European Commission

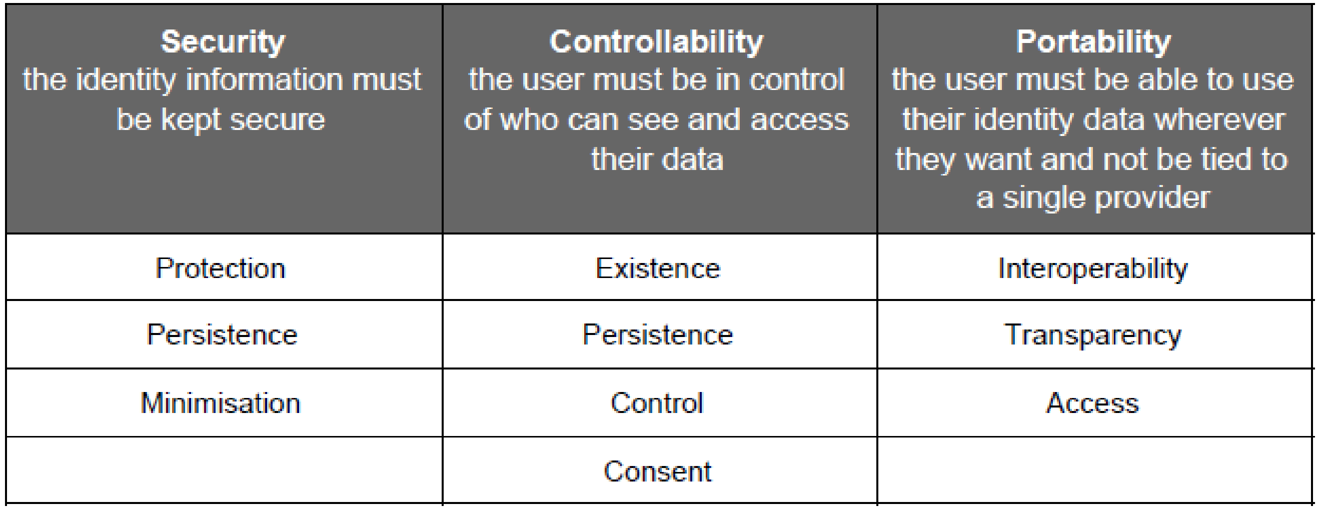
EBSI eSSIF Legal assessment wrt eIDAS and GDPR

2nd EBSI eSSIF Stakeholders meeting

Legal assessment is Work In Progress!

- The objective is to evaluate the potential legal issues that are horizontal to an SSI solution, including:
  - DIDs: What is the legal nature and ownership of DIDs (asset vs a special kind of pseudonym), how should be DIDs managed in case of minors and incapable persons, if DID may be subject to seizure, when DIDs may be deactivated, what is the legal regime of keys and wallets, etc.
  - VCs: What are the duties and responsibilities of VCs issuers, holders and verifiers. How to model the contractual/non-contractual relations between issuers & verifiers, and set up liability models. We should pay special attention to the legal aspects of the VC lifecycle (issuance, suspension and revocation causes, etc).
  - Alignment of the SSI solution with the eIDAS Regulation: aligning VCs with eIDAS eID rules, but also linking VCs to eSeals or eSignatures.
  - Trust framework: legal input regarding LoAs, governance aspects, conformity, etc.
- We expect to produce proposals to be used as policy input for the eIDAS 2020 review process.

Self-sovereign identities (SSI)

