SSI eIDAS Legal Report

How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market

Dr. Ignacio Alamillo Domingo

April – 2020

Blockchain / DLT Technologies

EUROPEAN COMMISSION

European Commission
B-1049 Brussels

2020

SSI eIDAS Legal Report

How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market

INTERNAL IDENTIFICATION

Specific contracts 003604 and 003491 under Framework Contract DI/07445-00 (STIS IV)

DISCLAIMER

The work was co-funded by the ISA^2 programme, as part of the Innovative Public Services action, and the CEF Digital programme, in the context of the European Blockchain Services Infrastructure building block. The H2020 EU Project OLYMPUS, under Grant 786725, supported part of this work.

The author is Dr. Ignacio Alamillo Domingo (Astrea La Infopista Jurídica), Lawyer, CISA, CISM, researcher at iDerTec (University of Murcia).

2020

2020

Table of contents

Table of figures

Glossary of terms and acronyms

Authoritative source	Any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity (eIDAS Security Regulation).
Consumer rights Directive	Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (Text with EEA relevance).
e-Commerce Directive	Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.
eID	Electronic identification means, as defined under eIDAS Regulation
eIDAS AdES Formats Decision	Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance).
eIDAS Cooperation Decision	Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) Nº 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance)
eIDAS Interoperability Regulation	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 of the European

	Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance).
eIDAS Notification Decision	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 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (notified under document C(2015) 7369).
eIDAS QSCD Decision	Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance).
eIDAS Regulation	Regulation (EU) Nº 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Text with EEA relevance).
eIDAS Security Regulation	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 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance).
eIDAS TL Decision	Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance).
eIDAS Trust Mark Decision	Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services (Text with EEA relevance)

eSign Directive	Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
ESSIF Architecture	The definition of ESSIF and all related actors and building blocks at functional level, at level of concepts, at level or resilience/trust requirements, at level of interactions (including all corresponding technical and operational standards).
ESSIF Infrastructure	All supporting capabilities/services which support the functioning of ESSIF and all its members and framework-abiding relying parties, issuers and users.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
IdP	Identity Provider
MDS	Minimum Data Set, defined in the eIDAS Interoperability Regulation.
QTS	Qualified Trust Service, as defined under eIDAS Regulation
QTSP	Qualified Trust Service Provider, as defined under eIDAS Regulation
SSI	Self-Sovereign Identity
Subject	Anything that is known to exist somewhere in the real world and to which one can concretely refer to: can be people, organisations, things/devices, resources (EBSI ESSIF). The legitimate natural or legal person that is, or to be, represented by the electronic identification means (Guidance for the application of the levels of assurance which support the eIDAS Regulation).
TL	Trusted List

TS	Trust service, as defined under eIDAS Regulation.
TSP	Trust Service Provider, as defined under eIDAS Regulation.

Part 1. An introduction to Self-Sovereign Identity

1. THE TRANSFORMATION OF DIGITAL IDENTITY

Digital personhood is understood as the projection of personality rights to the Internet space, through the creation and control of user agents (personal profiles, in some cases, avatars), which are used in interactions on the Internet, with frequent support in corporate or social network service providers, known as identity providers (IdP).

It is a model characterised by direct personal agency in the network, as opposed to third party management through passive user profiles, and its legal regime is configured as a result of three forces in permanent tension: identity, privacy and law enforcement (Alamillo Domingo, 2010b).

Under the expression "digital identity", we refer to techniques that allow people and organisations to identify themselves and act on networks, using more or less strong authentication mechanisms.

From a more technical perspective, digital identity is a form of identity resulting from the digital codification of identifiers in a way that is suitable for processing and interpretation by computer systems (Jøsang, Fabre, Hay, Dalziel, & Pope, 2005). Moreover, following these authors, “a person’s or an organisation’s identity consists of the individual characteristics by which that person or organisation is recognised or known”, elements that “can be acquired, such as name, address, nationality, registration numbers and memberships, or can be inherent, such as with biometrics”.

Different from digital identity is the concept of identifier. In fact, “any characteristic element can be called an identifier when it is used for identification purposes”. While “it is assumed that identities are unique, i.e. no two human beings or organisations have the same identity”, on the contrary, “the same person or the same organisation can have different identities in different contexts, and each identity is reflected by a different set of identifiers·. Thus, “an identifier is usually only unique within a given context [and] the different types of identifiers can be quite varied in their characteristics, and may be transient or permanent; inherent or applied; self-selected or issued by an external authority; interpretable by humans, computers, or both, etc” (Jøsang, Fabre, Hay, Dalziel, & Pope, 2005).

Digital identity has evolved significantly in the last 25 years, including hierarchical public key infrastructures and federated, user-centric, delegated authentication.

All these identities, are digital, because they are assigned, stored and managed electronically, in identity databases, which vary from identity silos completely disconnected from each other to complex networks of interconnected identity data, in the financial or crime-fighting domains. Furthermore, all these identities can be considered as “second- or third-party identities”, because they are provided to us by organisations or people different from us. They are second-party identities when they only serve to establish electronic relationships to the organisation or person that has supplied them to us, and they are third-party identities when they serve to establish relationships to organisations and people different from those that have provided them to us, as happens with qualified electronic signature certificates or

with delegated authentication infrastructures, such as those currently adopted under the eIDAS Regulation.

More recently, with the advent of Web 2.0, we users have begun to act as issuers or guarantors of our own identity, disclosing a set of personal data that allows third parties to recognise us. Specifically, on the social Web radically new examples of electronic relationships appeared: social networks (Facebook, Google+), collaborative spaces (Google Docs, Box.com), social communication streams (Twitter), virtual worlds (especially in the gaming environment), or the Cloud, which were based on first-party identities; that is, self-generated and managed identities by the users themselves, under self-regulation criteria, such as convenience or pseudonymisation, in the process of acquiring and learning how to use their digital personhood.

These systems constituted a new paradigm in identity management, based on the self-management by the user of the entire life cycle of her identity, with greater control over the disclosure of personal data. They were the so-called "first-party" or "user-centric" identities, and promised a new privacy model under true user control, but maintaining the dependency of user with respect to the identity provider.

The existence of all these systems, and their application in heterogeneous environments, led to the emergence of a digital identity ecosystem, with an increase in complexity in the management of the data itself, and the appearance of new risks for the privacy of natural persons.

From this initial perspective, it can already be indicated that the digital identity is a human artefact, an electronic document with a series of information referring to a person –not the person itself– issued by the person himself or by third parties, including the State, public and private organisations, and other citizens.

From a social point of view, digital identity presents a series of specific properties, identified by the OECD (Rundle, y otros, 2007):

- Identity is essentially social. Since the people you refer to are social and live in society, they need to be able to recognise who they interact with in their relationships, especially when those relationships are persistent over time. As we project our personality onto the web, especially on social media, our digital neighbours effectively characterise and recognise us, even on occasions when there has been no face-to-face identity verification.

- Identity is subjective. Both the perception of the "I" that we all have and the different perceptions of the "we" that others attribute to us constitute subjective identities, based on the experience that different people construct and that allow them to recognise us; that is, identity is somewhat subjective to the people who attribute it to us.

  The experience in digital scenarios where multiple participants intervene, such as collaborative environments or social networks has shown that we are known for what we disclose, and for what other people we interact with interpret, so it is advisable to be cautious.

- Identity is valuable. By accumulating historical data regarding people's actions, informational capital is created that can be used to establish personalised relationships and to make decisions in our relationships with people, with a greater degree of trust, as the theory of games and, in particular, expectations management.

  As time has proved, the business model of Internet intermediaries, especially search service providers, and more recently, of Cloud service providers, consists of learning from our actions to offer us highly personalised advertising or to improve search results, relying on digital identities registered by the provider or even linked to the access device, as in the case of the cookie-based digital identity.

  It is a model in which digital identities are generated and managed without the need to know the name and surname of natural persons, which does not prevent the provider from identifying you and knowing you perfectly, provided that a reasonable period of use of the service has passed.

  Likewise, the main social network service providers have shown how the modelling of the digital person as an information graph, which in turn is a node of the social graph, allows the creation of social profiles where information about the person is integrated, purportedly under your control.

- Identity is referential. In fact, an identity is not a person, but a reference to a person. Even in the event that a person develops various own profiles, or if third parties develop profiles about us, ultimately the set of attributes that identify a person must refer to him reliably.

  One of the most interesting discussions on digital identity refers precisely to the semantics of identifiers on the Internet, especially in light of the advent of the so-called Semantic Web, where people, objects, resources ... are identified by URIs or uniform resource identifiers, whose semantics must be properly defined (Halpin, 2011).

- Identity is composite. While some information is provided voluntarily by ourselves, other information about us is constructed by third parties, without our participation.

  Around this characteristic of identity, many of the problems of lack of control in the emerging social networks are visualised, such as user labelling, and the response that providers provide, in the form of greater participation and control in relation to what third parties they publish about us.

- Identity is consequential. Because identity information speaks to our past actions, the decision to exchange identity information carries consequences: in some circumstances, disclosure of this information can lead to harm, and in other cases, precisely nondisclosure, which can create risks.

  Many of the risks associated with digital identity derive from our overexposure to the network, in the form of profiles and social streams based on our identity, especially at a time when there is still a significant lack of awareness by users about the difficulty of making disappear a content published on the Internet.

- The identity is dynamic, because it is in constant change and modification, so that any file with identity data can be found obsolete at a certain time. Especially on the Internet, digital identity should be viewed as a stream of information rather than a still photo of a person. This flow is generated in the conversations of social networks, and the digital biography compiled and exposed by the main social networks, actively.

- Identity is contextual. As we have seen previously, people have different (partial) identities that we may want to keep completely separate. Given that information can be harmful used in the wrong context, or simply be irrelevant in that context, keeping identities segregated from each other allows us to have more autonomy.

- Identity is potentially misleading, since the process of identifying and associating identity data is inherently error-prone. This issue should be highlighted: no identity/authentication mechanism is free from possible error, in spite of the probability that it is higher in some cases than in others.

An additional property of digital identity is that it sometimes allows authentication; that is to say, the possibility that we associate technical mechanisms that allow us to demonstrate who we are on the Internet and that we act on one of our identities: these are “active” identities, unlike our “passive” identity information or that reside in databases.

Some of these identities can be considered a public good, and are even mandatory (a State issued electronic ID, for example), while other identities are considered a kind of private asset, and their obtention and usage is voluntary (such as an electronic signature qualified certificate issued by a qualified trust service provider), or is associated with a specific service or legal relationship (for example, a strong customer authentication provided by a payment service provider under PSD2 Directive).

Not all identity authentication mechanisms can be considered equal, but the identities assigned to us have different qualities and limitations of use. For this reason, we speak of multilevel identity and authentication systems, which classify these mechanisms in degrees of security for the purposes of their use, in accordance with considerations based on risk analysis. This is something known as authentication levels of assurance in technical specifications[1].

In short, the relationship between personal identity and authentication mechanisms is increasingly important, since only people who can authenticate themselves are electronically active and capable agents, being able to exercise their rights online, but at the same time they are faced with various abuses and fraud related to the so-called "identity theft".

