Use Case & Legal impact
aka Towards ESSIF v2 / EBSI v2

Legal Questions
(New) Use Case Requirements
Finetuning the Datamodel

Improving the design of ESSIF v2
(and maybe food for thought/input/candidatures/….)

Forecast
ESSIF in the world of eIDASv2

Limitations of ESSIF v1 / EBSI v1

Due to time/resource limitations ESSIF v1 / EBSI v1 does not fully reflect the architectural / technical specifications listed here.

The specifications should be read as “target” and ESSIF v1 / EBSI v1 should be understood s a non-production “demonstrator”

In reality these specifications will be fine-tuned in light of ESSIF v2 / EBSI v2 and taking into account the lessons learned from v1 + input from the use cases + legal considerations.

- Use Case & Legal impact
  - Legal Questions popping-up
  - (New) Use Case Requirements
  - Finetuning the Datamodel

- ESSIF v1 -> ESSIF v2
  - Key Components
  - Key Flows
  - Supporting Services
  - Security Concerns
  - Trust Framework

- Forecast (Long Term)
  - eSeals / eSigs / Timestamps under eIDASv2?
  - Trusted Issuers under eIDASv2

European Commission

- Clear & Complete vision
- To be somewhat fine-tuned
- Bigger Effort expected
- Challenges expected

Legal Questions (work in progress)

Data / Information Modeling

- What about private <> gov-used DIDs?
- Relationship DID <> different types of DID-keys
- Inheritance of attributes > obligations of issuers?
- Legal foundation for Verifiable IDs <> Verifiable Attestations
- Relationship key for Authentication <> keys for eSealing?

Legal Limitation wrt Flows?

- Clear directions on when (not) to anchor citizen DIDs
- Legal value of Verifiable ID publication of (Trusted) Issuers
- Clear legal statement on inheritance of eIDAS attribs towards Verifable IDs + LoA-model
- Rules for issuance and resulting LoA of attestations
- When should a presentation be signed by a submittor (in definition of eDAS-esignatures)?
- Legal aspects wrt Identification / Authentication (and DID-key strength)

Legal question wrt Core Components

- like in banking sector >> some minimum obligations for holders?
- MIMIMUM requirements for environments of Issuers issuing high LoA VCs.
- Guidance for relying parties on how (not) to process received VCs

Legal question wrt Supporting Components

- Legal guidelines for registrars as to keep the Trusted Issuer Ledger clean (especially in case of high LoA)
- As some DIDs are sensitive / important to fully trusted >> need for specific registrar for eg gov issuers?
- As resolvers can “translate” DID-documents for parties >> need to have rules in this space?
- Guidelines for parties that offer compliant PDSs / Wallets

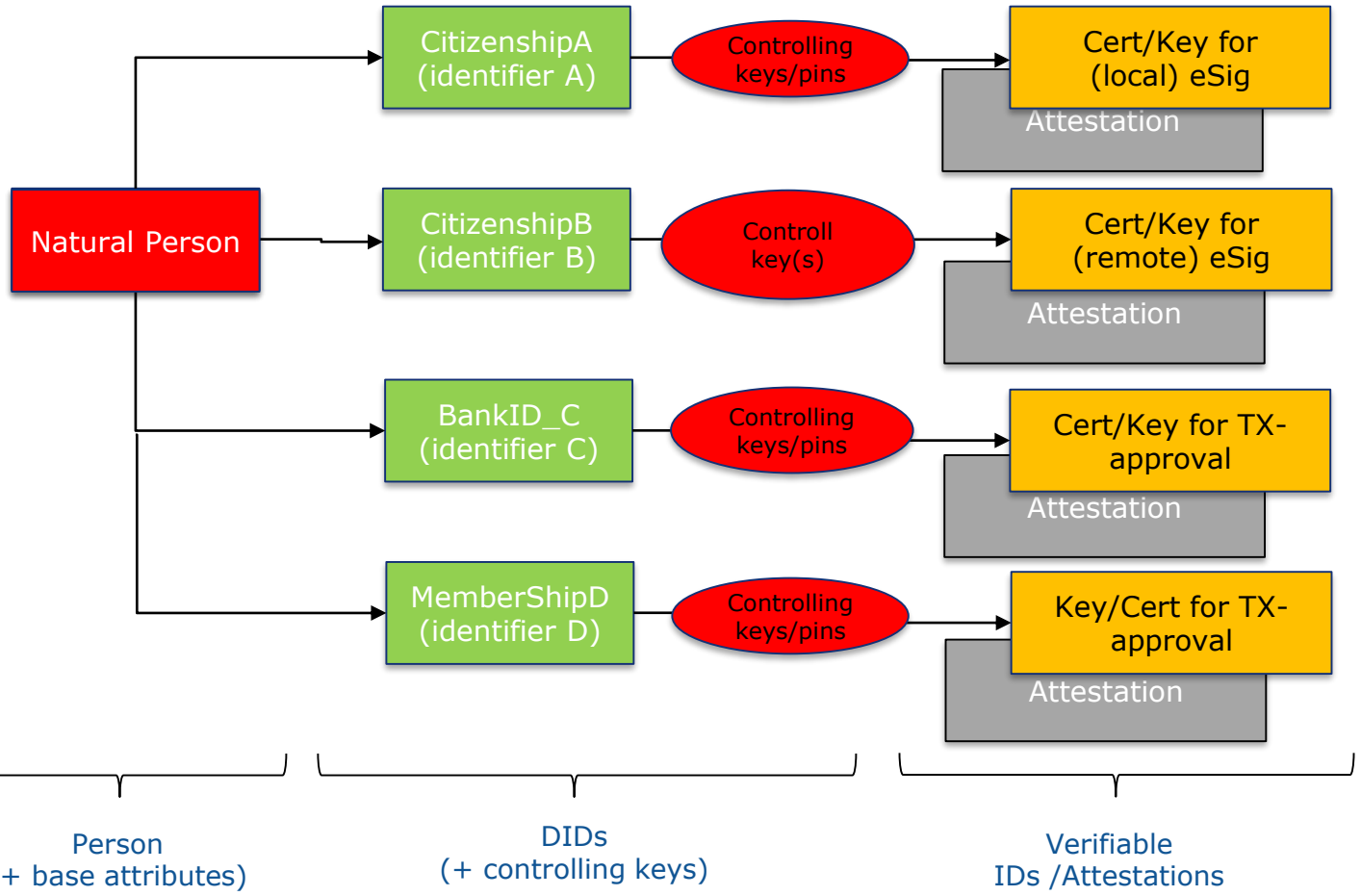
Upcoming requirements (work in progress)