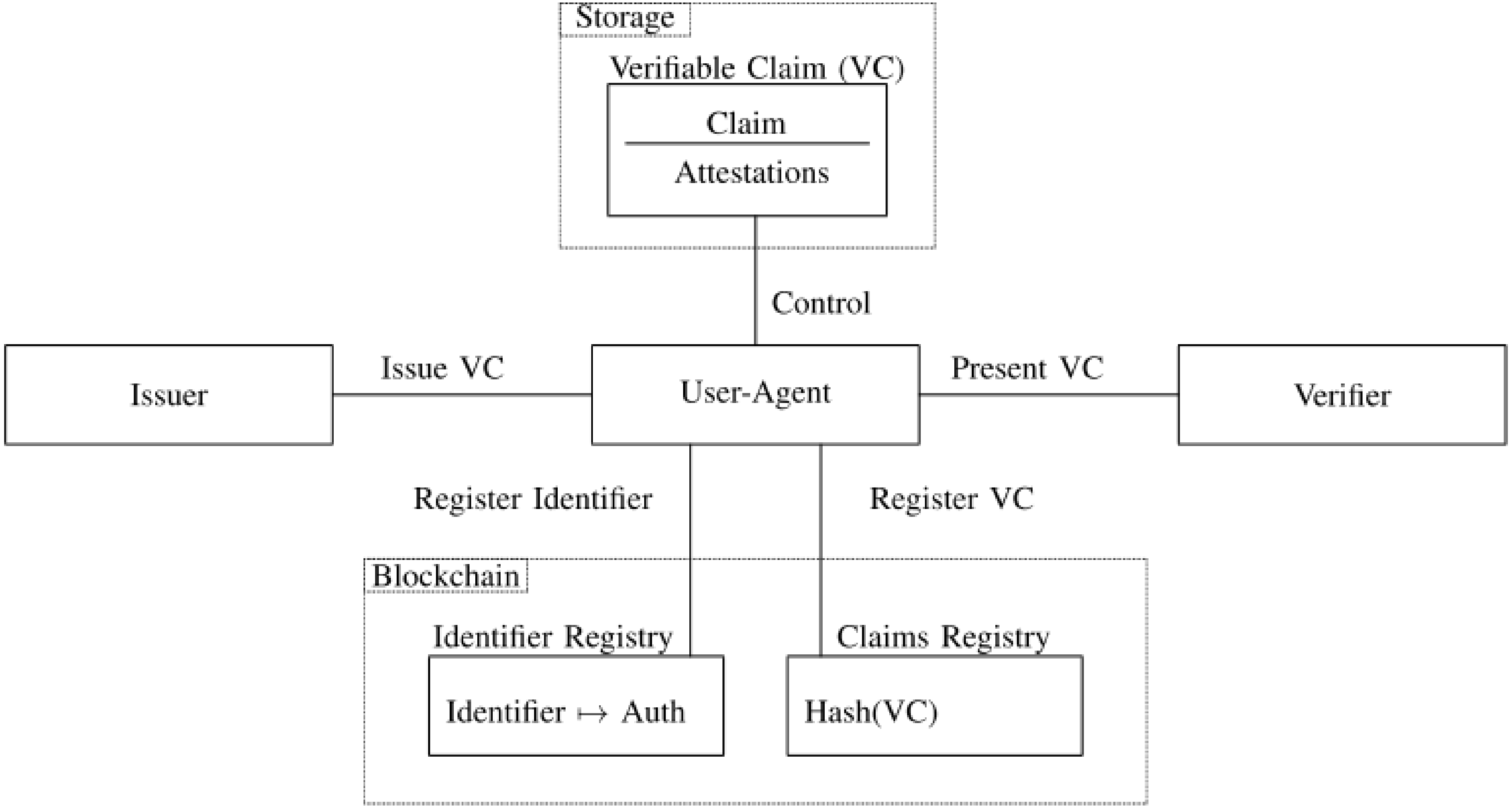


Security the identity information must be kept secure	**Controllability** the user must be in control of who can see and access their data	**Portability** the user must be able to use their identity data wherever they want and not be tied to a single provider
Protection	Existence	Interoperability
Persistence	Persistence	Transparency
Minimisation	Control	Access
	Consent	

C. Allen / The Path to Self-Sovereign Identity (2016)

"Self-sovereign identity is the next step beyond user-centric identity and that means it begins at the same place: **the user must be central to the administration of identity**. That requires not just the interoperability of a user's identity across multiple locations, with the user's consent, but also **true user control of that digital identity**, creating user autonomy. To accomplish this, **a self-sovereign identity must be transportable**; it can't be locked down to one site or locale".

An SSI Architecture (illustrative)

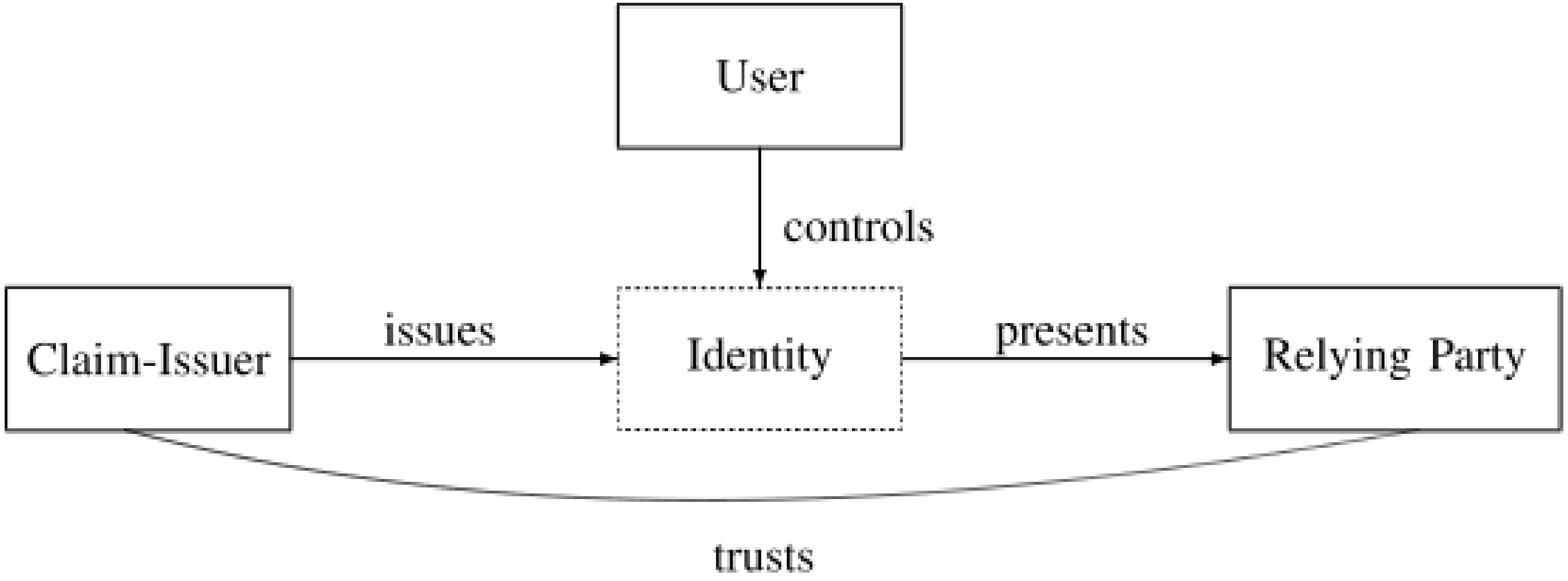


A. Mühle et al. / Computer Science Review 30 (2018) 80–86

SSI benefits

- Compared to previous identity management systems (centralized, based in PKI, federated and user-centric), SSI introduces key benefits.
- As identity information, and specially credentials, are not stored by a central Identity Provider, SSI **reduces the risk of massive identity theft**.
- The SSI "Identity Provider" (the claim/credential issuer) does not intervene in the authentication process, and therefore has not information about the online user activity, **reducing** the "big brother" risk and **GDPR compliance costs**.
- SSI allows the user to decide **which identity data to share**, with whom, and with which limits and constraints for third parties, even using zero knowledge proofs.
- Even if SSI allows revocation of credentials, the base identity (the Decentralized ID or DID) can not be suspended nor revoked except by the user, **ending with "digital feudalism" business models**, aligning identity management with GDPR principles.