Normally, we all have many identities, partial, that are appropriate to the different roles and activities that we carry out during our lives, which use is protected in a particularly intense way under personal data protection regulation. Thus, any regulation of digital identity must be formed from the social construction of the risks around identity, its use and (possible)

[1] See ISO/IEC 29115:2013. Information technology — Security techniques — Entity authentication assurance framework, for instance.

misuse, as well as the adoption and respect of the fundamental right to data protection (Alamillo Domingo, 2010b).

The importance of digital identity manifests in all social sectors and, of course, is reflected in public policies, in the form of an incipient "right to digital identity". In this sense, (Sullivan & Burger, 2019, pp. 233-234) emphasise that "on 25 September 2015, the United Nations (UN) General Assembly formally adopted the 2030 Agenda for Sustainable Development which consists of 17 Sustainable Development Goals (SDGs) and 169 specified targets to be achieved by member nations within the next 15 years", including SDG 16.9, mandating nations to "[b]y 2030 provide legal identity for all, including birth registration", a goal that underpins seven other SDGs to be achieved by the UN member nations. As these authors point out, "this is the first time that a legal identity for all persons has been officially stated as a global objective", recognising that "has significant implications for governments and individuals". Furthermore, they signal as an important issue that "«legal identity» is not defined in SDG16.9 and unlike the terms «legal person» and «legal entity», legal identity is not a term which has legal meaning", adding that "identity is not a concept traditionally recognised by the law in many countries, particularly those with a common law legal heritage", and that "even in civil law countries, where there is a legal concept of identity, it was developed for another era and does not address the nature and implications of a digital identity".

For these authors, "an individual right to identity exists under international law and is poised for greater recognition in light of UN SDG 16.9 and the use of blockchain for identity", adding that "digital identity is protected under Article 1 (1) of the ICCPR[2] because the Article protects individual autonomy and that is directly relevant to the use of blockchain for identity authentication, especially considering that it purports to give the individual control over his/her identity information and who can access it" (Sullivan & Burger, 2019, pp. 254-255).

2. SELF-SOVEREIGN IDENTITY

Digital identity management systems based in distributed ledger technologies (DLT) may play an important role in the implementation of a personal right to identity, with a strong view of self-determination and personal autonomy, at least when we refer to natural persons.

These distributed ledger technologies, and in particular blockchain technology, normally based on public key cryptography, allow the creation of an immutable registry that is managed in an absolutely decentralised way, allowing new applications hitherto unthinkable, with a transforming potential beyond any doubt.

As far as we are concerned now, (Swan, 2016) characterises blockchain technology as a software protocol and a distributed logbook for recording transactions, which can act as a global computational substrate for processing any type of digitised activity. From an abstract point of view, blockchain technology allows updating all the nodes of a network in a

[2] International Covenant on Civil and Political Rights (ICCPR), which was adopted by the UN General Assembly Resolution 2200A (XXI) of 16 December 1966, entered into force on 23 March 1976, in accordance with Article 49, for all provisions except those of Article 41; 28 March 1979 for the provisions of Article 41 (Human Rights Committee), in accordance with paragraph 2 of Article 41.

distributed computing environment with the current state of the world, thus allowing to confer a shared state of trust to a distributed system; that is to say, when a performance is recorded using these technologies, what really happens is that this record is made in a large number of different places, instead of a single centralised place, so we can consider that such record is true.

In short, we are faced with a system in which we can write any information we want, using a network node; from that moment, said information will be copied to all the remaining network nodes, so none of them will be able to delete said information unilaterally. Only with the help of a large number of nodes could an insertion in said network be eliminated, so it is not necessary to trust any one of them in particular, and that an information insertion that has spread within the network is considered be considered "true". This does not mean, of course, that the information itself is true, but it only that is true that this information was written, and not any other information.

One of the interesting use cases of DLT refers to the so-called self-sovereign identity (SSI), which is the one created and managed by each person individually, without the intervention of third parties. SSI systems have been proposed as the next step in the evolution of the identity management practice. As explained by (Allen, 2016), "rather than just advocating that users be at the center of the identity process, self-sovereign identity requires that users be the rulers of their own identity".

This author builds on the notion of Sovereign Source Authority (SSA), "the actual default design parameter of Human identity, prior to the «registration» process used to inaugurate participation in Society" by (Marlinspike, 2012), who considers that "the act of «registration» implies that an administration process controlled by Society is required for «identity» to exist. This approach contrives Society as the owner of «identity», and the Individual as the outcome of socio-economic administration"[3].

For (Allen, 2016), any "self-sovereign identity must also meet a series of guiding principles", based in previous works related to user-center identity management systems, including (Cameron, 2005). These principles should guide the design of SSI solutions, but of course they have evolved and still evolve as new potential implementation appear.

- Existence. Users must have an independent existence, in a self-referential approach, meaning that the person is the kernel of self, because Self-Sovereign Identity references every individual human identity as the origin of source authority (Marlinspike, 2016).

- Control. Users must control their identities, but this doesn't mean that a user controls all of the claims on their identity, if they are not central to the identity itself.

- Access. Users must have access to their own data, being able to easily retrieve all the claims and other data within his identity.

[3] Marlinspike's approach toward individualism certainly reminds American transcendentalism (https://plato.stanford.edu/entries/transcendentalism/) and other philosophical movements that consider society as a personal decision, an opt-in system, due to the inherent self-sovereignty of any human.

- Transparency. Systems and algorithms must be transparent, using free, open-source, well-known, and as independent as possible of any particular architecture.

- Persistence. Identities must be long-lived, but respecting the right to suppression.

- Portability. Information and services about identity must be transportable. Tu ensure this, identities must not be held by a singular third-party entity, even if it's a trusted entity that is expected to work in the best interest of the user.

- Interoperability. Identities should be as widely usable as possible. This principle builds on previous efforts to build an identity metasystem or layer for the Internet (Cameron, 2006).

- Consent. Users must agree to the use of their identity. The author notes that this consent might not be interactive, but it must still be deliberate and well-understood and we may add that fully compliant with the applicable data protection regulation.

- Minimalisation. Disclosure of claims must be minimised.

- Protection. The rights of users must be protected in case of a conflict between the needs of the identity network and the rights of individual users.

In words of (Marlinspike, 2016), "Self-Sovereign Identity must emit directly from an individual human life, and not from within an administrative mechanism created by, for, as abstractions of individual human activities, and must remain amenable in design and intent directly by individual humans with original source authority".

Allen's and Marlinspike's construction of self-sovereign identities account for a narrow concept of "identity" as a specific identifier that allows self-management, in the sense of being able to authenticate the person, self-assert claims, receive and control third-party asserted claims and share them, without any dependence from a third party, being that third party a public or a private identity provider. The ideological approach does not preclude the possibility that other parties issue identity assertions, if they are not "central to the identity itself" (Allen, 2016), recognising the notion that identity is a social construct. Thus, SSI can support quite different models for issuing and sharing identity assertions or claims.

From a technical perspective, this verifiable, self-sovereign digital identity is based on a type of identifier, which is called a "decentralised identifier" (DID), and, in technical terms, it is a URL –that is, an identifier universal or uniform resource locator, with its own rules of syntax and processing– which relates a subject with a "decentralised identification document" (DID document), which describes how such DID should be used, and, in particular, how the DID document supports the authentication of the subject associated with the DID, as shown in Figure 1. It is also important to remark that the DID, by itself, as identifier, it is not an identity.

One of the peculiarities of a DID is that it is based in DLT or other forms of decentralised networks[4], so it does not require a centralised registration system, allowing the implementation of a Decentralised Public Key Infrastructure (DPKI), a combination of DIDs for decentralised identification and Decentralised Key Management System (DKMS), as opposed to the classic hierarchical PKI systems, which are precisely based on the centralization of the issuing function in the hands of a provider, although with nuances (in fact, the PKI is not an absolutely centralised system either, but there are multiple providers, with their own PKIs, that compete with each other, which has forced to establish trust models that are somewhat decentralised, although it can be said that the centralization of trust management has shifted towards trusted lists and browsers).

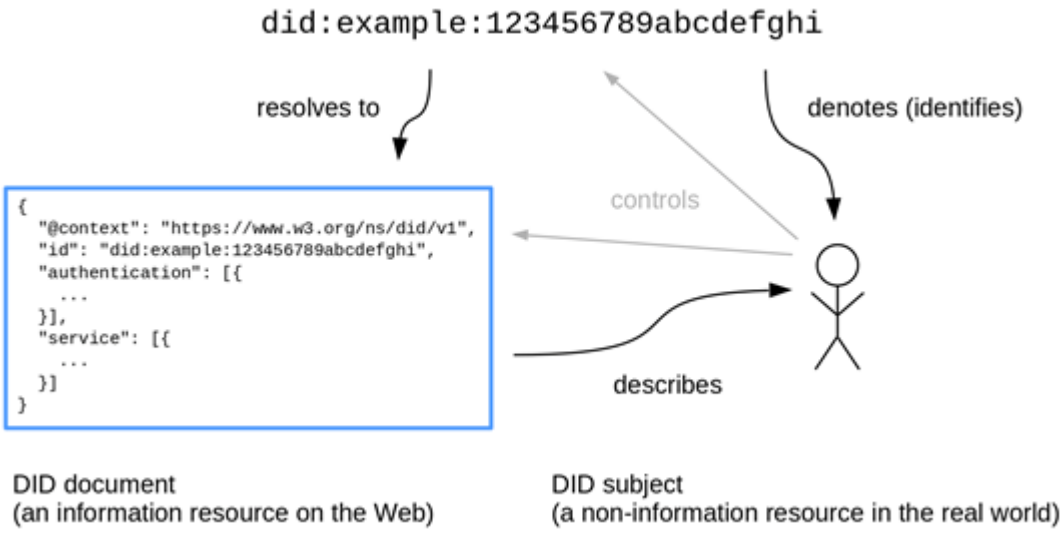

Figure 1. Relationships between DID, DID document and subject (Reed & Sabadello, 2020)

Thus, DKMS is proposed as a new approach to cryptographic key management intended for use with blockchain and distributed ledger technologies where there are no centralised authorities, inverting the core assumption of conventional PKI architecture, namely that public key certificates will be issued by centralised or federated certificate authorities (CAs); because with DKMS, the initial "root of trust" for all participants is any distributed ledger that supports a DID (Reed, Law, Hardman, & Lodder, 2018).

Starting from a DID –such as, for example, `did:example:123456789abcdefghi`–, anyone can go to the Internet to obtain the corresponding DID document that describes the DID in question (an operation called DID resolution), and use its contents to authenticate the subject and to obtain attributes or claims about it, such as name and surname, or other personal information to share. As can be seen, the DID document is outside the blockchain, which allows compliance with data protection regulations.

Building upon DID documents, advanced self-sovereign identity proposals use verifiable credential sharing syntaxes, such as that described in the Verifiable Credentials data model

[4] (Stokkink & Pouwelse, 2018) consider that, by leveraging a blockchain structure, transparency, persistence, full control, existence, access and consent principles are achievable.

promoted within the W3C Consortium, related to the subject's corresponding DID, as shown in Figure 2.

