

eID for legal person

State of the art analysis



Table of contents

- Electronic identification context in Europe
- Overview of existing initiatives in Europe (and potentially around the world)
- Synthesis

eID: electronic identification of a natural or a legal person, **or a natural person representing a legal person**

eID scheme: system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons

eID means: material and/or immaterial unit containing person identification data and which is used for authentication for an online service

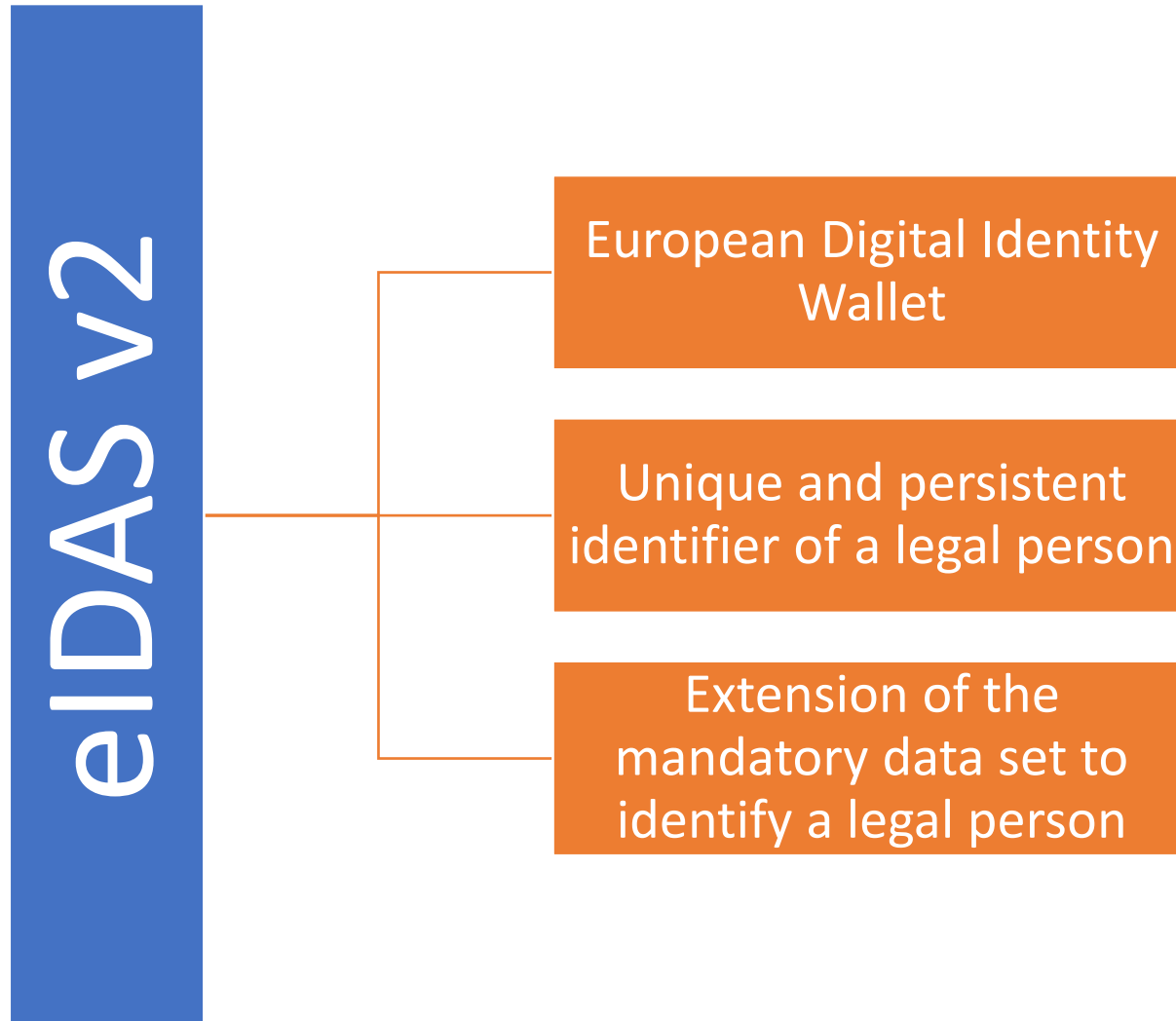
The eIDAS Regulation is accompanied by an implementing act (2015/1502), which allows Member States to define their electronic identification scheme precisely.



Except at the “definition level” (art 3), eIDAS regulation does not explicitly define how to materialize the link between a natural and a legal person

Limits of current regulation

- No real technical standards
- No control on eID means schemes that are not notified: market already offers solutions for the electronic identification of legal persons, but it is not possible to ensure the strength of the processes and the legal acceptance of this identity
- **Various initiatives** in Europe to define:
 - The process to link an eID of a natural person to a legal person
 - The data structure to identify a legal person is not standardized