SSI trust relations do not essentially change...



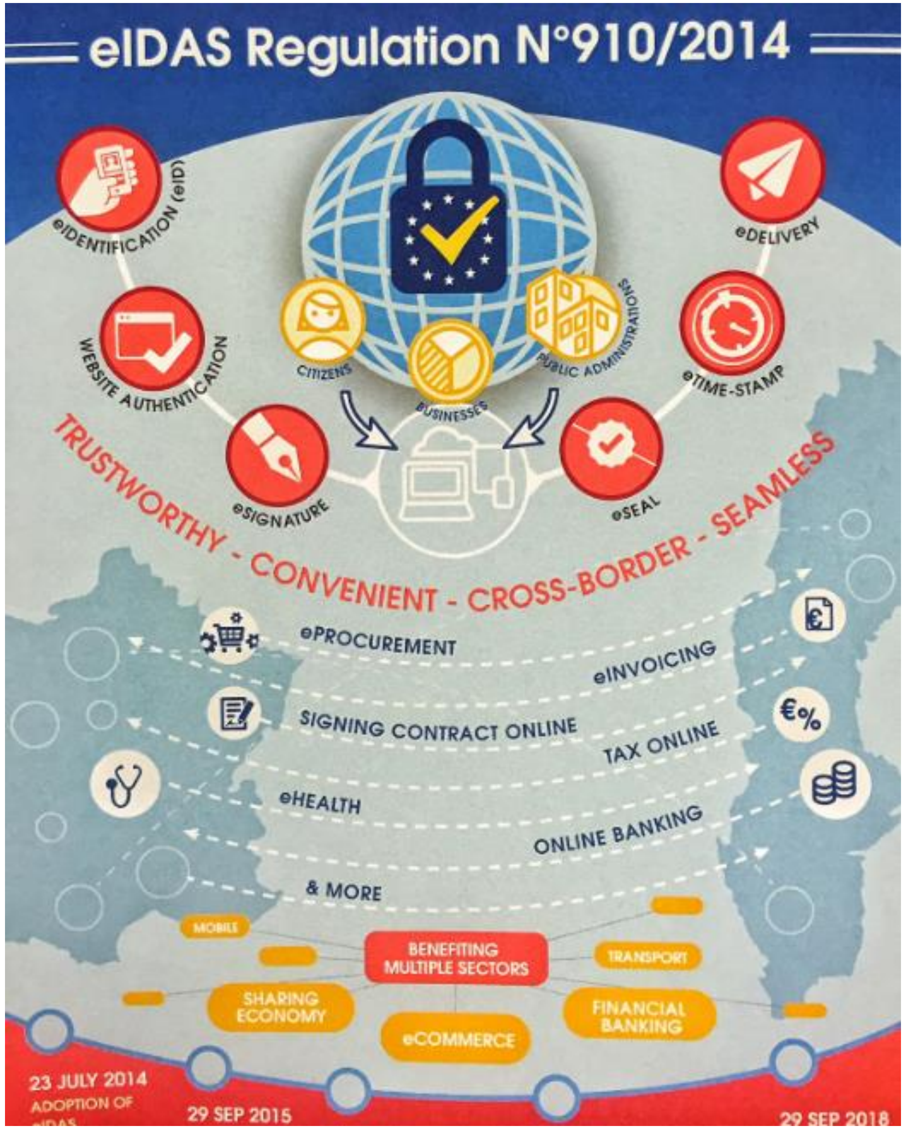
A. Mühle et al. / Computer Science Review 30 (2018) 80–86

A big SSI challenge! The need for trust anchors

- We still need to identity the “real identity” of a DID subject, in a trustworthy manner, both to issue credentials and to consume them.
- We need to define governance frameworks for the **usage of SSI in legally binding transactions**, where social trust frameworks may not be acceptable in terms of liability or regulatory compliance (e.g. in KYC/AML environments).
  - Verifiable credentials level.
  - DID level.
  - Key management level.
  - DLT (Blockchain) level.

- **Trust anchors**, well defined in identity trust frameworks, may be really helpful. Especially when based in a well defined and tech-neutral Law…

eIDAS: the Digital Single Market trust foundation



“Electronic identification (eID) and electronic Trust Services (eTS) are **key enablers** for secure cross-border electronic transactions and central building blocks of the Digital Single Market […] a **milestone** to provide a predictable regulatory environment to **enable secure and seamless** electronic interactions between businesses, citizens and public authorities” (EU Commission, 2015).

eIDAS: the Digital Single Market trust foundation

- "By providing the building blocks for ensuring trust, convenience, and security in the online environment, the eIDAS regulation represents a **major contribution to the European Digital Single Market** […] opens the door for end-to-end electronic transactions and processes that **replace the traditional activities and manual processes**, while keeping the **same legal value** […] opportunities for organizations implementing eIDAS trust services are **evident**: increase the efficiency of the business processes, reduce their operational costs, grow their business, and build a competitive advantage" (Deloitte, 2016).
- "The GDPR and eIDAS are seen as providing the **right foundation** for a true DSM […] eIDAS is often presented as an excellent initiative with **impact beyond European borders** […] an example of an **EU success**. Its regulation and specifications have managed to set a **common framework in a fragmented market** for using digital services across Europe" […] digital identity and e-services are **crucial for EU nationals**, and can also help with European challenges such as the current migration crisis" (PwC, 2018).