Topic	Attention Points > v2
Support for eIdentification (in alignment with eIDAS v1)	• Compliance for level substantial in line with eIDAS v1 • Compliance for level high/qualified in line with eIDAS v1 • Support for revocation-lists
Diploma Use Case	• Datamodel mapping with Europass (incl DID mapping) • Ledger for authorized / trusted issuers • Inheritance of attributes to be clarified • LoA of Qualifications TBD
Noterization Use Case	• Identification / Authentication of Legal entities • Support for applications action on behalf of • Support for verifiable consents
EU Health Card	• AuthN based on eID and on V.ID • Issuance at level "substantial"
Digital Driving License	• AuthN based on eID and on V.ID • Issuance at level "substantial"
Asylum	• Need for asylum "registrars" • Need for "fingerprint' on ledger • Asylum card LoA "substantial"
Registration for Subsidy	• Support for all v2 flows • Insert ability to negotiate accepted VCs
…..	• ….

DID-Controller key(s)
=?
DID-Authentication-keys

European Commission

Identities <> DIDs <> Verifiable IDs
(a non-technical perspective)



- Use Case & Legal impact
  - Legal Questions popping-up
  - (New) Use Case Requirements
  - Finetuning the Datamodel
- ESSIF v1 -> ESSIF v2
  - Key Components
  - Key Flows
  - Supporting Services
  - Security Concerns
  - Trust Framework
- Forecast (Long Term)
  - eSeals / eSigs / Timestamps under eIDASv2?
  - Trusted Issuers under eIDASv2

European Commission

- Clear & Complete vision
- To be somewhat fine-tuned
- Bigger Effort expected
- Challenges expected

Architecture v1/v2 – Core Components

Topic	To Do > v2
Detailed Datamodel	Formal V.ID model incl trust-vectors Formal / full alignment with Europass Aligned with legal recommendation
User/Holder - Wallet – UI	Secure WebUI + MobileApp with secured connection with distributable App.
User/Holder - Wallet – Core	Distributable Secure Wallet/App. Policy Engine
User/Holder – Wallet – Secure Enclave	Implementation of v1 secure element
User/Holder – Wallet – Identity Hub	Implementation of v1 DIF-identity hub
Relying Party – Core	Production grade code True eIDAS-authN (OIDC) support True V.ID support (incl trust vectors) Policy Engine + Allowing “negotiation”
Relying Party – Secure Enclave	Implementation of v1 secure element
Relying Party – Data Store	Implementation of v1 DIF-identity hub
Issuer – Core	Production grade code Full Relying Party functionalities Configurable policies per issuable VC
Issuer – Secure Enclave	Support for multiple levels of trust Compliant with eIDAS remote esealing
Issuer – Data Store	Implementation of v1 DIF-identity hub

- Clear & Complete vision
- To be somewhat fine-tuned
- Bigger Effort expected
- Challenges expected

Architecture v1/v2 – Key Flows

Topic	To Do > v2
Holder registration	Support for multiple DIDs Possibility to put DIDs & V.IDs in ID Hub
Relying Party Registration	Multiple types of DIDs? Multiple type of V.IDs Ledgers per domain?
Issuer Registration	Multiple types of DIDs? Multiple type of V.IDs Ledgers per domain?
Linking of eSealing certificate	TBD based on legal study
Holder Authentication with eID	Code / Ref implementation to put next to or integrate in OIDC-setup supporting multiple LoAs
Holder Authentication with V.ID	Code / Ref implementation to integrate in OIDC-setup supporting multiple LoAs
Issuance of a V.ID	Policy based Support for multiple LoAs
Issuance of a V.Attestion	Policy based Support for multiple LoAs
Submission of (a) VC(s)	Support for expressing accepted VCs Support for submission outside AuthN-flow

