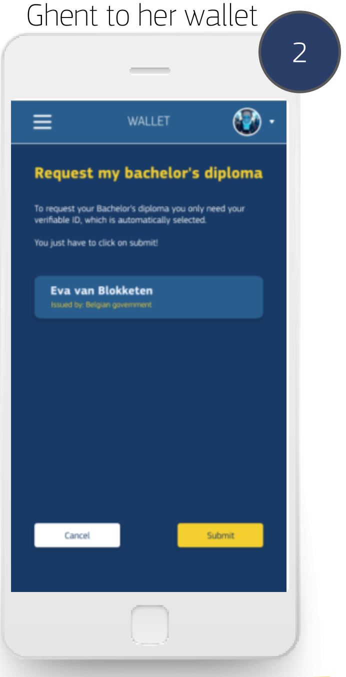
Example (1): Eva requests the issuance of her Bachelor's diploma to the University of Ghent (BE)

Eva initiates the request for the issuance of her Bachelor's Diploma



- Connect to University platform
- Initiate the action

Eva directs the issuance of her Bachelor's Diploma from the University of Ghent to her wallet



Request my bachelor's diploma

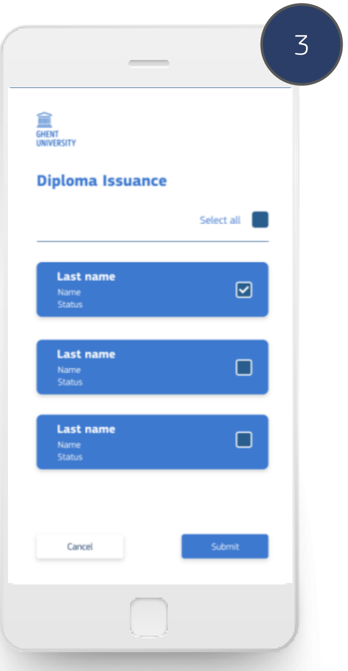
To request your Bachelor's diploma you only need your verifiable ID, which is automatically selected.

You just have to click on submit!

Eva van Blokketen
Issued by: Belgian government

- Select Verifiable ID
- Submit the request

The University of Ghent issues the Bachelor's Diploma

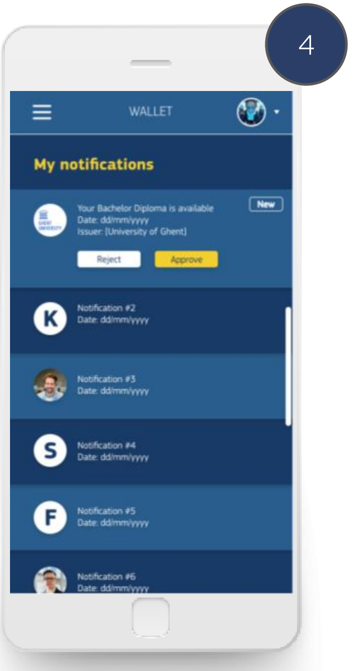


Diploma Issuance

Select all □

Last name Name Status	☑
Last name Name Status	□
Last name Name Status	□

Eva receives and accepts the Bachelor's Diploma.



My notifications

Your Bachelor Diploma is available
Date: dd/mm/yyyy
Issuer: [University of Ghent]

Notification #2
Date: dd/mm/yyyy

Notification #3
Date: dd/mm/yyyy

Notification #4
Date: dd/mm/yyyy

Notification #5
Date: dd/mm/yyyy

Notification #6
Date: dd/mm/yyyy

- Get notification
- Accept the credential
- Store in the wallet.

European Commission

Thank you !