eIDAS – The Regulation in a nutshell

2 MAIN CHAPTERS SUBJECT TO DIFFERENT RULES AND REQUIREMENTS

Chapter II

Mutual recognition of e-identification means

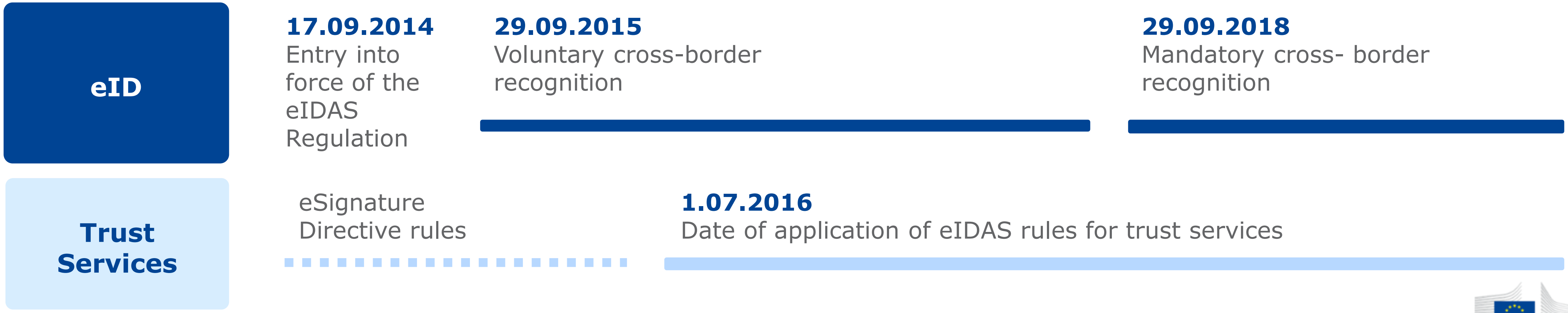
Chapter III

Electronic trust services

+

Chapter IV

Electronic Documents



eID

17.09.2014
Entry into force of the eIDAS Regulation

29.09.2015
Voluntary cross-border recognition

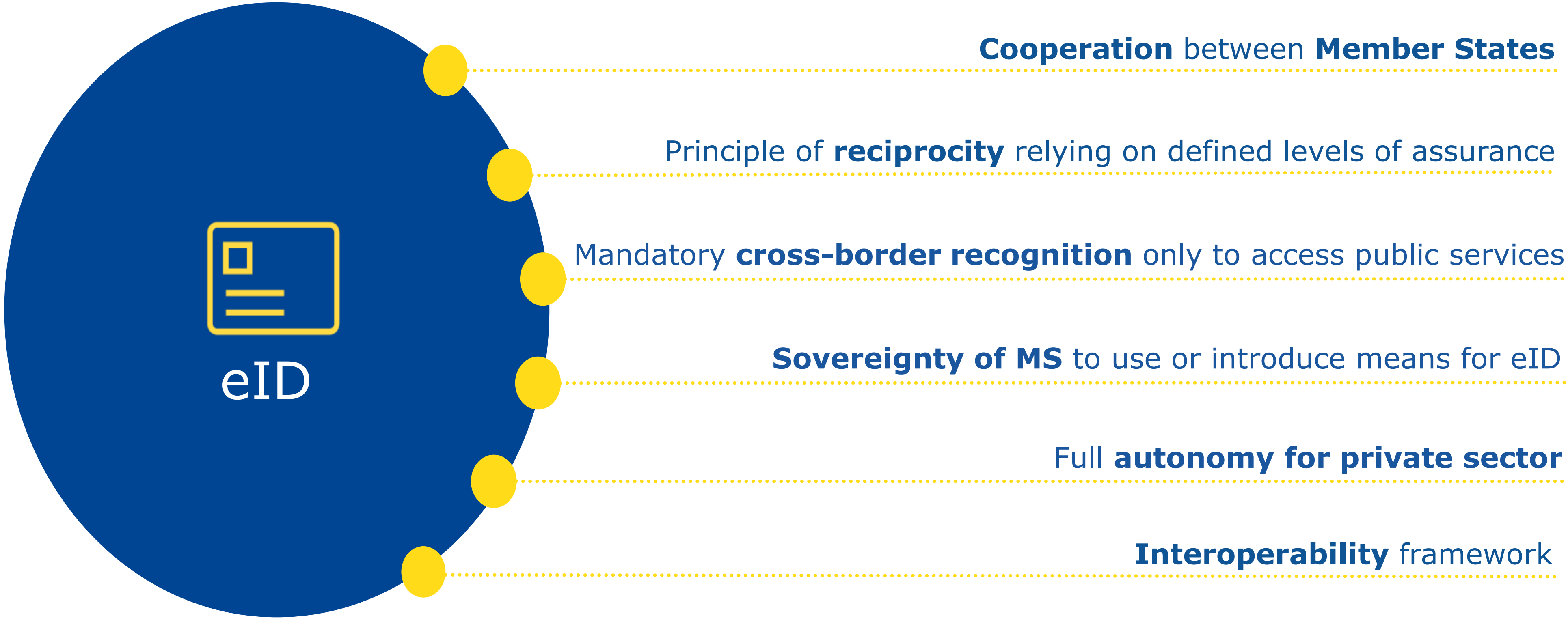
29.09.2018
Mandatory cross- border recognition