- Clear & Complete vision
- To be somewhat fine-tuned
- Bigger Effort expected
- Challenges expected

Architecture v1/v2 – Supporting Services

Topic	To Do > v2
Generic Ledger setup	Support for multiple Ledgers
Generic SC model	Configurable SCs for <listed> tasks
DID registrar	Access control-based registration (depending on required LoA)
DID resolver	V1 resolver (incl "transformations") !esealing!
DID:ebsi-ledger	Configurable anchoring depending on the community Adherence to legal recommendations
Trusted Issuer Ledger	Selective Ledger for Trusted Issuers "per type" Registration of Enriched information (V.ID + allowed attestations)
Anchoring ledger for party VC	Anchoring of publicly relevant VCs
VC exchange noterization	Selective anchoring depending on type of event.
Signature Validation Service	eIDAS compliant signature validation
Certificate Validation Service	OCSP validation for QTSPs

European Commission

- Clear & Complete vision
- To be somewhat fine-tuned
- Bigger Effort expected
- Challenges expected

Architecture v1/v2 – Increasing Security Posture

Topic	To Do > v2
User/Holder-Wallet	Secure-by-design / Hardening Correct secret-mngt True secure enclave "Privacy compliant" ID Hub
Relying Party Environment	Secure-by-design / Hardening Correct secret-mngt True secure enclave "Privacy compliant" ID Hub
Issuer Environment	Secure-by-design / Hardening Correct secret-mngt True secure enclave "Privacy compliant" ID Hub eIDAS compliant eSealing
Registration	Selective (permissioning where needed)
Resolving	Enriched resolving (where needed)?
Authentication	Support for different LoA's
Issuance	Subject to rules engine Support for multiple LoA's
Node operator obligations	Secured setup / well-defined API-AuthN-patterns / ABAC-base access controls Well defined TOM (incl Security / Risk Mngt Obligations)
Ledger obligations	Support for multiple domains Support for different Trust levels Governance model in place

Required Foundation > Trust Framework

ESSIF Trust Framework

ESSIF Policies for ESSIF-TSPs (Issuers)

Policies for ESSIF-TSPs (Ledgers)

ESSIF Guidelines for Owners/ Subjects

ESSIF General Usage Conditions (for Relying Parties)

ESSIF Technical Standards

ESSIF Guidelines for Wallet Providers

Related Regulations & Practices

Required > Operational RuleBook

- Use Case & Legal impact
  - Legal Questions popping-up
  - (New) Use Case Requirements
  - Finetuning the Datamodel
- ESSIF v1 -> ESSIF v2
  - Key Components
  - Key Flows
  - Supporting Services
  - Security Concerns
  - Trust Framework
- Forecast (Long Term)
  - eSeals / eSigs / Timestamps under eIDASv2?
  - Trusted Issuers under eIDASv2

In case of "cross-border" the element of notified schemes come into play!

eIdentification under eIDASv2?

eIDAS v1	eIDAS v2
'electronic identification means' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;	DID-/Verifiable ID documents and DID-controlling/authentication-keys to be recognized as "electronic identification means"
'person identification data' means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;	Verifiable IDs (in combination with DID-AuthN-/controlling-key) can proof the identity of any entity
'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;	**Trusted Issuers** issuing Verifiable IDs (who are held to do the necessary registration/validation-activities including verification of the strength of the DID-keys)
'authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;	Combination of the presentation of the Verifiable ID and the proof of "control" over the DID key

Mind that the "overall LoA" depends on
the LoA of the DID-key
and of the LoA of the verifiable ID
and the Trust Level of the Trusted Issuer

Legal value / equivalance in case of eSeal/eSig?

European Commission

eSeals / eSigs / Timestamps under eIDASv2?

eIDAS v1	eIDAS v2
'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;	"Fingerprint" of the VC obtained through a "trusted notarizing party" + unique UUID = sufficient (much like remote signing via remote signing service)?
'electronic seal' means 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;	"Fingerprint" of the VC obtained through a "trusted notarizing party" + unique UUID = sufficient (much like remote signing via remote eSealing service)?
'electronic time stamp' means 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;	Establishing inside the "fingerprinted meta-data" the time at which a VC was "notarized" to the trusted ledger, sufficient?
'validation data' means data that is used to validate an electronic signature or an electronic seal;	All metadata that has been notarized for a VC on a trusted/recognized ledger

Trusted Issuers under eIDASv2

eIDAS v1	eIDAS v2
'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;	<u>Already possible now?</u> (Q)TSP for Qualified Timestamping (on ledger) <u>New (Q)TSP services:</u> • (Q)TSP for DID-registration / DID-custodian? • (Q)TSP for Issuance of Verifiable IDs • (Q)TSP for Issuance of Verifiable Attestations • (Q)TSP for notarization • (Q)TSP for archiving
Trusted List for QTSPs	Trusted List for all new (Q)TSP services (also for substantial ?)