Therefore, in SSI-based credential management systems, the user can obtain credentials claiming identity attributes, issued by entities that have previously verified them, and share them with third parties.

Unlike authentication delegation systems, in which an identity provider intervenes in each authentication, in these self-sovereign identity systems such intervention disappears, as shown in Figure 3.

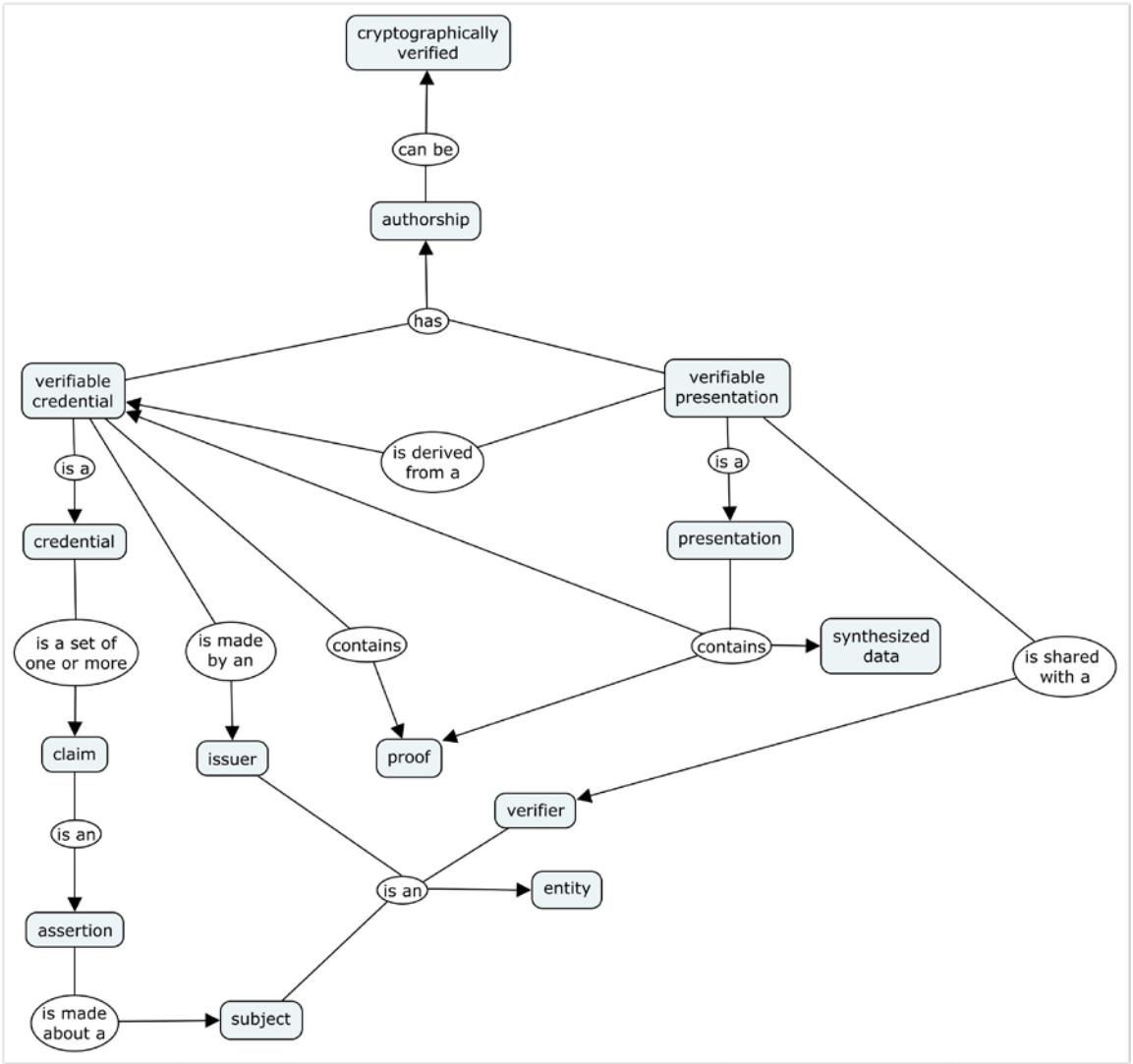

Figure 2. Verifiable Credentials and Presentations conceptual map (Alamillo Domingo, 2019b).

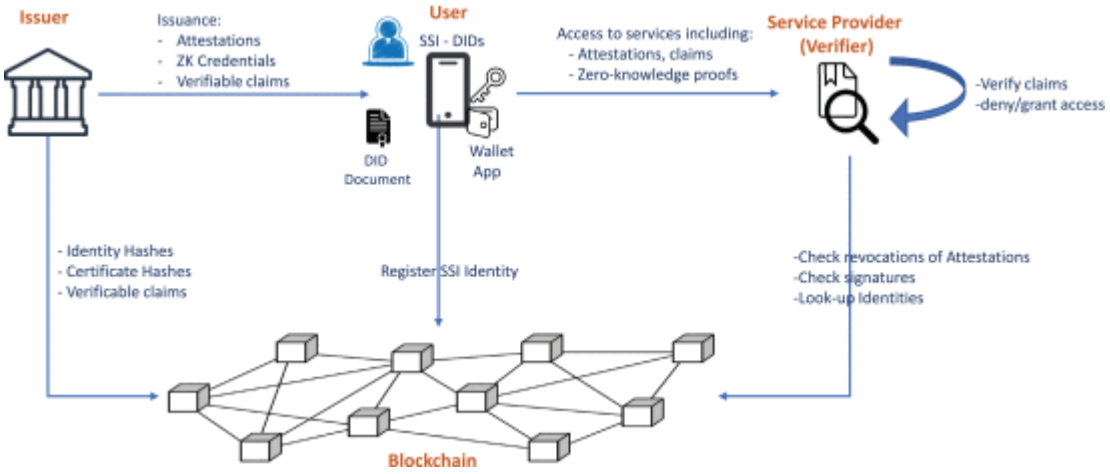

Figure 3. Self-Sovereign Identity Management Model in Blockchain (Bernal Bernabé et al, 2019)

Thus, SSI is supposed to increase subject's electronic privacy, because it reduces two of the main risks associated with authentication delegation systems; namely, the possibility of identity theft with respect to data managed by the identity provider; and, more importantly, the monitoring of user behaviour by the identity provider, that have access to authentication transaction metadata, something that allow the creation of user profiles.

While (Bernal Bernabé, Canovas, Hernández-Ramos, Torres Moreno, & Skarmeta, 2019) recognise that IdM based on self-sovereign identities "focuses on providing a privacy-respectful solution", in which "citizens are not anymore data subjects, instead, they become the data controller of their own identity", they also identify a number of privacy challenges that appear in the application of blockchain technology in different domains, including transaction linkability issues, private-keys management and recovery, malicious smart contracts, non-erasable data & on-chain data privacy, post-quantum computing resistance, crypto-privacy performance, privacy-usability, malicious-curious trusted third parties, privacy enforcement in constrained systems, privacy interoperability across different blockchain-enabled scenarios and compliance with privacy and data protection regulations.

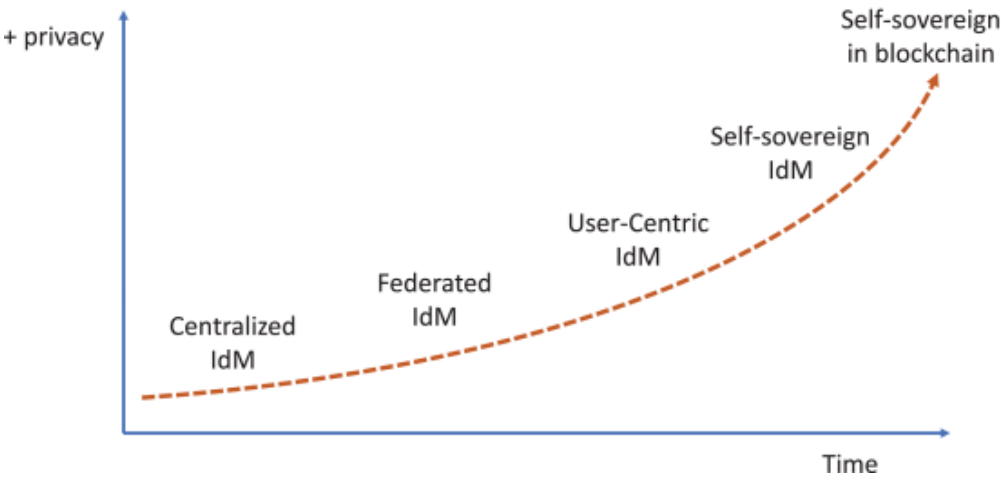

Figure 4. Identity management methods evolution over time, according to privacy preservation capabilities (Bernal Bernabé et al, 2019)

From a legal perspective, some of the risks of centralised delegated authentication identity management systems have been analysed by (Timón, et al., 2020), using a data protection impact analysis methodology to evaluate how oblivious authentication solutions –such as PESTO (Baum, Frederiksen, Hesse, Lehmann, & Yanai, 2019)– reduce exposure. This work is relevant as shows how distributed computing applied to password-based authentication systems reduce risk. The technologies developed in the OLYMPUS project help protecting the use, by legitimate users, of their SSI-control keys, especially when using Cloud wallets.

From a different perspective, whether SSI will provide fully autonomous agency to netizens is something yet fully unclear. As (Trotter, 2014) explains, "autonomy as self-sovereignty is the quality of living in accordance with one's inner nature or genius" and, as such, "a condition for autonomy as self-sovereignty is living apart from, or in defiance of, powers that compel one to forfeit or exchange quantities of life for «goods» that one does not recognize as such, or does not recognize as worth the exchange". Furthermore, "autonomy, thus conceived, is «self-governance» only in the sense that certain prerogatives of personal choice are granted to individuals, so long as they conform to some variation in the inventory of permissible lifestyles", but recognising that "ultimately, each of us is owned by the state, which grants leeway –albeit sometimes in an apparently liberal and generous manner– to govern and dispose of certain aspects of our bodies and lives, so long as the state regards such prerogatives as in the collective best interests". Trotter's characterisation of personal autonomy shows quite well the philosophical basis of SSI as human autonomy, but also the restrictions that such a system must accept when designed for a societal use, because it is not possible to create a system that allows full autonomy in real world, less if that system is to be used to enter intro relationships in regulated environments.

Truly, as (Sullivan & Burger, 2019, p. 256) say, "the point of identity, especially digital identity, is to enable the individual to conduct transactions, whether they be transactions with the government, such as receiving benefits, paying taxes, voting, and so on; or transactions with other entities, such as banking, receiving a salary, buying goods, paying rent, and so on", adding that "these transactions, particularly the commercial transactions, happen because the parties involved trust the credentials. Specifically, they trust the credentials do in fact represent the authenticated identity the claim to represent". Governmental intervention as producer or trustworthy documents for traditional know-your-customer processes is important, but there are cases where "establishing trust using conventional means […] would be virtually impossible", so "by using public blockchain technology, they are able to establish trust in their crowd-sourced identity verification system", establishing "trust in the veracity and integrity of their identity assertions by leveraging the immutability of the blockchain and opportunity to have the data on the blockchain publicly available".