Trust Services

eSignature Directive rules

1.07.2016
Date of application of eIDAS rules for trust services

eIDAS: Key principles for eID



Cooperation between **Member States**

Principle of **reciprocity** relying on defined levels of assurance

Mandatory **cross-border recognition** only to access public services

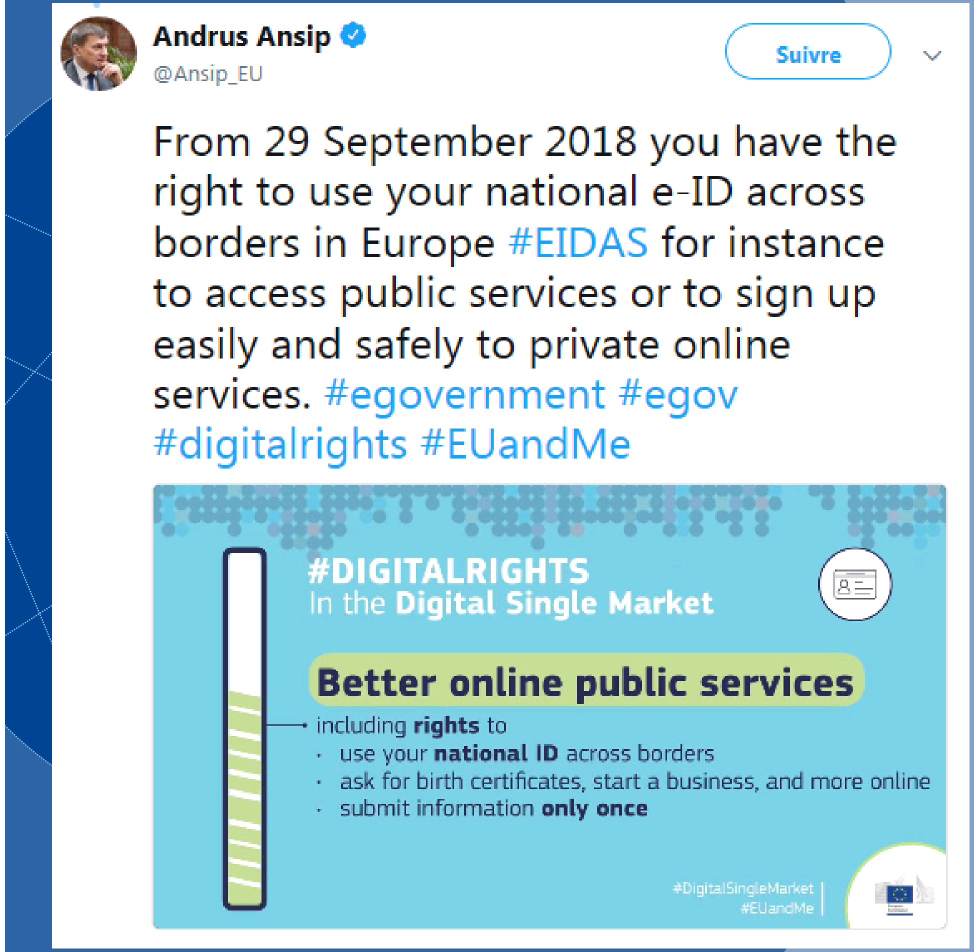
Sovereignty of MS to use or introduce means for eID

Full **autonomy for private sector**

Interoperability framework

***The Regulation does not impose the use of eID**

eID schemes notified



From 29 September 2018 you have the right to use your national e-ID across borders in Europe #EIDAS for instance to access public services or to sign up easily and safely to private online services. #egovernment #egov #digitalrights #EUandMe