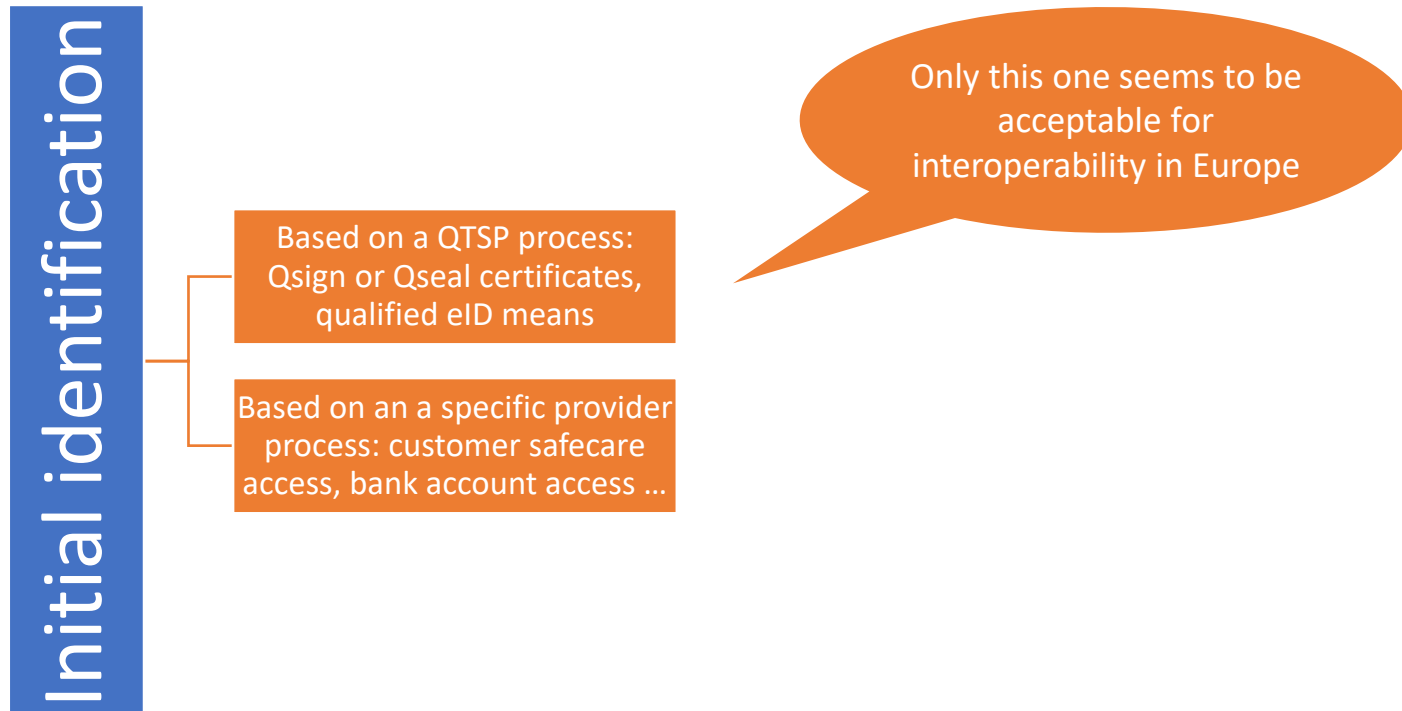
eIDAS v2 extends the identification of legal persons to new services but does not yet technically define the processes for linking a natural person to a legal person, or the conditions for accessing the legal person's data.

The notified identification schemes will have to evolve to consider these elements.

Main challenges to achieve...

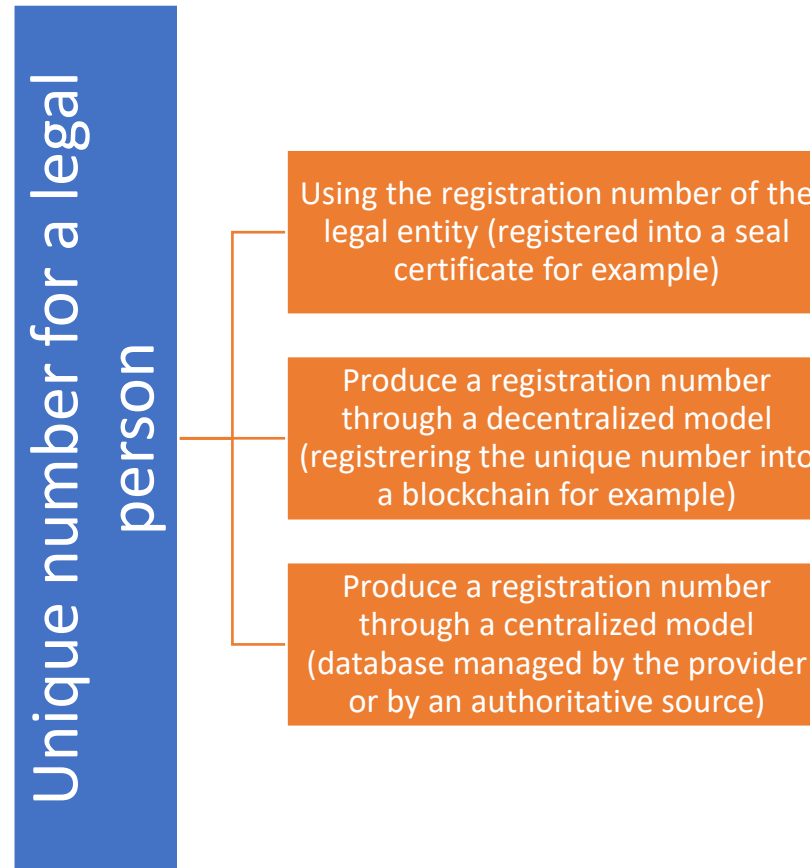
Objectives:

achieve a first robust identification of the natural person representing the legal entity

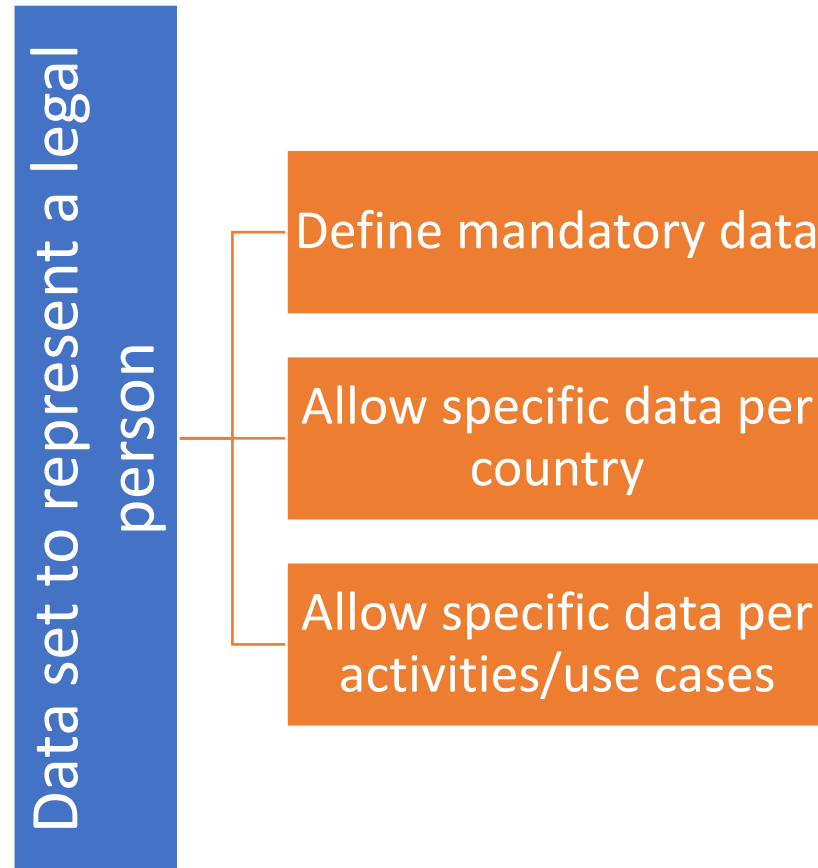


Define the unique identification of a legal person

Objectives: answer to the eIDAS v2 requirement of having a unique and persistent identifier of a legal person