With respect to the "ownership" of the identity token, though, it is also interesting to point out that (Arslanian & Fischer, 2019) have produced a high-level taxonomy based primarily on the intended usage and functionalities of the token related to crypto-assets, considering identity attributes as non-fungible non-transferable crypto-assets: they are non-fungible because a given token with identity attributes is not functionally identical to and interchangeable with any other token of the crypto-asset; and they are non-transferable because identity attributes are inalienable and, therefore, non-tradeable. This would be the legal consideration of a DID or any other tokenised identity attribute.

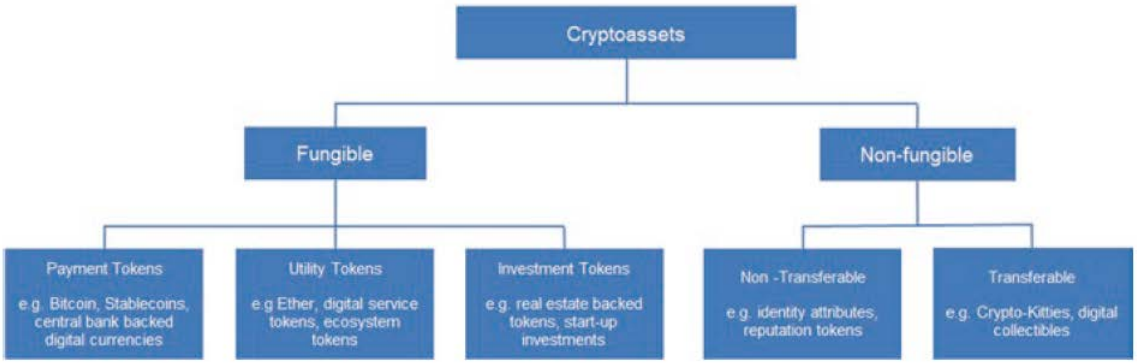

Figure 5. Proposed taxonomy of crypto-assets (Arslanian & Fischer, 2019)

For (Lim, et al., 2018, p. 1744), who conducted a wide survey of relevant blockchain-based identity management solutions, "self-sovereign identity management, blockchain and Distributed Ledger Technology are going to patch the gap that current technology falls short of providing a secure and cost-efficient identity management framework". While "Blockchain identity management and authentication solution by design is distributed, decentralized and fault tolerant which decreases the deployment and maintenance cost […], scalability seems to be the biggest challenge with public blockchain", due to what "by centralizing some parts of the technology, blockchain identity management will be more cost effective and secure".

Also, for these authors, "blockchain technology does not resolve access management issues such as key management problem that is inherent in server centric and federated identity environment", and "another long-running problem with identity is around the verification of user identity, in which there is no one responsible and liable for vetting data, the same problem where federated identity projects have become stuck" proposing "the solution to this problem is probably to extend the notion of zero knowledge proof in self-sovereign identity management".

(Kuperberg, 2019) has conducted a systematic survey of blockchain-based identity and access management (IAM) solutions that "covers features, prerequisites, market availability, readiness for enterprise integration, costs, and (estimated) maturity", using a complete use case approach (Figure 6) in support of an evaluation framework consisting of 75 criteria, including 12 compliance and liability criteria (Figure 7).

For this author, "in terms of compliance and liability […] all of the studied offerings are in the very early stages. In particular, GDPR compliance […] can only be offered by running a permissioned consortial network where the location of the blockchain nodes is strictly regulated. For the Sovrin network, there is a series of articles covering GDPR in details, but no guarantees are given. None of the solutions is certified by a trusted third party (such as TÜV)" (p. 17); thus, he concludes that the "the high maturity of conventional IAM solutions is not yet found in the blockchain-based IAM solutions and offerings", assuming that "for the decentralized and sovereign identities, such sophistication remains a very large challenge" (p. 19), reinforcing the need for projects such as EBSI ESSIF and its alignment with the trust framework embodied in the eIDAS Regulation, even assuming the potential need to update or extend it. In fact, this author expects "to see research on large-scale hybrid deployments in the areas of e-government and eIDs (electronic ID documents)" (p. 18).

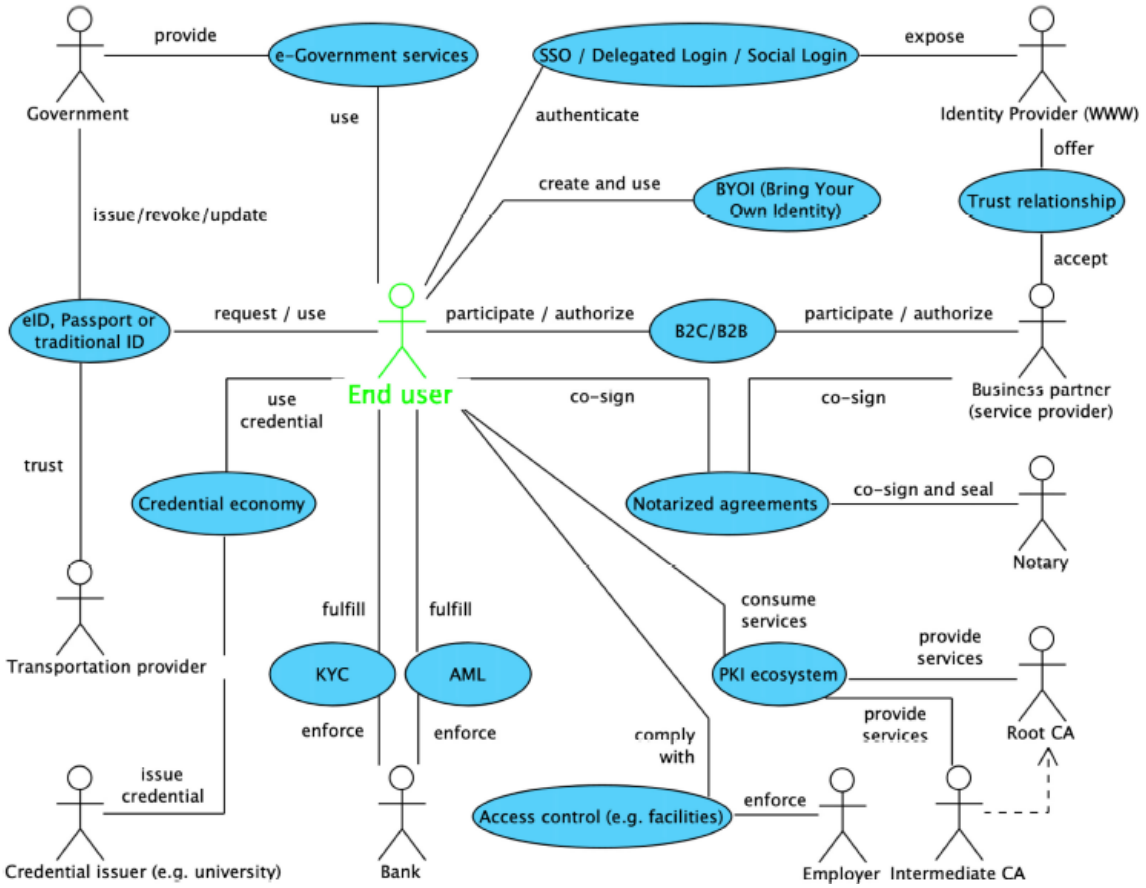

Figure 6. Use cases and actors for identity management (Kuperberg, 2019)

Number	Criterium description
CL01	GDPR Compliance and Support (incl. inspection, download and deletion of personal data), explicitly asserted and guaranteed by the vendor / service provider - mandatory for services available to EU customers
CL02	Control over geographical distribution of data (e.g. restriction to EU or exclusion of certain countries)
CL03	Credentials and access material can be rotated and withdrawn following central rules
CL04	Audit trail (user actions such as logins are protocolled, and so are changes to identity or access properties and privileges), in a GDPR-compliant way
CL05	Avoidance of liability for third-party offences (e.g. for situation where data is written to a shared co-owned ledger, but the data turns out to be punishable by law)
CL06	End-user data cannot be evaluated or sold by the identity provider (data sharing is turned off by default, but end users can choose to opt-in as well to opt-out again)
CL07	Identity export and transfer can be controlled to prevent identity theft (e.g. by preventing the export of a X.509 client certificate from a managed mobile/desktop device)
CL08	Hosting model (provider-offered service and/or provider-managed cloud hosting and/or customer-managed cloud hosting and/or customer-managed on-premise hosting)
CL08a	For hosted solutions: support desk (incl. contact over the phone) with quality-of-service
CL08b	For hosted solutions: Service Level Agreements (availability, performance, recovery time objective ...) and Support Level Agreements (bug fixing, patches, ...)
CL08c	No obligation for service providers to use a proprietary token/cryptocurrency to pay for IAM services
CL09	Certification by third parties (e.g. TÜV) w.r.t. security and data protection (implementation and/or deployment)
CL10	Payment model for service use (e.g. prepaid, postpaid or pay-as-you-go) and fixed prices in a convertible fiat currency (to prevent cryptocurrency rate fluctuation risks)
CL11	Purchase/usage includes rights to audit or even to reuse the source code; reuse rights might be restricted, as in the case of GPL open-source license
CL12	IAM network traffic from/to IAM-using backend applications can be isolated from internet traffic (e.g. through a VPN or a VPC)

Figure 7. Compliance and liability criteria (Kuperberg, 2019)

(Stokkink & Pouwelse, 2018, p. 1337) discuss the problem they perceive with the current identity ecosystem, "the first half of the problem we observe in the current identity ecosystem, is the fact that identity holders should also be the identity owners. This first half can be more formally described as the need for Self-Sovereign Identity. The second half of the problem consists of the passport-level attributes in this identity. In other words, identities

which are recognized by governments and therefore have legal value", adding that "in the context of blockchains we can formalize this second half of the problem as the need for legally valid signatures", in a clear reference to trust services regulation.

3. SSI AND TRUST GOVERNANCE

Major challenges of blockchain technology adoption for e-Government normally identified by scholars in literature reviews include the new governance frameworks and legal and regulatory support (Batubara, Ubacht, & Jansenn, 2018, p. 7). For these authors, "the absence of a general application platform, in which security, scalability, interoperability, reliability and flexibility of blockchain technology for e e-Government applications are addressed, raises the need for a proper design solution at the architecture level in accordance with the specific requirements from e e-Government processes", adding that "a proper legal framework within which blockchain can be utilized should be prepared", but also that "changes in legal frameworks and governance arrangements require careful considerations, especially in a changing environment with many uncertainties".

The emergence of identity management solutions based in blockchain, specially SSI, is also changing the way trust is governed, notably from the perspective of the relying parties consuming claims shared by subjects.

(Mühle, Grüner, Gayvoronskaya, & Meinel, 2018) show that in SSI systems "in order to accept the identity, the relying party needs to have a trustful relationship with the claim issuer", even if the system is under the full control of the person.