#DIGITALRIGHTS
In the Digital Single Market

Better online public services

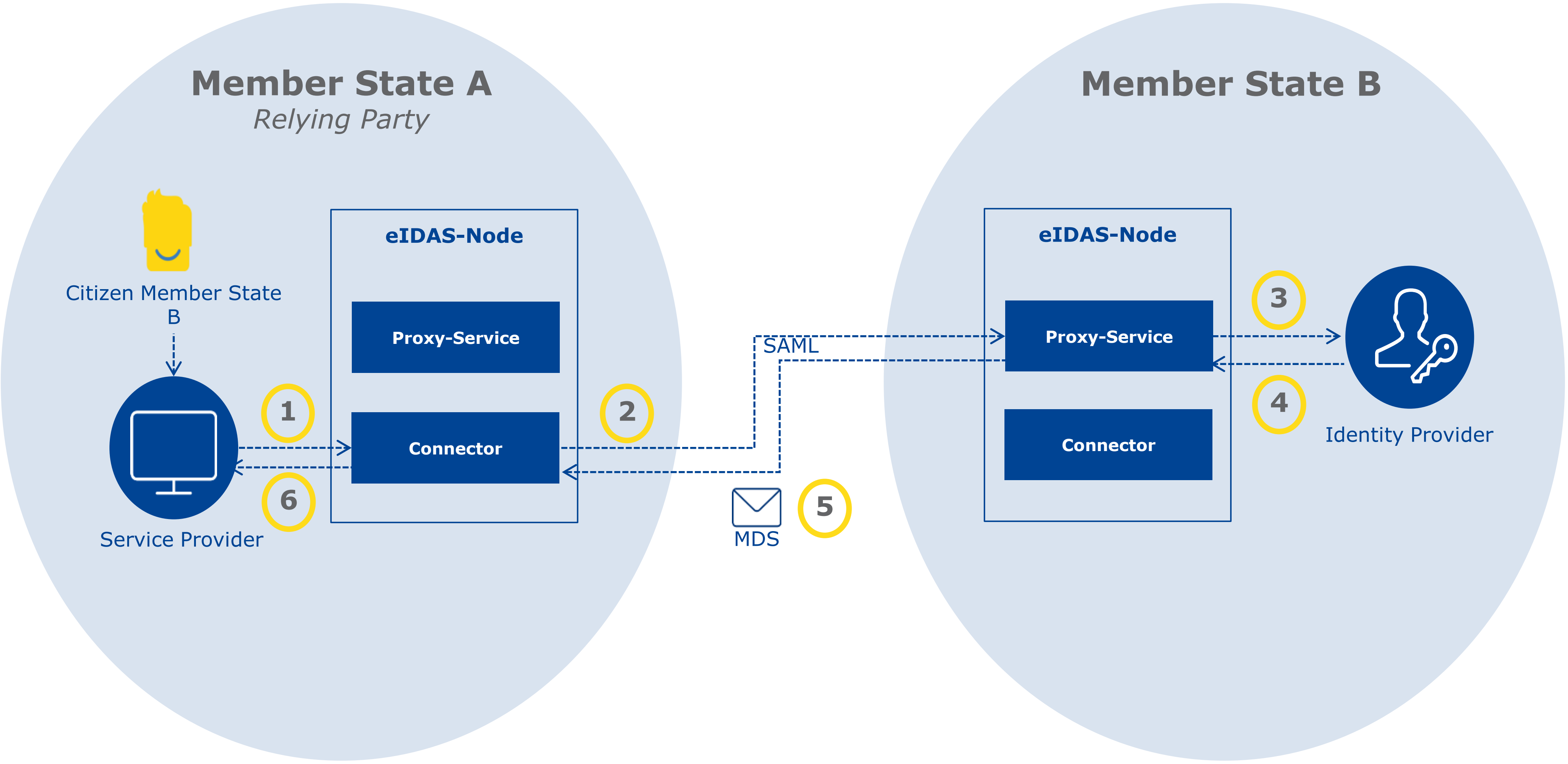
including **rights** to

- use your **national ID** across borders
- ask for birth certificates, start a business, and more online
- submit information **only once**