Objectives: Define and shared the data set of information representing the legal person



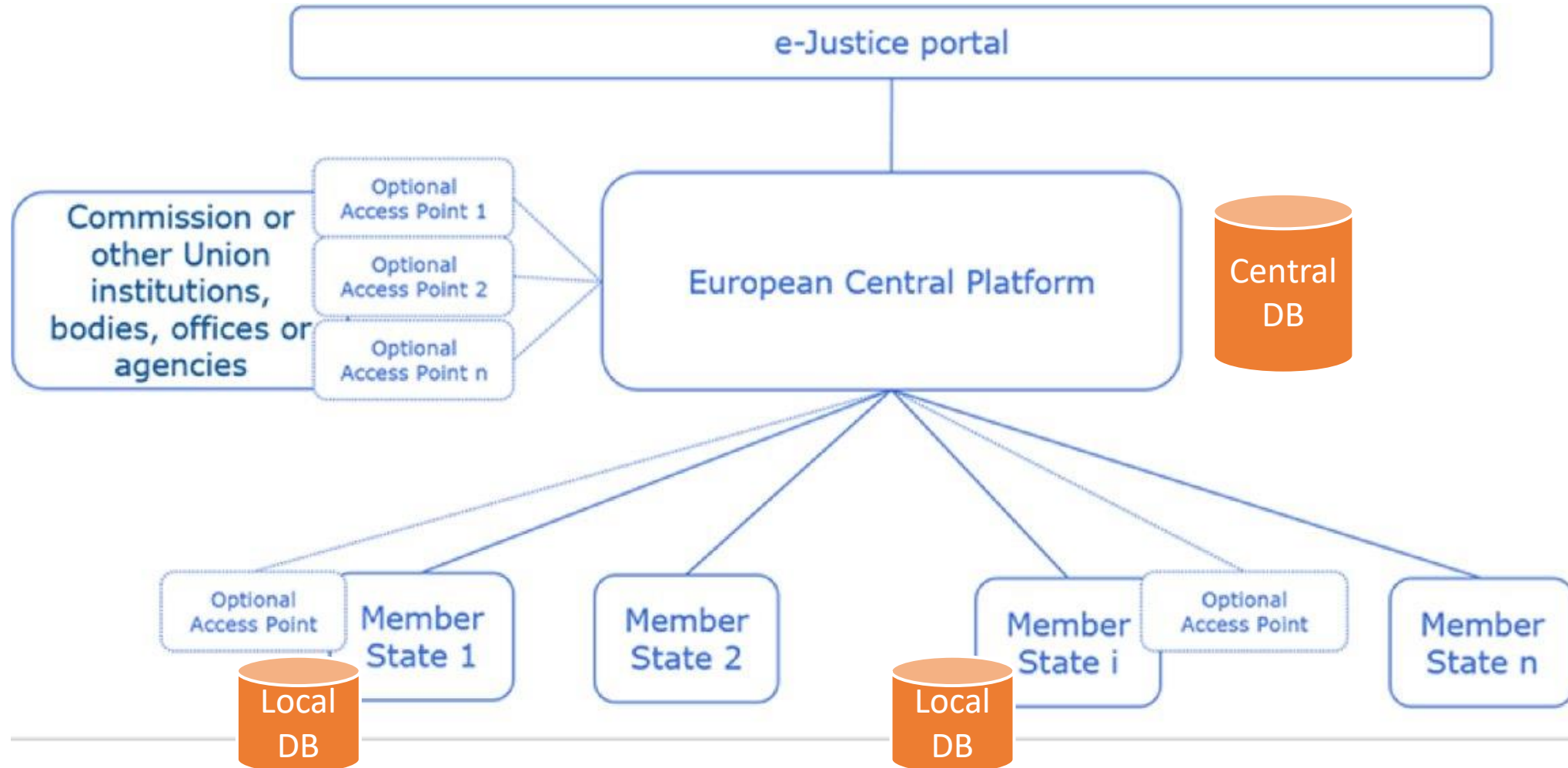
Overview of initiatives in Europe (and potentially around the world)

Norms & standards: CIR (EU)
2021/1042: technical
specifications and procedures
for the system of
interconnection of registers

- Established a BRIS (Business Registers Interconnection System)
- Define functions to create, modify and revoke data of a legal entity
- Define functions to exchange/access to a register between Member States
- Define a structure of an European Identifier for legal entity (EUID)

EUID element	Description	Additional description
Country code	Elements making it possible to identify the Member State of the register	Mandatory
Register Identifier	Elements making it possible to identify the domestic register of origin of the company and of the branch respectively	Mandatory
Registration number	Company/branch number refers to the registration number of the company/branch in the domestic register of origin	Mandatory
Verification digit	Elements making it possible to avoid identification errors	Optional

Norms & standards: CIR (EU) 2021/1042: proposed architecture





Norms & standards: TS
119461: Policy and
security requirements
for trust service
components providing
identity proofing of
trust service subjects

- Based on EN 319401 requirements for managing the service
 - Defined attributes for identify a legal person:
 - Full name
 - Country of registration
 - Unique identifier of the legal person
 - Defined attributes for natural person representing legal person
 - Family name, first name
 - Unique identifier of the natural person
 - Role of the natural person with respect to the legal person
-


















Norms & standards: EN 319412-3: Certificate profile for certificates issued to legal persons & LEI standard

- Profile used by (Q)TSP to produce X509 certificates for legal person
 - No certificate's field to identify the link with a natural person (except the SAN with email data)
 - Identification of the legal person is placed into following fields:
 - OrganizationName: legal name
 - OrganizationIdentifier: contains the eIDAS legal unique identifier following the LEI format (ISO 17442 – worldwide standards) – « LEIXG-<LEI number affected to the legal entity> »
-

LEI structure

- Worldwide database of Legal Entity data set
- 20-character, alpha-numeric code based
- Interface to search LEI status