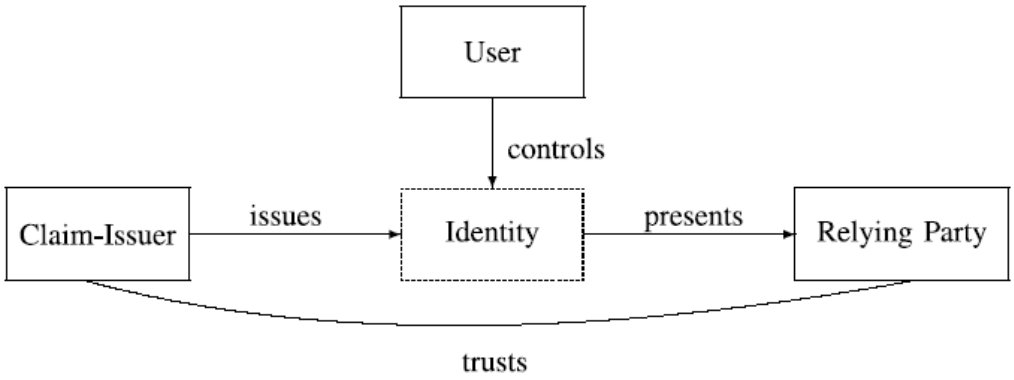

Figure 8. SSI trust relationship (Mühle et al, 2018)

In a different work, the same authors have analysed different trust models in blockchain-based identity management. Starting from the foundational work of (Jøsang, Ismail, & Boyd, 2007) on decision trust (defined by the later authors as "the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible"), they identify the different components to be considered when a service provider needs to trust a digital identity (Grüner, Mühle, Gayvoronskaya, & Meinel, 2018).

Thus, according to these authors, "in terms of identity management, considering digital identities, claims and attestations, the service provider or any other relying party depends on the identity provider for correctness and validity of the provided information. A service provider needs to trust that the digital identity is valid. Furthermore, trust into claims is required to rely on correctness and actuality of the statements. Moreover, trust into attestation

issuers to properly attest claims is an additional significant demand", assuming that "the required trust for a specific situation and information strongly depends on the extent of the potential negative consequences as well as the subjective risk appetite the service provider is willing to take". This problematic is not really specific to blockchain-based identity management systems; thus, "in addition to trust considerations on the overall identity management layer as application domain, the used blockchain technology requires reputation and trust management in additional functional components", such as the consensus protocol or the peer-to-peer communication (Grüner, Mühle, Gayvoronskaya, & Meinel, 2018, p. 1477).

Adopting the SSI principles imply, generally speaking, an increased complexity in trust management and a shifting from hierarchical or federated trust assurance frameworks –such as current eIDAS Regulation for electronic identification means notified for cross-border transactions–, to network-based socio-reputational trust models or accumulative trust assurance frameworks that use quantifiable methods to aggregate trust on claims and digital identities[5].

For (Haddouti & Ech-Cherif El Kettani, 2019), results of an evaluation of three popular identity management systems using blockchain technology show that "even if the main goal to adopt a Blockchain technology as infrastructure for Identity management is the removal of the central authority, this may not be a realistic goal in IdM applications due the context of identity maintaining a profound need for trust", signalling also the need to "build a more consistent view of Identity Management in order to preserve privacy when Blockchain is used" (p. 7).

It seems clear that designing SSI solutions aligned with legislation is a key identified need. In this sense, (Bouma, 2018) coined the expression Legally-Enabled Self-Sovereign Identity or LESS Identity, signalling a specific category of these solutions, different from those supported by social trust mechanisms, such as reputational ones. This concept imply that minimum disclosure, full control and necessary proofs requirements are legally-enabled; that is, backed up by the necessary or applicable legal framework to protect both the subject and those who are providing services to her.

[5] The latter is the proposal of (Grüner, Mühle, Gayvoronskaya, & Meinel, 2018, p. 1476).

Part 2. The eIDAS Regulation

The creation of trust in Internet transactions has been identified as one of the main needs for the proper functioning of the Information Society and, from the perspective of the European Union, of the internal market.

Due to the design of the Internet architecture, which somehow considered security as an optional service, to achieve an environment in which people feel safe and confident it is necessary to promote the adoption of such security services.

Moreover, a regulation of legal institutions that establish legal security bases in relation to these resulting services is an appropriate way to help people increase their confidence in the validity and effectiveness of their Internet activities.

Therefore, in recent years, the political and legislative agenda has incorporated specific lines of action in this regard, especially in the European Union, aimed at recognizing the legal effects of electronic equivalents of the main formal elements. of the written document; that is, the guarantee of the identity of the parties and the delivery of the consent, the moment of the delivery of said consent, and the moments of issuance and reception of the previous elements, when the parties are at a distance.

The 23rd of de July of 2014 the Council of the European Union passed in first reading the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), an important and transformative milestone in the legal regulation of the assurances of juridical traffic performed electronically (De Miguel Asensio, 2015, págs. 969-970).

The eIDAS Regulation constitutes the main trust framework in the European Union and the European Economic Area for natural and legal persons agency in the Internet.

This Regulation has, as stated in Article 1, a triple and apparently heterogeneous object, by virtue of which "(a) lays down the conditions under which Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State; (b) lays down rules for trust services, in particular for electronic transactions; and (c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication".

Numerals (a) and (c) of Article 1 list different types of "electronic evidence" of legal actions or transactions performed by individuals or entities –or of the computer systems they use, even without direct intervention in each case–, positioning the Regulation as a fundamental rule of the electronic accreditation of legally relevant actions, with a general and non-sectoral scope, as was already the case in Directive 1999/93/EC (Illescas Ortíz, 2001, pág. 89), especially in transactions in the internal market, although not exclusively limited to them.

Indeed, the legal institutions[6] listed in these two numbers –the electronic identification means of a natural or legal person, the electronic signature of a natural person, the electronic stamp of a legal person, the electronic time stamp, the certification of electronic delivery and Website authentication– correspond to technical artefacts that allow the accreditation of acts, but also of other facts, with and undoubted evidential relevance in the electronic space; that is, they are artefacts that support electronic evidence, in a functionally analogous way to how it has been happening in the physical world, especially in transactions accredited through the use of paper supports.

Thus, while an electronic signature, being equivalent to the handwritten signature, accredits the fact in which a legal act is manifested (the issuance of a declaration of will, for example), the electronic time stamp, by linking a series of data in electronic format with a specific moment, to provide proof that these latest data existed at that moment, accredits a gross fact, of the physical world, which will support, where appropriate, a specific legal or institutional fact (the issuance of the said declaration before a specific moment, for certain legally established purposes).

We are going to refer to these institutions as sources of electronic evidence from a procedural point of view, to differentiate their own legal regime from the regulation of the means of evidence provided in procedural laws. These are legal institutions that are born from the existence of technological security mechanisms and services related to entity authentication, the data origin, data integrity and in support of non-repudiation, with the aim that these technologies benefit from legal recognition, allowing their use to replace their paper-based correlates. For this reason, and to differentiate their use for other purposes, we refer to them, collectively, as accreditation institutions for electronic legal acts (Alamillo Domingo, Identificación, firma y otras pruebas electrónicas. La regulación jurídico-administrativa de la acreditación de las transacciones electrónicas, 2019a).

When we say that these institutions correspond to technical artefacts that constitute electronic evidence sources, we do so in the same sense that, in fact, it already happens with traditional "non-electronic" evidence sources. Indeed, the trace in which a handwritten signature consists is also a technical artefact (Fraenkel, 2008, p. 17), even though it is based on the technology of ink and paper, to which we are so accustomed, and which it has been clearly institutionalised in the legal world. Likewise, identity documents constitute physical artefacts with greater or lesser security measures, designed for personal exhibition in processes that require the determination of said identity.

However, attention needs to be drawn to two issues. First, the different purpose of the eIDAS Regulation in relation to the means of identification and the other sources of electronic evidence (Graux, 2011, pp. 21-22); while in the first case the object of the standard is limited to "the conditions under which Member States recognise electronic identification means […] falling under a notified electronic identification scheme of another Member State", in the second the object is "legal framework for "such electronic evidence, including electronic documents.

In both cases, in addition, Article 46 of the eIDAS Regulation strictly orders that "an electronic document shall not be denied legal effect and

[6] We use this expression following (Boer, 2009, p. 89).

admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form", a reference that clearly reinforces the purpose of the standard to support the electronic performance test, whose most recognised source and medium is precisely the document (Rodríguez Ayuso, 2018, pág. 80).

Second, numeral b) of Article 1 of the eIDAS Regulation refers to the establishment of "rules for trust services, in particular for electronic transactions", announcing the connection between the sources of electronic evidence – as well as their validity and effects– and the trust services that will support them, services that are provided by public and private sector entities without distinction, and in the latter case are characterised by being a commercial activity.

The eIDAS Regulation represents a more than notable milestone in this process of legal institutionalization of the mechanisms for the accreditation of electronic legal acts in which these sources of electronic evidence consist, and the services on which they are based; especially in view of the major objectives underlying its approval, which are to remove obstacles to the functioning of the internal market; strengthen trust and, finally, increase legal certainty (Gobert, 2015, p. 4).

In any case, the eIDAS Regulation uses the term "trust" profusely, but it does so in a very specific way, very focused on a category of electronically provided services that, in some way, offer trust to transactions, without addressing other dimensions of this phenomenon, widely analysed, especially from the sociology of risk and security (Pelletan, 2017).

In this part we introduce the main contents of the eIDAS Regulation that may be related to applications that make use of SSI technologies, including:

- The legal regime of electronic identification means.
- The legal regime of electronic signature and electronic seal.
- The legal regime of trust services for the transactions in the interior market.

4. THE LEGAL REGIME OF ELECTRONIC IDENTIFICATION MEANS FOR CROSS-BORDER TRANSACTIONS

The European Union regime of electronic identification is mainly contained in Chapter II of the eIDAS Regulation, further developed by the following implementing acts, setting rules regarding the electronic identification pan-European scheme:

- Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) Nº 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market ("IDAS Cooperation Decision").
- 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 of the European Parliament and of the Council on electronic identification and trust

services for electronic transactions in the internal market ("eIDAS Interoperability Regulation").

- 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 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market ("eIDAS Security Regulation").

- 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 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (notified under document C (2015) 7369) ("eIDAS Notification Decision").

The eIDAS Regulation considers that "citizens cannot use their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes in their country are not recognised in other Member States", and also that "mutually recognised electronic identification means will facilitate cross-border provision of numerous services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities" (Recital 9).

According to Recital 12 of eIDAS Regulation, "one of the objectives of this Regulation is to remove existing barriers to the cross-border use of electronic identification means used in the Member States to authenticate, for at least public services", while under Recital 17, "Member States should encourage the private sector to voluntarily use electronic identification means under a notified scheme for identification purposes when needed for online services or electronic transactions".

Under the eIDAS Regulation, thus, a mutual recognition system is created to allow citizens and business to identify themselves when accessing public services, and also private services if the Member State authorises this possibility.

4.1. Legal concept of electronic IDentification (eID)

According to Article 3 (1) of the eIDAS Regulation, electronic identification is defined as "the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person".

This definition is mainly intended to support the cross-border authentication when accessing public services. This definition is certainly scarce, for which we must turn to other definitions of the same legal text and rely on previously existing self-regulation and on the self-regulation of the public sector created

specifically for this institution, especially in the STORK projects and the CEF eID Community.