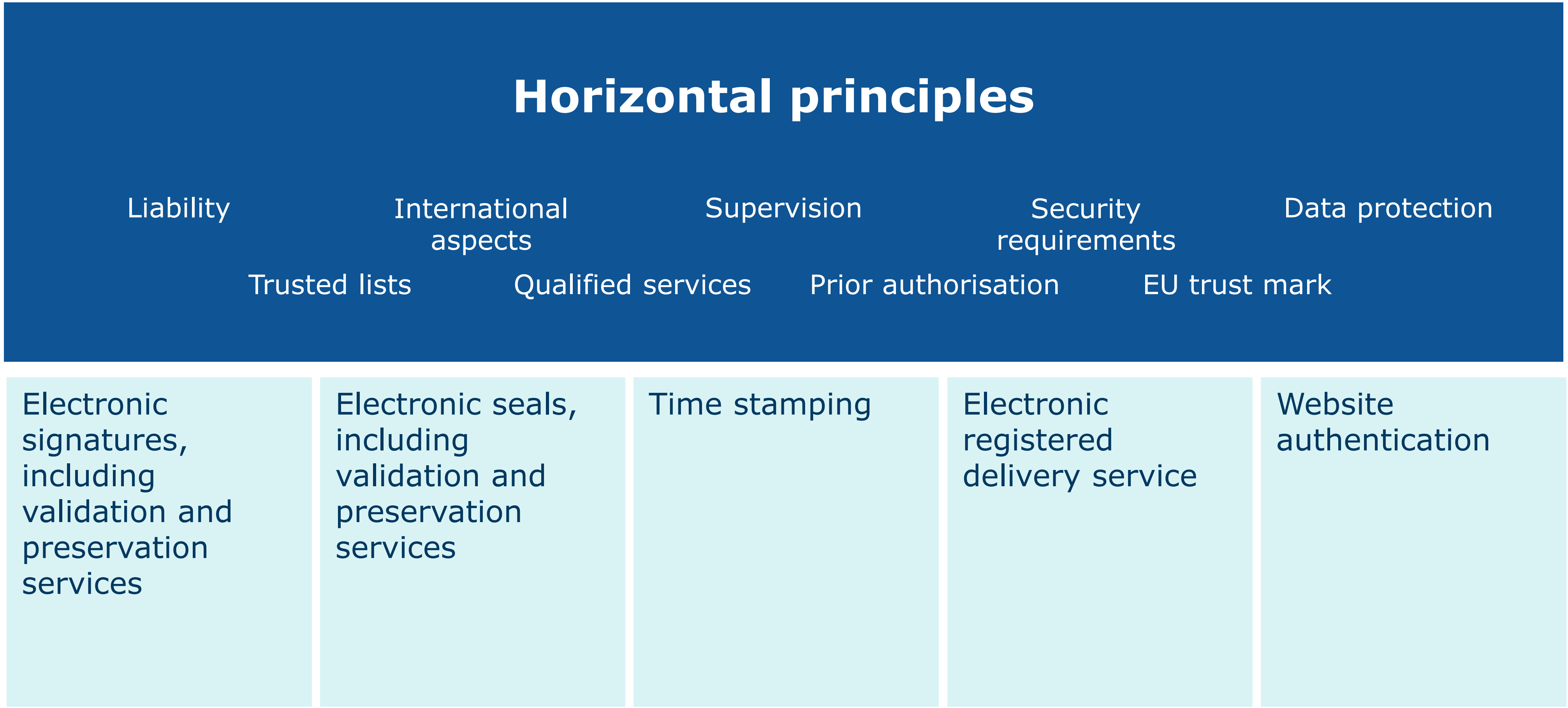
#DigitalSingleMarket
#EUandMe

Notified eID schemes:
Belgium (eID, Itsme), **Portugal** (Cartão de Cidadão), **Czech Republic** (CZ eID card), **Germany** (National Identity Card, Electronic Residence Permit), **Estonia** (ID card, RP card, Digi-ID, e-Residency Digi-ID, Mobiil-ID, diplomatic identity card), **The Netherlands** (eHerkenning), **Italy** (eID, SPID eID), **Latvia** (eID karte, eParaksts karte, eParaksts karte+, eParaksts), **Spain** (DNIe), **Slovakia** (Slovak Citizen eCard, Foreigner eCard), **Croatia** (Personal Identity Card (eOI)), **United Kingdom** (GOV.UK Verify), **Luxembourg** (eID card).

eIDAS (current) Interoperability Architecture



eIDAS – Trust services



Horizontal principles

Liability

International aspects

Supervision

Security requirements

Data protection

Trusted lists

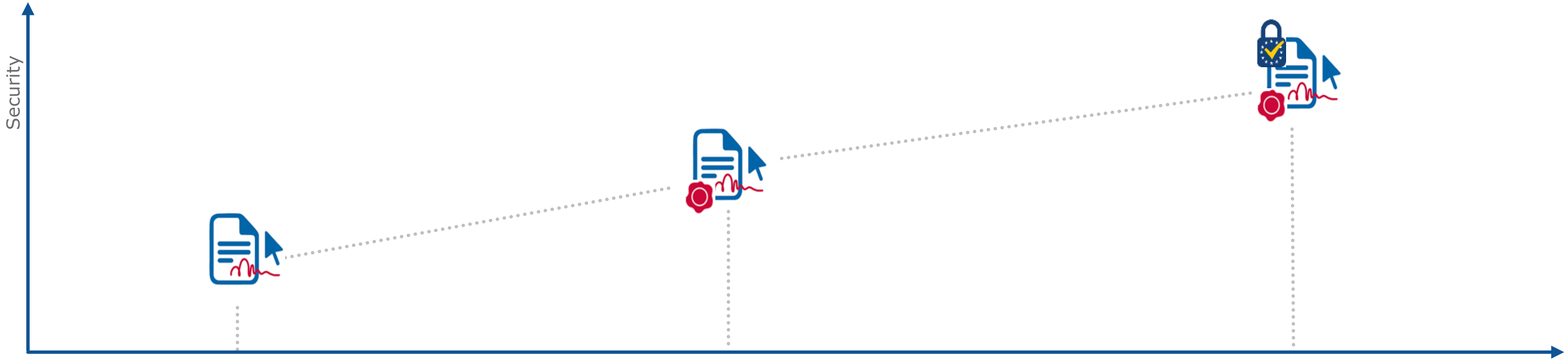
Qualified services

Prior authorisation

EU trust mark

Electronic signatures, including validation and preservation services	Electronic seals, including validation and preservation services	Time stamping	Electronic registered delivery service	Website authentication

Types of e-signatures and e-seals



Simple (SES)

- Demonstrates the intent of the signer
- Associated with the document or data the signer intends to sign or seal.

Advanced (AES)

Simple electronic signature, which also:

- Identifies, is uniquely linked and under the sole control of the signer/sealers
- Detects subsequent changes to the document
- For mutual recognition by public services, must be in ETSI formats (ASiC, PAdES, CAdES, XAdES)

Qualified (QES)

Advanced electronic signature, which also:

- Is based on a qualified certificate
- Is created using a qualified signature creation device

Equivalent to handwritten signature.

Additional supporting evidence required

No additional supporting evidence required

Cannot be denied legal effect just because it's electronic.

Role of eIDAS Regulation in the SSI space

- eIDAS Regulation constitutes the main **electronic identification trust framework** in the European Economic Area.
- eID is a **building block of the Digital Single Market**, allowing the establishment of cross-border distance electronic relations in the e-Government field.
- eIDAS may be extended to include the recognition of **eIDs for private sector uses**, such as AML/CFT, online platforms, etc.
- Its **technology-neutral approach** could easily allow the usage of SSI systems, constituting a real opportunity for their adoption.
- eIDAS Regulation has a **strong influence in the international regulatory space**, thanks to UNCITRAL recent works.

SSI/eIDAS use cases

- Using eIDAS identification means (and qualified certificates?) to issue verifiable credentials
  - The first use case considers the utilization of an electronic identification system for the validation of the identity attributes that are to be included in any assertion associated to a DID. This would be a scenario in which a means of identification recognized in accordance with the eIDAS Regulation is used to verify the information that will be included in a Verifiable Credential (eSSIF Verifiable IDs).
  - eIDAS Interoperability regulation defines minimum data sets for natural persons and for legal persons, while Annexes I and III of eIDAS Regulation define the same data set in the case of qualified certificates.
  - The main advantage of using this approach is that the Verifiable Credential inherits the level of assurance of the eIDAS electronic identification means, allowing a person with this kind of eID to get different Verifiable IDs and leveraging their use in the space of decentralized transactions, gaining real privacy.
  - This is specially true in case the focus on the recognition of specific types of Verifiable ID Presentations.