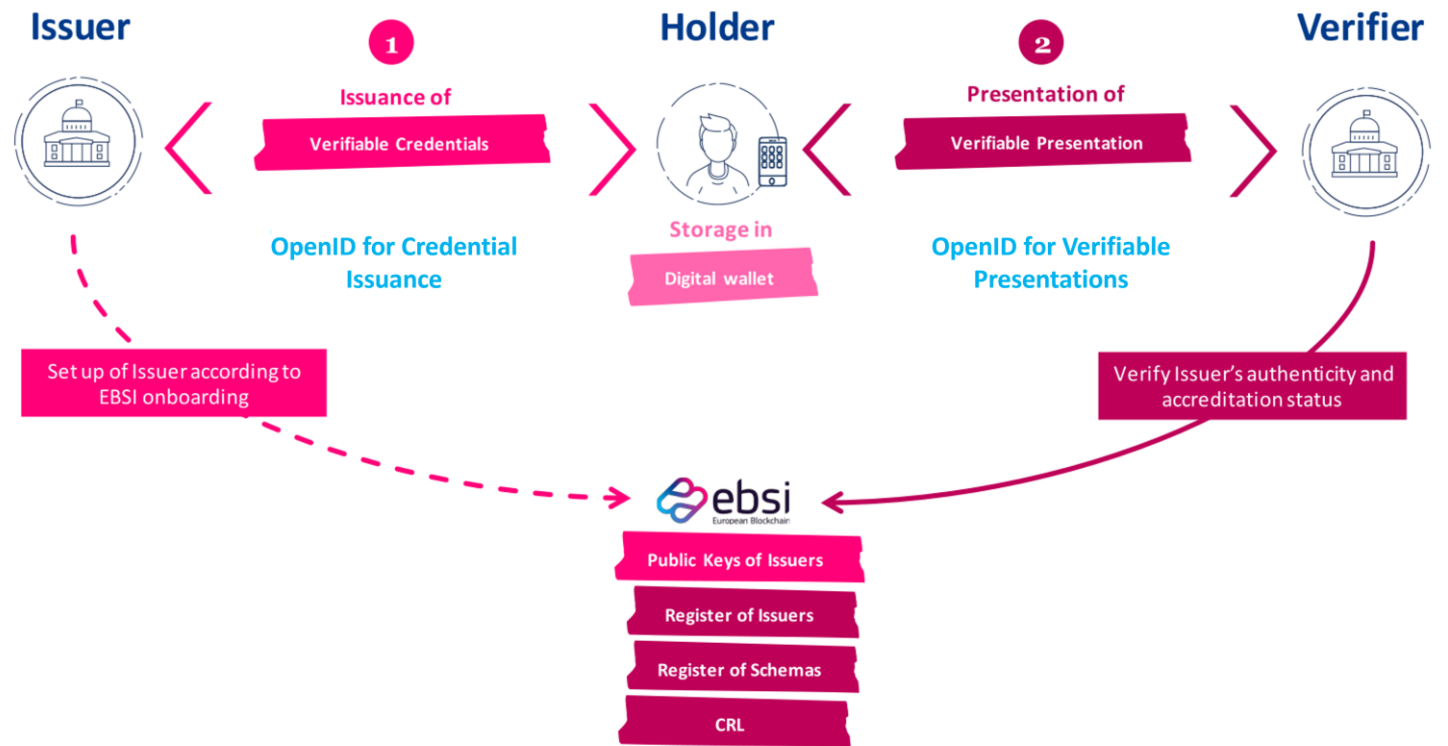
Country ▼	Entity Status ▼	Legal name ▼	LEI ▼	Reg. Status ▼
 France	 ACTIVE	AREVA	9695007B0RXQCHHTGR34	 LAPSED
 France	 ACTIVE	TRIGA INTERNATIONAL	969500H185MFOLUE1B54	 ISSUED
 France	 ACTIVE	FRAMATOME	969500805IIXK0UGWJ07	 ISSUED
 France	 INACTIVE	AREVA FRANCE ACTIONS SALARIES	969500P7GCO1L368DS02	 RETIRED
 France	 INACTIVE	AREVA INTERNATIONAL ACTIONS SALARIES	969500K8CL22H6R19618	 RETIRED

Entity		[1,1]
LegalName	lei:NameType	[1,1]
OtherEntityNames	lei:OtherEntityNamesType	[0,1]
TransliteratedOtherEntityNames	lei:TransliteratedOtherEntityNamesType	[0,1]
LegalAddress	lei:AddressType	[1,1]
HeadquartersAddress	lei:AddressType	[1,1]
OtherAddresses	lei:OtherAddressesType	[0,1]
TransliteratedOtherAddresses	lei:TransliteratedOtherAddressesType	[0,1]
RegistrationAuthority	lei:RegistrationAuthorityType	[0,1]
LegalJurisdiction	lei:JurisdictionCodeType	[0,1]
EntityCategory	lei:EntityCategoryTypeEnum	[0,1]
EntitySubCategory	lei:EntitySubCategoryTypeEnum	[0,1]
LegalForm	lei:LegalFormType	[0,1]
AssociatedEntity	lei:AssociatedEntityType	[0,1]
EntityStatus	lei:EntityStatusEnum	[1,1]
EntityCreationDate	lei:LEIDateTimeProfileGeYear0001	[0,1]
EntityExpirationDate	lei:LEIDateTimeProfile	[0,1]
EntityExpirationReason	lei:EntityExpirationReasonEnum	[0,1]
SuccessorEntity	lei:SuccessorEntityType	[0,*]
LegalEntityEvents	lei:LegalEntityEventsType	[0,1]



European Commission initiative: European Blockchain Service Infrastructure (EBSI)

- Trust chain for validating legal entity information
- Identification based on the principle of verifiable credentials (W3C standard)
- And on the implementation of a dematerialized identifier (DID) with registration in the blockchain
- Process for registering, modifying and revoking a legal entity
- Storage of information relating to the legal entity in the European wallet
- Recording evidence in the blockchain