Article 3 (3) of the eIDAS Regulation defines person identification data as "a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established"; that is, a digital identifier, such as a name, one or two surnames, a registration number assigned by the Government (in the case of Spain, one of the most widely used – in physical identification, but not in remote electronic identification—, is the Document number National Identity). Given the existence of various sets of data that identify a person, and the difficulty of creating a unique identification aggregated with all possible identification data, we will refer generally to partial electronic identities.

Electronic identification is a process where we use identifiers of natural or legal persons, but we have not yet established what kind of process is or for what purpose, so we must continue to deepen the analysis of the eIDAS Regulation. Article 3 (4) of the eIDAS Regulation defines an electronic identification scheme as "a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons", while Article 3 (2) clarifies that electronic identification means are "a material and/or immaterial unit containing person identification data and which is used for authentication for an online service".

From these definitions, we can begin to better understanding the concept of electronic identification, since it is characterised by a regime that supports the process of electronic identification by issuing units that contain identification data and that serve for cross-border authentication. This is a legal abstraction that refers to a large number of potential technologies such as digital certificates in computer applications or cryptographic cards, physical or logical devices that generate unique authentication codes (such as single-use passwords), among many others.

This important amount of electronic identification means, which is available to the Member States, introduces an element of strong diversity between them, both in terms of security and interoperability, hindering or directly preventing cross-border operations.

It is also necessary to note that, according to Article 3 (5) of the eIDAS Regulation, authentication is defined as "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".

It is very remarkable the fact that this definition refers to three well-known security services: while entity authentication seems to be the main purpose of the authentication purpose, the legal definition also includes data source authentication and data integrity.

Entity authentication would therefore be the core innovation of the new regulation, since Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (eSign Directive, no longer in force) sufficiently covered data authentication as well as integrity, typical properties of electronic and advanced electronic signatures. In that sense, Article 2 (1) of the eSign Directive defined electronic signature as "`data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication`" (data origin authentication), while Article 2 (2) (d) of the same Directive required that an advanced electronic signature "`is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable`" (integrity property).

It has to be highlighted that the "authentication" definition contained in the eIDAS Regulation includes as well data source authentication and data integrity security services: if we compare this definition with that of an electronic seal contained in Article 3 (25) of the eIDAS Regulation itself, we will see that the seal also serves for exactly the same purpose of guaranteeing the origin of the data and the integrity of the same data. And that the advanced electronic seal, in addition, identifies its creator (see Articles 3 (26) and 36 (b) of the eIDAS Regulation).

It does not seem, however, that it is mandatory for a concrete electronic identification mean to support all these security services, in view of the use of the "or" conjunction used in the definition, so that there will be identification means that will allow only the authentication of entities –what is commonly perceived as "identification"–, while others may also offer the guarantee of data source authentication and even data integrity. This will be related to the technology used for the implementation of the authentication process: e.g. when using an authentication mechanism based in digital signature, the authentication information will be supporting entity authentication, but also data origin authentication and data integrity; on the contrary, using a password based mechanism, only entity authentication will be supported.

Entity authentication, data origin authentication and data integrity may also be provided by (advanced) electronic signatures for natural persons, and (advanced) electronic seals for legal persons. That means that, both in the case of advanced electronic signature and advanced electronic seal, we will find the possibility that some electronic identification systems offer exactly the same functionalities, as for example in the case of the use of digital signature based on a non-qualified certificate –where applicable, with the support of a cryptographic card– used as an electronic identification means. Indeed, it is clear that technologies such as the digital certificate-based signature can function indistinctly as an electronic identification means and as a trust service, so we should inquiry the reason why certain technology is designated as an electronic identification mean, a trust service (producing an electronic signature or electronic seal), or both at the same time; and the response can be found in the simple political will of each Member State, that in the exercise of its sovereignty may decide what such system legally is –by virtue of its recognition

as such– and even the legal effects that it wishes to give it. And if the only difference is compliance with the conditions of one or another legal regime, this implies that all qualified certificates issued in a Member State, regardless of the ownership of the service, public or private, are potential candidates to be recognised as electronic identification means by that State, and then notified, under the eIDAS Regulation.

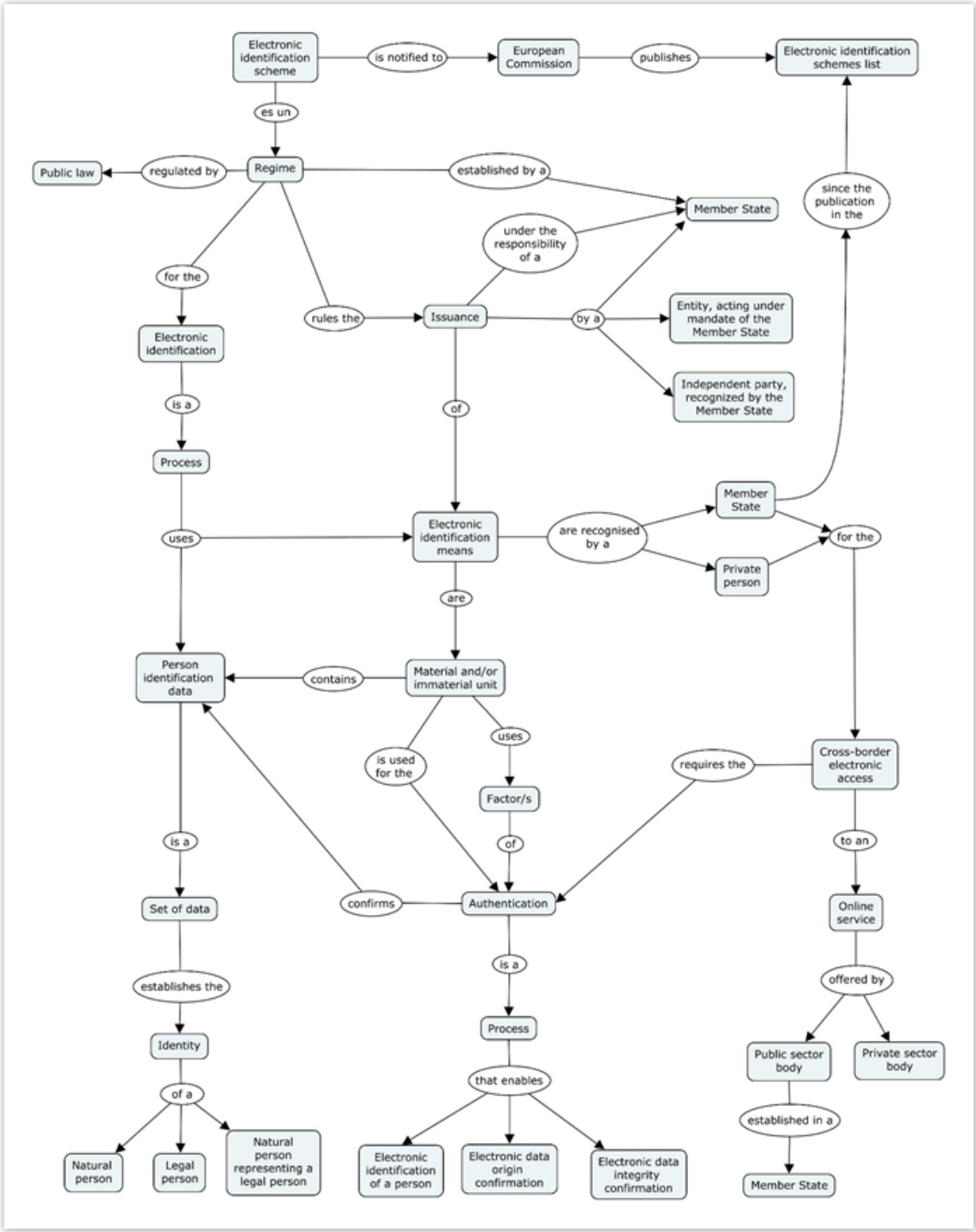

Figure 9. Electronic identification conceptual map (Alamillo Domingo, 2016)

4.2. The scope of the eIDAS Regulation and its relationship with national law

Having presented the concept of electronic identification in the eIDAS Regulation, it is convenient to delimit the scope of the mentioned Regulation, and its relation with the regulation in the national level.

The first thing to be said is that the eIDAS regulation is limited to establishing "the conditions under which Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State" as stipulated in Article 1 (a) thereof, conditions which strongly orbit around the issues of security and interoperability of systems and electronic identification systems and means.

In order for the juridical effect of cross-border recognition to take place with respect to electronic identification systems, three conditions must simultaneously concur, according to Article 6 (1) of the eIDAS Regulation:

- The electronic identification means must have been issued under an electronic identification scheme included in a list published by the Commission, in accordance with Article 9 of the eIDAS Regulation itself, for which purpose there must have been notified in advance by the Member State.

- The security level of this electronic identification means must correspond to a level of security equal to or higher than the level of security required by the public-sector body to access that online service in the first Member State, provided that the security level of the said electronic identification means corresponds to a substantial or high level of security.

- The public body in question must use a substantial or high level of security in relation to access to that online service, a provision which surprisingly precludes the possibility that a person with a better system than the requested by the public-sector body can actually use it, as for example will happen with a Spanish citizen who intends to use his electronic DNI to access a service in another Member State that only requires a low quality password, due to the low security sensitivity of the service.

The key fact is eIDAS Regulation is based on a pre-existing reality, which is the identification systems that Member States have in the past established for their citizens, mainly to facilitate access to public services, which were not covered by the electronic signature Directive. Similarly, Recital 12 of the eIDAS Regulation itself clarifies that "the aim of this Regulation is to ensure that for access to cross-border online services offered by Member States, secure electronic identification and authentication is possible" to facilitate the electronic development of the internal market, to comply with the legal requirements reflected in different legislative instruments, including Directive 2006/123/EC

of the European Parliament and of the Council of 12 December 2006 on Internal market and Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, both expressly mentioned in the eIDAS Regulation, and in other instruments of cross-border relationship between citizens and the public sector, such as certain cases in the field of electronic public procurement, electronic invoicing, corporate law or electronic tax management; or even for access to official personal data or for electronic voting.

Ultimately, the eIDAS Regulation is extremely respectful of the competences of the Member States in the area of electronic identification, limiting itself to establishing a framework for the mutual recognition of those systems and to legitimise the provision, by the European executive power, of a European public service. A sign of this respect is that the Regulation "does not aim to intervene with regard to electronic identity management systems and related infrastructures established in Member States" (Whereas 12), which therefore fall within the exclusive competence of the Member States; and that "Member States should remain free to use or to introduce means for the purposes of electronic identification for accessing online services [... and] to decide whether to involve the private sector in the provision of those means" (Recital 13), which again fall within the sphere of exclusive competence of each Member State of the Union.

Finally, Recital 13 of the eIDAS Regulation also states that "Member States should not be obliged to notify their electronic identification schemes to the Commission [...] the choice to notify the Commission of all, some or none of the electronic identification schemes used at national level to access at least public online services or specific services is up to Member States".