SSI/eIDAS use cases

- Using qualified certificates to support verifiable claims (EBSI eIDAS bridge) and legal evidences with full legal value
  - Qualified certificates are regulated under articles 28 (natural persons) and 38 (legal persons) of eIDAS Regulation.
  - They confirm the identity of the natural person or the legal person.
  - May also contain other identity data, such as mandates.
  - When qualified certificates are operated in the Cloud, they are specially suitable to authenticate and protect Verifiables Credentials using qualified electronic signatures and electronic seals, thus providing the maximum legal effect and acceptance to blockchain-based transactions.
  - Of course, with qualified certificates we have confirmation of identity but not confirmation of authority to issue a particular claim. Thus, we need to define governance rules (eSSIF Trusted Issuers).

SSI/eIDAS use cases

- Using SSI VCs as an eIDAS identification means
  - Although electronic identification under eIDAS Regulation is today clearly aligned with SAML-based infrastructures (see Opinion No. 2/2016 of the Cooperation Network on version 1.1 of the eIDAS Technical specifications, and eIDAS eID Profile, nothing in the eIDAS or its implementing acts should prevent the usage of a SSI system as an electronic identification means.
  - Thus, the second use case considers a Verifiable Credential as an eIDAS compliant electronic identification means, enabling –at least– transactions with Public Sector authorities and Public Administrations and, if so decided by its issuer, also with private sector entities, for AML/CFT and other uses.
  - Again, it would be better to put the focus on a specific type of Verifiable Presentation as an electronic identification means, including rules on the different Verifiable Credentials presented.
  - Interesting also in light of the future UNCITRAL law.

SSI/eIDAS use cases

- Using blockchain plus SSI as an electronic registered delivery service
  - Article 3(36) of eIDAS Regulation: a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorized alterations.
  - Article 43 of eIDAS Regulation
    - 1. Data sent and received using an electronic registered delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.
    - 2. Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.

Legal assessment relevant findings

- eIDAS is an appropriate regulatory framework to embody specific SSI solutions, such as EBSI eSSIF Verifiable IDs proposal, aligned with assurance level substantial (or high, depending on the user device and setup).
- A proposal could be to approve eSSIF Verifiable IDs as a new instance of electronic identification interoperability network type (not a specific technical solution, but a set of rules to allow for the usage of different market solutions). It would be convenient to slightly modify three implementing acts:
    - Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014.
    - Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014.
    - Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014.

Legal assessment relevant findings

- As eIDAS does not regulate the eID itself (because it is considered a national prerogative), but only its cross-border recognition, many legal issues will be dependent on national legislation, affecting the effective use of the eSSIF Verifiable ID:
  - The possibility of using a notified Verifiable ID to authenticate in front of private sector consumers.
  - The possibility of delegating Verifiable IDs to different holders.
  - All the legal regime of issuance and use of Verifiable IDs to minors o incapable persons.
  - The possibility (and the legal regime) of Qualified Trust Services Providers issuing Verifiable IDs as derived identities anchored in Qualified Certificates.
  - Any legal rule regarding user’s traceability when receiving and sharing Verifiable ID’s.
  - It would be convenient to widen the legal scope of the eIDAS legislation, to reduce the complexity of the system.

Legal assessment relevant findings

- eIDAS does not currently offer an appropriate legal framework for other types of Verifiable Credentials
    - This is reasonable from the perspective of the legal regime of the content (e.g. a diploma).
    - It would be an opportunity to extend the eIDAS Regulation to schemes for the self-managed sharing of identity attributes (e.g. eSSIF Verifiable Attestations), leveraging the legal infrastructure to create the general framework for this process. Other legal norms would define the rules associated to the content (thus fostering the reusable building block concept).
    - It will require major changes in the eIDAS Regulation.
- Immediate legal challenges
    - Define governance rules for any eSSIF-compliant solution (usually known as an identity trust framework).
    - Define a legal charter defining the rights, obligations and liabilities of all parties (issuers, users and consumers, but also Member States granting any notified system based in Verifiable Credentials), for any eSSIF-compliant solution.

GDPR assessment

- The legal grounds for the data processing can vary according to the application developed for which the data is processed.
  - While consent can be the main framework within which the controllers find legitimation to process personal data, the legitimate interests of the controllers in the different use cases can be assessed according to article 6(1)(f) GDPR, "including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place" (Recital 47 GDPR).
- The generation of public and private keys that will constitute the identity of the data subject in order to permit them to sign each transaction constitute pseudonymous data and thus are considered personal data.
  - The existence of public keys on blockchains, combined with necessary privacy enhancing mechanisms (PETs) will fulfil the data minimisation requirements of the GDPR. The DID document of each citizen will contain the public key of the individual and a DID address, all encrypted with the private key of the citizen and stored on the shared database Kassandra, the private key will be stored solely in the citizen's device.

GDPR assessment

- Regarding the consideration of hashes as personal data
  - EBSI v.1.0 will not pose a significant reidentification risk due to the limited amount of participating entities and user base, the risk-based assessment will have to become broader for subsequent versions.
  - In the case of only hashes of sufficiently blinded diploma data being stored on the blockchain to allow prospective employers to verify data provided to them off-chain, the hashes stored on the blockchain are thus likely not to be considered personal data. However, this is only the case when the possible parameter space of the original data is sufficiently large and/or sufficient blinding was actually carried out.
  - The design of the system should also include assessment of organisational measures that guarantee the removal of any information that allows for reidentification.
  - Given the aforementioned risk-identification, management of technical and organisational measures that data controllers need to take into account, EBSI v.1.0 can be launched in compliance with data protection rules and the GDPR.
- A full DPIA should be produced, specially from the cryptographic perspective.

Thanks!

Questions?

2nd EBSI eSSIF Stakeholders meeting