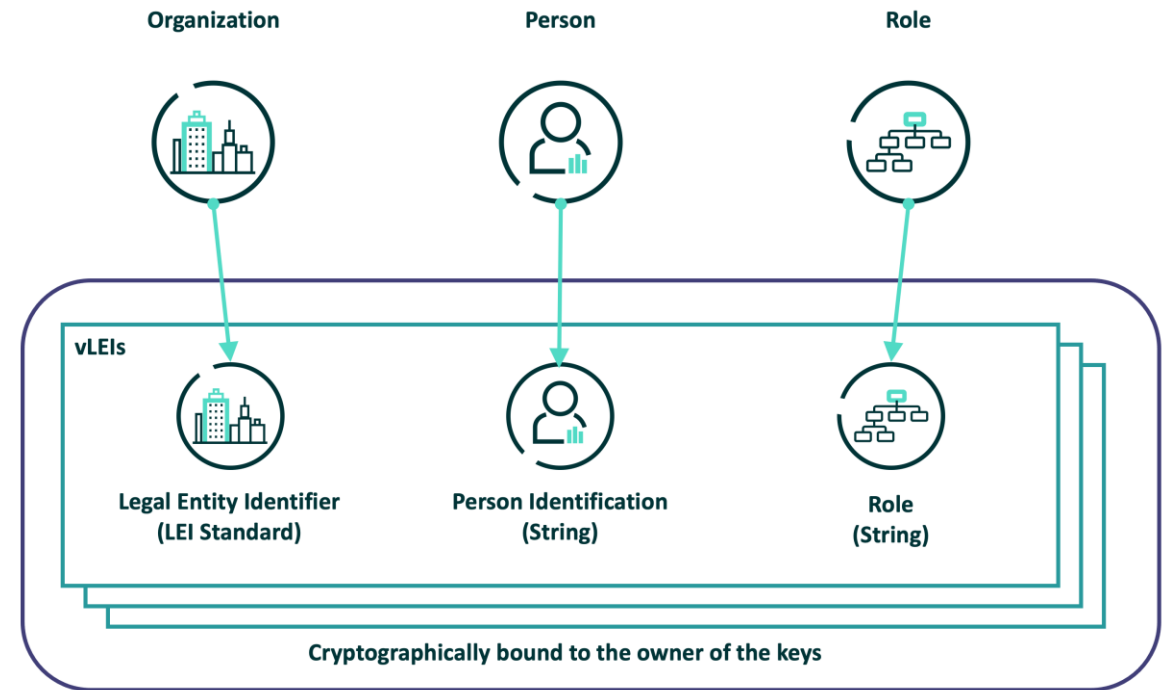


GLEIF initiative

Global Legal Entity Identifier Foundation: support the implementation and use of the Legal Entity Identifier (LEI) and make a verifiable LEI (vLEI) - the secure digital counterpart of a conventional LEI

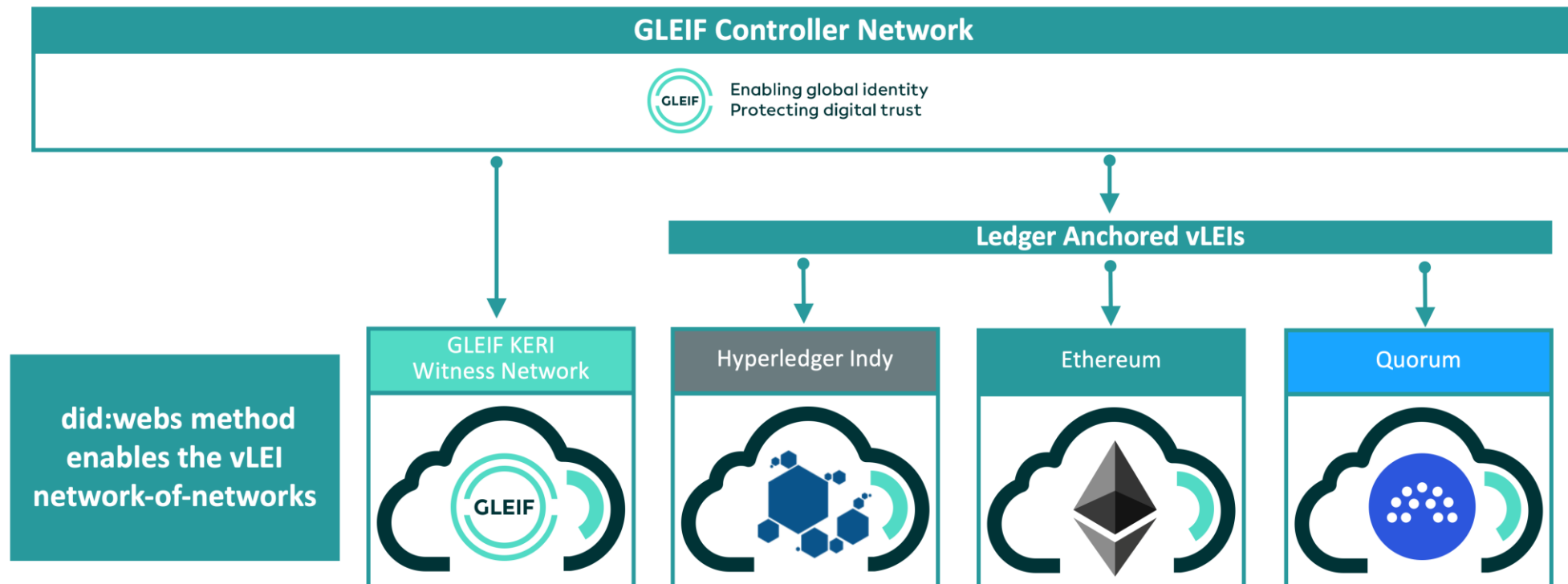
vLEI concept

A trusted organization to validate legal data set of an entity and link to an authorize natural person



vLEI concept

Compatible with any blockchain to register DID objects associated to a legal entity transaction





Netherland
initiative (Eherkenning)
solution based
on a notified
schemes for
legal person

- EHerkenning is a secure and reliable login means
 - Access to over 500 different services and service providers
 - Offer the possibility to manage roles and mandates of people in the organization
- Several level of assurance (eIDAS compliant for substantial and high level)



eHerkenning: level of assurance


	EH2 (eIDAS basic)	EH2+ (eIDAS basic)	EH3 (eIDAS sub.)	EH4 (eIDAS high)
Login method	User name and strong password	2-factor authentication via user name and password, in combination with SMS code or PIN code via a token	2-factor authentication via user name and password, in combination with SMS code or PIN code via a token or app with QR code	Via PKI certificate or 2-factor authentication.
Application procedure	Online with approved supplier	Fully online or Partly online and partly offline (by post)		
Identity check	Copy of a legal ID document (WID)		Via legal ID document (no copy) and face-to-face check. This takes place at a location of your choice Identity check applies for the legal representative, the authorization manager and the user.	
Check of authority	Via Chamber of Commerce registration			
Delivery	Often online, based on a reliable source document	Activation code and password. You will receive the activation code and password separately	Online and offline (for example via registered post)	Offline (from most suppliers). For example via registered post or personal pick-up.