Thus, it is a regulation with a strong element of voluntary participation by Member States. We can therefore find a second element of diversity between the different Member States of the European Union, including Member States introducing electronic identification systems and notifying them for their cross-border use, against Member States that introduce these electronic identification systems only for internal use.

In fact, from the perspective of the eIDAS Regulation, we can see that electronic identification is a collection of electronic public services, unlike trusted services –which can be offered as public services o services of a commercial nature– that may be provided under direct or indirect management techniques, although it could also be a private service recognised by the Member State (cf. Article 7 (a) of the eIDAS Regulation), always under its liability according to Article 11 of the eIDAS Regulation.

As a result of this model, the eIDAS Regulation will not apply to electronic identification systems provided by public or private entities that have not been recognised by a Member State, which would be outside of its scope. This does not mean that an electronic identification means cannot be issued by the private

sector on its own, nor that it doesn't get any recognition, but that this activity is carried out in accordance with national law, or in a self-regulated manner, based on agreements between the parties.

In addition, the eIDAS Regulation does not really constitute the legal basis for the regulation of electronic identification systems, but only for their mutual recognition between the Member States of the European Union. Thus, this regulation will be found, where appropriate, in the national level. Certainly, the freedom that each Member State has to regulate its electronic identification system or systems is conditioned by the rules of the eIDAS Regulation, because compliance with them is a mandatory condition for mutual recognition, so that its effectiveness as a regulatory instrument it's undeniable. Finally, it should be noted that the analysis of the eIDAS Regulation clearly shows that its provisions only apply to online authentication, which would exclude face-to-face authentication, a fact which is relevant from the perspective of the free movement of persons physically travelling to the territory of another Member State. According to (Somorovsky & Mladenov, 2017, p. 32), "eIDAS is not a standalone Single-Sign-On solution but a compatibility layer between different eID integrations", which "does not perform the authentication itself and relies on the eID integration of the chosen target".

From the perspective of the substantive legal effects of the electronic identification systems to which we have just referred, the eIDAS Regulation focuses precisely on their mutual recognition within the territorial scope of application of the regulation, extending the right of use of such systems to the rest of the Member States of the European Union. This it is derived from Article 6 (1) of the eIDAS Regulation, when it states that "when an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that service online" provided that it meets the requirements and conditions laid down in the Regulation and the corresponding implementing acts, to which we will refer shortly.

This recognition does not occur immediately, but is deferred over time, and more specifically, within a maximum period of one year since the publication of a list of identification schemes by the European Commission.

On the other hand, Article 6 (2) of the eIDAS Regulation also determines that electronic identification systems that do not meet these requirements and conditions may also be subject to recognition by other Member States, albeit in a completely voluntary manner.

This legal effect of cross-border recognition of electronic identification is guaranteed only in relations between individuals and public sector bodies, which, in accordance with Article 3 (7) of the eIDAS Regulation, are defined as "a state, regional or local authority, a body governed by

public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate", in a clear example of the connection of this institution with the policies of the European Union regarding the use of electronic means in the field of Member States' Public Administration.

4.3. Eligibility criteria for the notification of electronic identification schemes

For an electronic identification scheme to be notified, it must meet a series of conditions (eligibility criteria), according to Article 7 of the eIDAS Regulation. Any new system (e.g. based on SSI technology), must comply with all the criteria, to be notified, as a previous step to receive the mutual recognition legal effect.

4.3.1. Electronic identification systems that may be subject to notification

Article 7 (a) of the eIDAS Regulation states that the means of electronic identification under the electronic identification system must have been issued, alternatively, by the notifying Member State, at the request of the Member State making the notification, or independently of the Member State making the notification and recognised by that Member State.

This is a sample of the public service nature of electronic administration that permeates the regulation of electronic identification in the eIDAS Regulation, and represents a new sample of potential diversity among the Member States of the European Union. The eIDAS Regulation provides for up to three possible legal regimes for electronic means of identification, subject to notification, which have in common the necessary prior intervention of the State concerned for its cross-border recognition.

The first possibility is to notify an electronic means of identification issued by the Member State itself; that is to say, of their ownership, as for example would happen with systems such as the Spanish electronic DNI, etc, while the second possibility concerns the notification of an electronic means of identification issued by an entity other than the notifying State, but under its mandate, in accordance with national law.

These two first cases of issuing electronic identification means would be assimilated to true public services, at least in its broader or imprecise notion, which identifies it with general administrative activity. From this perspective, the main difference between the two cases would be given by the management modality of public service, which would be direct in the first case and indirect in the second case, being applicable the legal procedures established for the management of public services, depending on the type of Administration that is the owner or principal of the service, as well as the corresponding rules for public procurement.

However, depending on the case, we can also consider the issuance of electronic identification means as a public service in the strict sense, by concurring with the conditions that the doctrine has been demanding for it, as evidenced in cases such as the Spanish DNI-e or the German nPA, the issuance of which are reserved to the State. This consideration, referring to the identification means, is compatible with the broad notion of electronic public service on the globally considered identification system, which allows the coexistence of these monopolistic means with other private means.

Finally, the third possibility is based on the legal act of prior recognition by the State of an electronic identification system different from the previous ones –issued independently of the State–, a category where we can include electronic identification systems operated by private entities, including financial entities, operators of electronic communications services, or providers of information society services, such as service portals Internet, or social networking, among many others.

This third case is more complex, because the State is not the owner of the public service, nor is it provided under its mandate, in a scenario where the State could simply be just a consumer of the electronic identification means issued by private companies. Let us imagine, for example, that a State decides to acquire the right to use the electronic identification means supplied to citizens by a private entity so that they can access public services, instead of directly issuing them. It would not be appropriate if these means could not also be used for access to the public services of third-country bodies. Thus, this third case departs from the concept of public service and operates as a mechanism for extending the service acquired by State to the private sector, vis-à-vis third States.

It is also in this third possibility that we can find the most innovative and possibly most appropriate solutions considering the nature of the Internet network, strongly marked by the intervention of multiple intermediaries, and, therefore, it could become a new element of strong diversity among Member States of the Union.

This act of recognition of privately issued electronic identification means –that extends is usage to other Member States– is subject to national law and is not without major legal challenges. Firstly, to the extent that the act of recognition has the legal effect of enabling the electronic identification means for use in cross-border authentication, the way in which it is exercised will have clear effects on the market.

One possibility would be for the State to recognise all private providers who meet the conditions for this, although we could also find quantitative limits on the electronic identification means issued by private providers, forming a kind of virtual electronic public service. In this case, the effects on free competition arising from, for example, recognising a single private provider (or a small group of providers) should be carefully considered, since it could have a distorting effect on competition, granting these providers a competitive

advantage that would foster the use of the same system in private transactions, probably under a fee.

Given that, as we have seen, electronic identification systems can be used perfectly for the accreditation of identity in electronic business processes –and, depending on the technology on which it is based, also for integrity and data origin authentication– they are functionally equivalent to electronic signature or electronic seal based in trust services, we must assume that the possibility of their use by private parties –for a price– can act as a limiting factor to the development of the trust services market. We therefore consider that the Member State which avails itself of this option must be diligent in selecting the identity providers it recognises, guaranteeing reasonable conditions in relation to this activity.

And secondly, we must ask ourselves about the selection of the electronic identification system to be used, which we believe should be fully governed by national law and, more specifically, assuming that the provision of the service is not free for the Administration, by the rules of public procurement, currently contained Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (and its national implementations, of course), adopting the procedure that is most appropriate depending on the organisation of the service.

Although it is certainly not possible to rule out the possibility that the private provider of the electronic identification system does not charge any amount to the State that uses it, this possibility seems rather remote, given the obvious costs that this use may entail. Therefore, we would be faced with a potential service contract, if the Administration acquires the electronic identification system for itself (and possibly for private third parties), although it will also be possible to consider the possibility of an innovation partnership agreement.

Therefore, and in summary, the electronic identification system is, in any case, overall configured as a public service, regardless of the consideration of the issuance of electronic identification means within that same system, also as a public service, as a virtual public service or as a private service.

4.3.2. The use of electronic identification means for access to electronic public services in the issuing Member State

Article 7 (b) of the eIDAS Regulation requires that "`the electronic identification means under the electronic identification scheme can be used to access at least one service which is provided by a public-sector body and which requires electronic identification in the notifying Member State`".

It is a requirement that connects, as we have previously seen, the instrumental nature of electronic identification with respect to access to public services, and its main legal consequence is to prevent the notification of systems that are not used for this purpose.

This provision can be understood as reasonable since, as we have seen, notification of an electronic identification system has the effect of imposing an obligation on the other Member States of the European Union to allow the use of such a system for cross-border access to their own systems of electronic administration. It would logically prove absurd that an electronic identification system issued in one Member State which cannot be used in that Member State for access to eGovernment services could instead be used in the other Member States (especially in terms of liability).

This requirement may be an issue for the recognition of an SSI system, because it means that at least one EU government should previously accept the derived identity for an electronic government service in its jurisdiction.

4.3.3. The alignment of the scheme and the electronic identification means with a predetermined level of assurance

Article 7 (c) of the eIDAS Regulation requires that "the electronic identification scheme and the electronic identification means issued thereunder meet the requirements of at least one of the assurance levels set out in the implementing act referred to in Article 8 (3)" of the regulation itself, so that those who do not meet those requirements would be excluded from this possibility of mutual recognition.

The difference between the system and the identification means brings into account the type of security measures to be considered, some of which fall under the management of the system, with a more intense approach to procedures, and others in the electronic identification means, with greater focus and detail in the corresponding technologies. In any case, the recognition obligation only affects the electronic identification systems of level of assurance substantial or high, whereas, in the case of level of assurance low systems, such recognition is optional and, therefore, it will depend on the agreements to which the Member States may come with other Member States.

For the eIDAS Regulation, "the security of electronic identification schemes is key to trustworthy cross-border mutual recognition of electronic identification means" (Whereas 19), and thus, assurance levels must be defined to "characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned" (Whereas 16).

The eIDAS Regulation approach assumes the existence of diverse electronic identification means, offering different assurance levels, depending "on the degree of confidence that electronic identification means provides in claimed or asserted identity of a person taking into account processes (for example, identity proofing and verification, and authentication), management activities (for example, the entity issuing electronic identification

means and the procedure to issue such means) and technical controls implemented". Thus, "the requirements established should be technology-neutral" and "it should be possible to achieve the necessary security requirements through different technologies" (Whereas 16).

The notion of security level of electronic identification systems is, of course, not original to the eIDAS Regulation, but rather has been received by it, from the pre-existing reality, as have shown by (Graux & Majava, 2007), (Eertink, Hulsebosch, & Lenzini, 2008) or (Atzeni & Lioy, 2011), including the *Signposts* document (European Commission, 2005, p. 32), i2010 eGovernment Action Plan - Accelerating eGovernment in Europe for the Benefit of All (COM (2006) 173 final) and the Roadmap for a pan-European eIDM Framework by 2010 (European Commission. Information Society and Media Directorate-General. eGovernment Unit, 2006, p. 14), developing the aforementioned Action plan, or the IDA[7] and IDABC[8] initiatives.