Bulgaria initiative
(eID implementation
act): solution based
on a notified
schemes for legal
person with remote
identification
(substantial level)
done by Evrotrust

- eID schemes of Evrotrust (private company) has been retained by the Bulgaria government
- Two levels: substantial and high
- Depending on:
 - LoA of the identification means
 - Data set check during enrolment process
- Document authenticity check:
 - "True to the original" certification and a handwritten signature
 - Notary certification of the documents
 - Signing of the attached electronic formats of the documents with a valid certificate for qualified electronic signature / seal
 - Review and confirmation by using a specialized mobile or other application and after proper identification of the representative and / or legal entity by an employee of Evrotrust
- Legal existence of the entity:
 - Automatic based on authoritative source (UIC, BULSTAT)
 - Or by submitting proof:
 - Judgment or another document certifying the legal person set up
 - Document certifying their good standing
 - Unique national identifier





German initiative: Idunion solution (decentralized network based on authoritative identity source)

- Based on standards :
 - W3C for verifiable credentials
 - DID for registering object and unique identifier into a blockchain
 - DIDComm protocol to communicate data between agents

Human Trust

Technical Trust

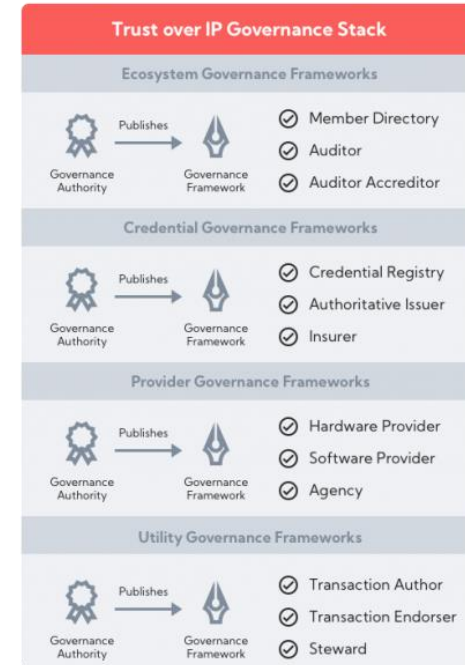
Layer 4

Layer 3

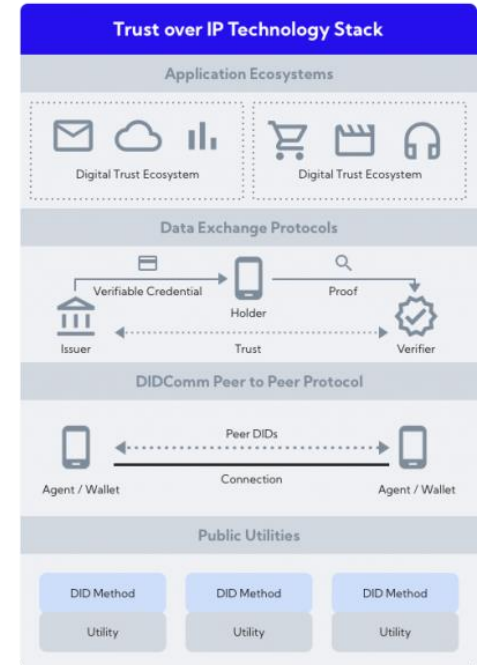
Layer 2

Layer 1

Governance

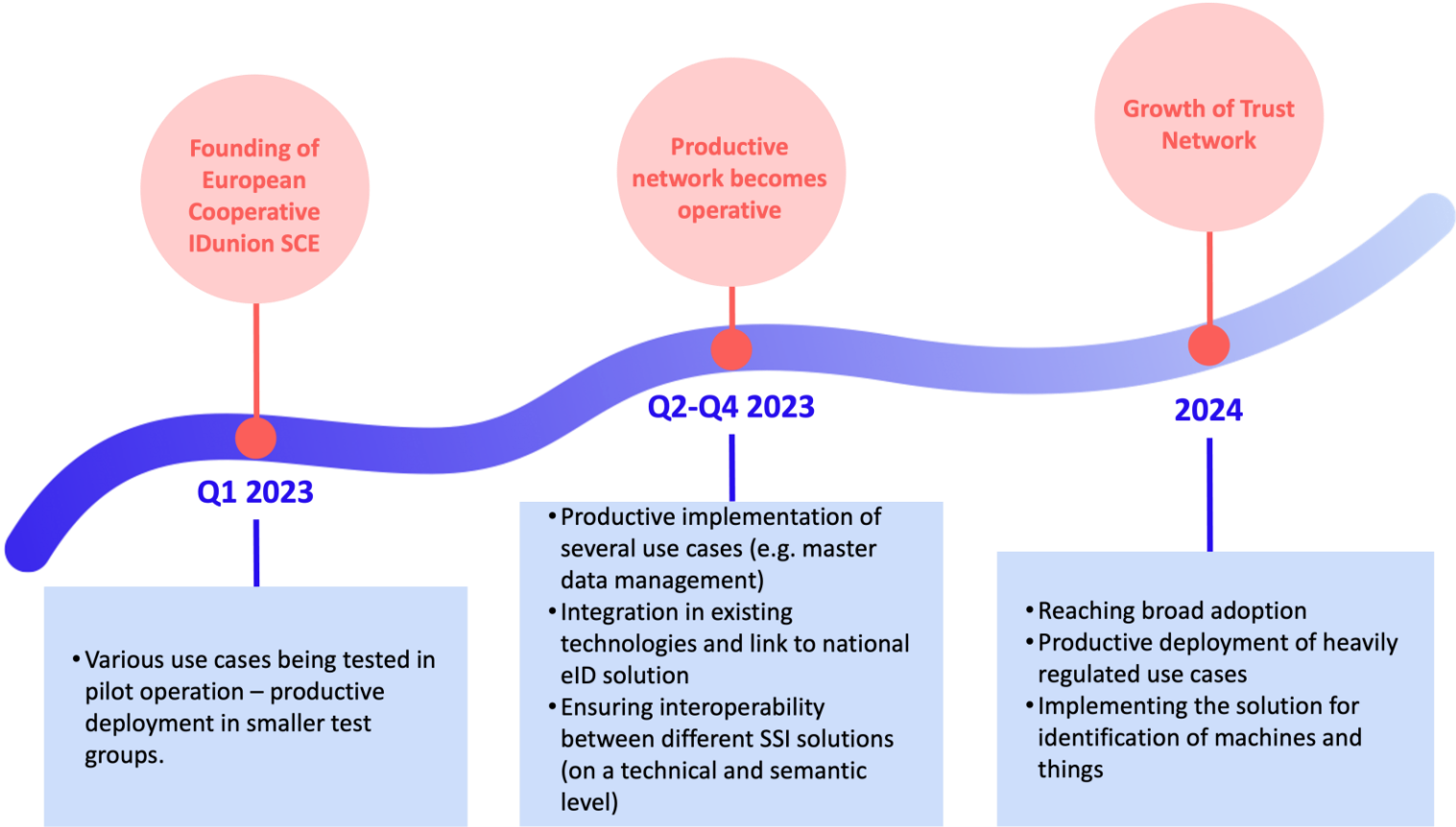



Technology





Idunion roadmap





Austria initiative: seal certificates based with identification of natural person based on Austria ID solution

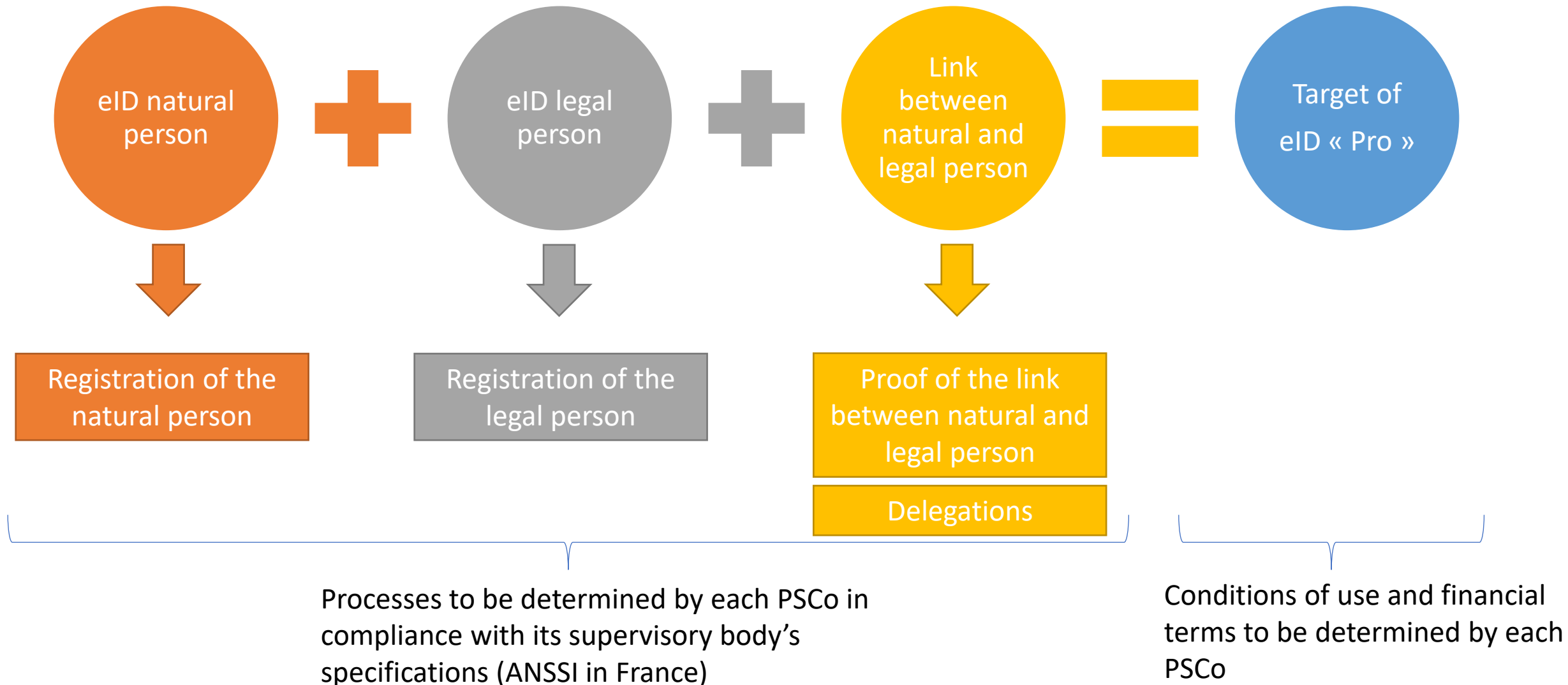
- Notified schemes
 - Qualified ID means based on smartphone application
 - ID Austria is available for natural and legal person
 - During authentication step, user can select to act on behalf of a legal person
 - Check are based on authoritative register (using a sector-specific identifier (ssPIN))
 - First time mobile application verification is done onsite
 - Activation of the link between natural and legal person through two method:
 - On-site Registration with IDA App
 - SMS-TAN-based Registration
-



French initiative on eIDs for legal entities : eID “Pro” working group from ClubPSCO

- A working group including service providers and ANSSI
 - Objectives :
 - Ensure the interoperability of the eID services for legal entity on the market to at least the substantial level, on the technical side (pivot format for the legal entity's data)
 - Define a coding system for the pivot format of legal entity data
 - define "tags" to manage roles and delegations
 - 2 use cases identified at this stage :
 - Authorization to sign for public contracts
 - Authorization for legal entities to receive QeRDS
-

Outside the scope of the eID "Pro" working group



Codification: what is the pivot format for legal entity data?

- The working group decided to use the OpenID Connect protocol as the basis for its work.
- The OpenID Connect protocol specification defines the standard fields that can be manipulated :

Fields
(...)
Name
given_name
family_name
birthdate
gender
(...)



Observation: there are no standard fields for identifying the data of a legal entity

Codification: what is the pivot format for legal entity data?

- The OpenID Connect protocol specification allows additional claims to be added, with appropriate naming to avoid collisions, in line with the JSON Web Token (JWT) specification.

What attributes are needed to identify a legal entity?

What fields should be applied to these attributes?

What data structure should be used for each attribute?

Codification: the working group's poposal

- This coding only shows the "minimum" data required to guarantee interoperability. Operators are free to add additional information as required.

Attribute	Field OIDC	Type	Mandatory	Description
Legal entity name	organization_name	String	YES	Official full name of the legal entity
Legal entity's unique registration identifier	organization_identifier	String	YES	Legal entity's registration reference based on CABForum structuring rules Example: NTRFR-123456789
Name of the agency (optionnal)	organizational_unit_name	String	NO	Full name of an agency of the organisation identified in "organisationName".
Agency's unique registration identifier (optionnal)	organization_unit_dentifier	String	NO	Facility registration reference based on CABForum structuring rules Example: NTRFR-12345678900023
Security level compliance	Security_level	String	NO	LOA eIDAS level achieved: substantial / high

SIREN or SIRET (in France)



- Optionally, the **ROLES / MANDATES** and **DELEGATIONS** of the Natural Person within the Legal Entity may be codified (**without mandatory dependency** between the ROLES and DELEGATIONS).
- For ROLES, coding is optional and is based on two (2) fields:

Fields	Content	
Role type	Legal Representative / Regulated Profession / Other	
Role name	Legal Representative	Chairman, Chief Executive Officer, Manager, ...
	Regulated Profession	Lawyer, Chartered accountant, Notary, ...
	Other	Operational title (e.g. Assistant, Production Manager, Porter, etc.)

- If these fields are used, the eID provider must communicate the naming system in its Service Policy to facilitate acceptance.
- A sector-specific naming system can be established between players, with values structured in the form xxxyyyValue, like the CABForum codifications.

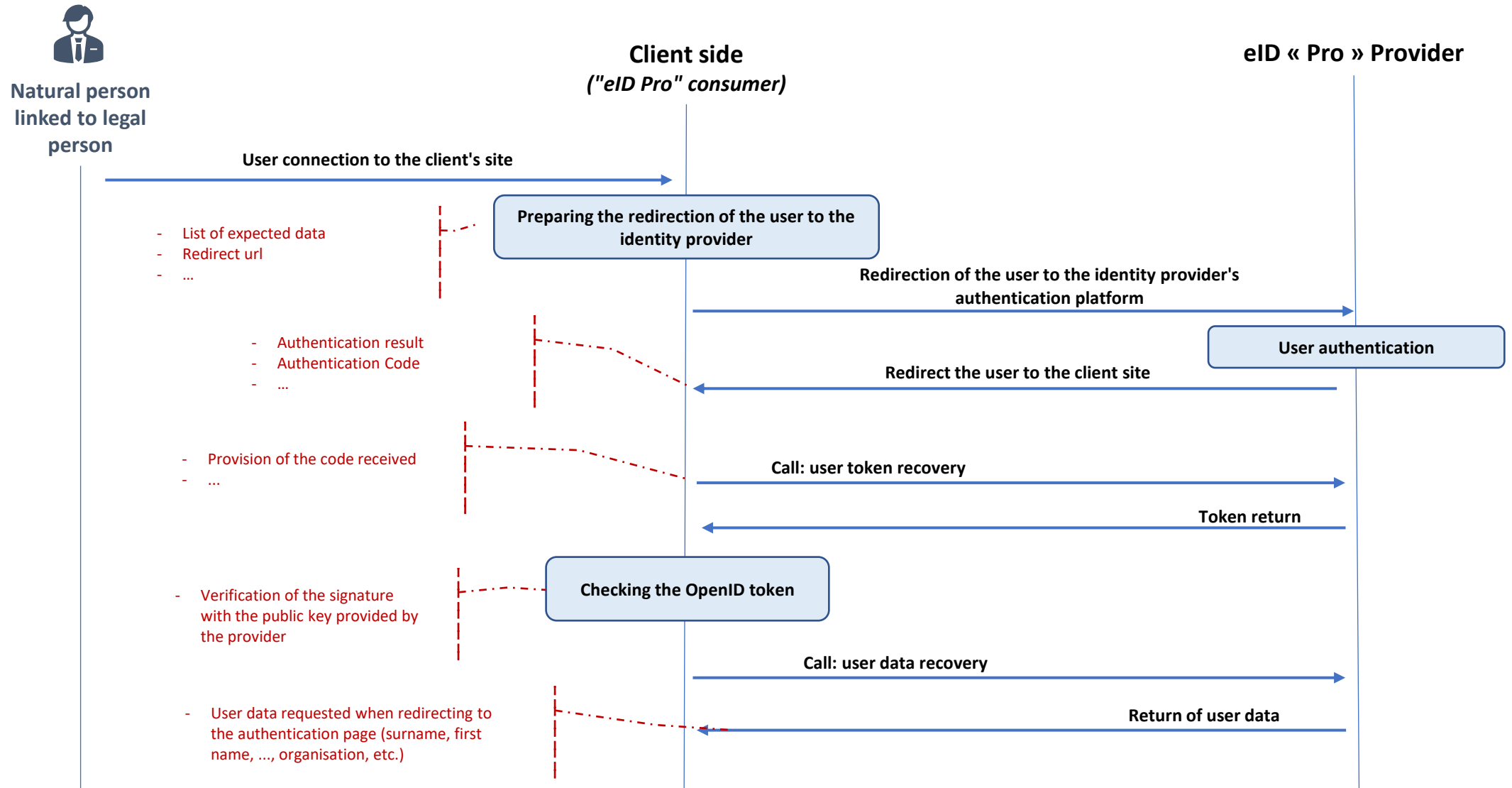
- For DELEGATIONS, coding is optional and is based on eight (8) fields:

Fields	Mandatory	Content
delegation_sector	YES	Delegation reference area
delegation_nature	YES	Type of delegation in the area concerned
delegation_termination_date	NO	End date of delegation
delegation_limitation_amount	NO	Limitation in financial value of commitment per act (coded as: id-etsi-qcs-QcLimitValue for a qualified certificate)
delegation_limitation_domain	NO	Limitation by area of commitment (definition by area)
delegation_sub-delegation	NO	Authorised sub-delegation, single-level, multi-level
delegation_validation_level	YES	Delegation validation level: Declarative – Certified
delegate_entite_identifier	NO	Legal entity's registration identifier (SIRET/SIREN in France) of the natural person receiving the delegation

- If these fields are used, the eID provider must communicate the naming system in its Service Policy to facilitate acceptance.

ClubPSCo OpenID Connect sequence

Le club des Prestataires de Services de Confiance



Synthesis

A growing market ...



Although the regulations and standards have not yet been finalized, market players are already organizing themselves to offer solutions for managing the eIDs of legal entities.



There are lots of initiatives in Europe, but the same technologies are often used:

Legal data through LEI standard

Used of verifiable credentials

Registering data on blockchains through DiD objects

... but with a few limits

- Identification processes are disparate
 - Need to strengthen processes to guarantee the identity of individuals and legal entities
 - Use audited processes, through qualified services (generally less user friendly)
 - No real sources of authority to establish the link between the natural person and the legal entity (except for a few sources that may be authoritative in some Member States)
- Centralized versus decentralized architecture: a boundary between control of practices and global consensus
- Recording data in blockchains whose future is not necessarily sustainable

Security at each step

	basic	Substantial/high
Identification/enrolment	Online	Face to face
Authentication method	Login / mdp	Strong authentication
Link between natural and legal person	Database of the provider	Authoritative source
Control of processes	No external check	Qualified TSP



Need to define a common set of standards and techniques in Europe

Define the LoA expected for the identity of a natural person

Define the information data structure for legal entities

Define the technical architectures for exchanging data between Member States (and also outside Member States)



Need to define qualification processes for players in this new market

Authoritative sources for each Member States, and centralization at Europe Commission level

Recording and securing information, non-repudiation of legal entity data

Trusted Data providers