The IDA authentication policy, based on the authentication policies previously existing in the Member States (mainly based on PKI), is particularly relevant for the evaluation and establishment, by the managers of sectoral networks and horizontal projects related to the security, of appropriate authentication mechanisms for their projects.

This authentication policy already defined four levels of security, three of which are nominally very similar to those defined in the eIDAS Regulation, and was subsequently taken as a starting point for subsequent work within the IDABC program and, more specifically, for the eID Interoperability for PEGS project (interoperability of electronic identity for pan-European eGovernment services).

This project was born with the objective of analysing the interoperability requirements of digital identity and authentication arising from the pilots of pan-European electronic Administration services, and also provides a characterization of security levels, considering the levels previously defined in the IDA's authentication policy, as well as other relevant experiences, notably the NIST Guidelines referring to the e-Authentication project of the US Federal Government, and policies of Member states such as France, Norway, the United Kingdom and Germany.

In both frameworks, the approach that supports the definition of authentication assurance levels is the same, and is based on the severity of the impact of the damages that could occur in the event of a threat to the misuse or

[7] Decision No 1720/1999/EC of the European Parliament and of the Council of 12 July 1999 adopting a series of actions and measures in order to ensure interoperability of and access to trans-European networks for the electronic interchange of data between administrations (IDA).

[8] Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC).

misappropriation of the identity of a person, an approach that, in light of Recital (16) of the eIDAS Regulation, has been embraced by legislation.

Thus, in the proposal for an IDABC multi-level authentication mechanism, the authentication assurance is based on an acceptable level of trust in an alleged real-world identity and in an electronic identity presented to a service provider using a credential (Graux & Majava, 2007, pág. 20). More specifically, the IDABC proposal defines a complete set of threats to authentication, which if occurring –with greater or lesser probability– could cause damage with a certain degree of severity.

The notion is that, the greater the probability and the greater the impact (more serious damage), the greater the risk associated with a specific threat is, so that the service provider can assess whether it is necessary to be more or less demanding in respect to the accreditation of the identity required.

		Impact of damages				
	Likelihood	Very High	High	Medium	Low	Negligible
Risk i	Almost certain	(1)	(1)	Level 4	Level 3	Level 3
	Likely	(1)	Level 4	Level 3	Level 3	Level 2
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1
(1): Not applicable to remote authentication over open networks.						

Figure 10. Risk matrix considered in IDABC

For example, if in the event of identity theft of a citizen there is a low impact regarding the confidentiality of her personal data (for example, because the service does not contain sensitive data) and the probability that such impersonation may occur is moderate, it will be enough to use an authentication mechanism that that offers a level 2 or low assurance. However, if the damage caused was high (because the data is sensitive), then it would be necessary to increase the level of required assurance to level 3 or substantial.

From the indicated IDABC works, we must refer to the STORK project, where there is an important advance in terms of the definition of authentication assurance levels, from the real pilots being carried out, establishing an approach based on the quality of different authentication solutions, so that each level of assurance describes the degree to which a party to an electronic transaction can trust that the identity information presented to it by an identity provider actually represents to the entity referred to therein (Eertink, Hulsebosch, & Lenzini, 2008, pág. 55).

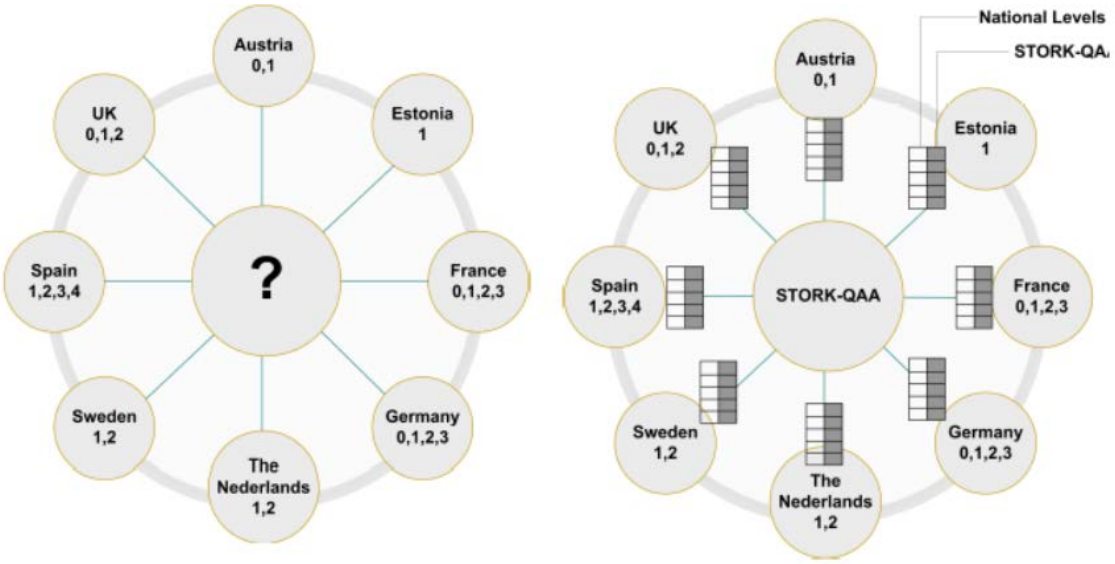

Figure 11. The need to define common authentication assurance levels in STORK

STORK's levels of assurance are defined in the Authentication Quality Assurance (QAA) framework, which is used to establish a mapping between the level of security of Member States' electronic identification systems between them. The levels are defined based on the requirements (typically, of a service) referring to the identity of a user (Hulsebosch, Lenzini, & Eertink, 2009, pág. 7), and thus, STORK does not address other forms of authentication incorporated to the definition of the eIDAS Regulation (such as data origin authentication), focusing on entity authentication (identification in strict sense).

For example, if in Spain it is considered necessary –for example, in application of the criteria contained in the ENS, the national security regulation for electronic administration procedures, due to the sensitivity of information– to demand a high level of access control, we should be able to determine which electronic authentication systems meet the requirements of the ENS in this regard. Instead of comparing the high level requirements of the ENS with all the electronic identification systems issued in the other Member States of the Union, something that is highly unfeasible, what will be done is comparing the requirements of this high level of the ENS with the requirements of the STORK QAA to select the applicable STORK level; from there, as any electronic identification system issued in another Member State is classified in one of the STORK QAA levels, we can recognise it as equivalent to the corresponding level of the ENS.

Furthermore, the STORK QAA levels are defined in terms of sets of requirements on relevant authentication factors, and each requirement defines the functional and technical properties to be satisfied by that authentication factor.

These factors are divided into organisational type factors, referred to the identity registration phase, including the quality levels of the identification procedure (ID), the quality of the credential issuance process (IC), and the quality of the issuing entity (IE); and of a technical nature, referring to the electronic

authentication phase, including the quality levels of the type and robustness of the issued credential (RC) and quality of security of the authentication mechanism (AM), as shown in (Hulsebosch, Lenzini, & Eertink, 2009, pág. 12):

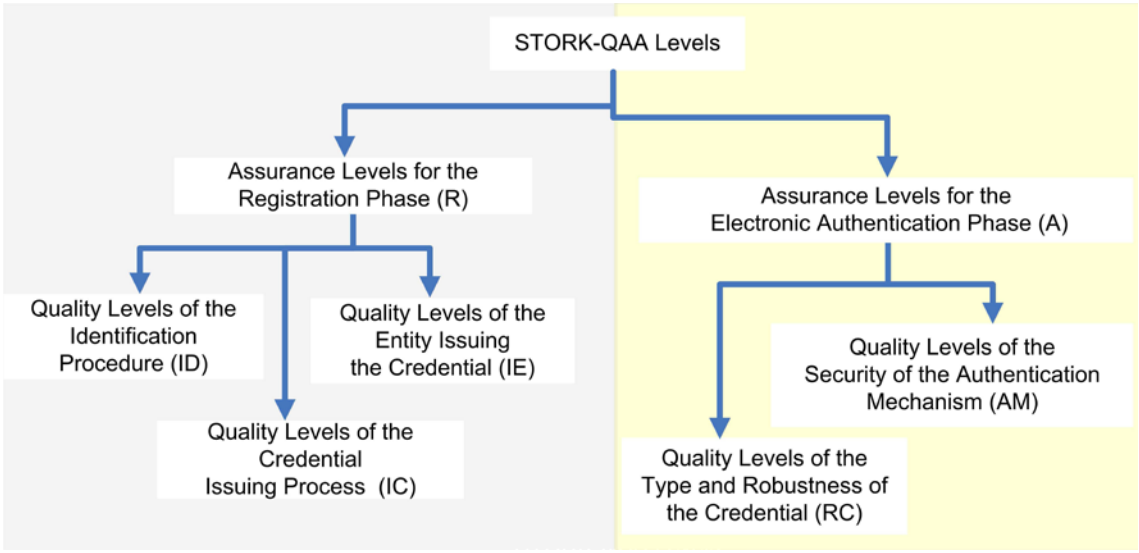

Figure 12. Relevant factors for QAA levels in STORK

The idea is that the minimum quality of an identification system corresponds to the minimum level that each of these five factors reaches, so the STORK approach is abstract, allowing the inclusion in it of the specific solutions existing in the Member States and their translation at the levels required for accessing services in the other Member States, as can be seen in the Figure:

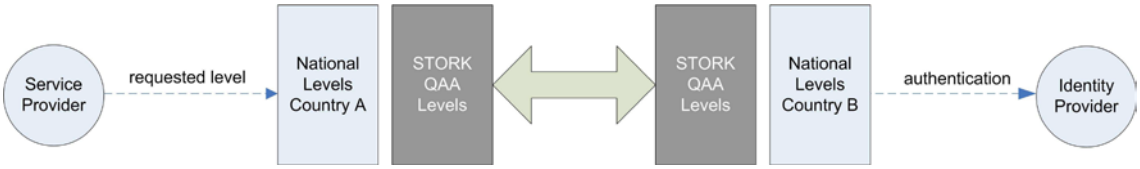

Figure 13. Authentication assurance levels mapping in STORK

Following the same example, Spain uses a three-level security scheme for authentication, so level 1 systems in Spain map against STORK levels 1 and 2; those of level 2 in Spain, against level 3 of STORK; and finally, those of level 3 in Spain, against level 4 of STORK. In an access to Austria, for example, where level 1 is required at the Austrian national level, since it maps against STORK level 4, level 3 of Spain will be required.

It is not surprising, therefore, that Recital (16) of the eIDAS Regulation expressly recognises that "various technical definitions and descriptions of assurance levels exist as the result of Union-funded Large-Scale Pilots, standardization and international activities", to add that "in particular, the Large-Scale Pilot STORK and ISO 29115 refer, inter alia, to levels 2, 3 and 4, which should be taken into utmost account in establishing minimum technical requirements, standards and procedures for the assurances levels low, substantial and high within the meaning of this Regulation,

while ensuring consistent application of this Regulation in particular with regard to assurance level high related to identity proofing for issuing qualified certificates", a reference that has the effect of conditioning the subsequent application of the Regulation, which must be aligned with said referents.

Assurance levels are described in Article 8 (2) of Regulation eIDAS, as a number of -high-level and somewhat abstract- criteria that support a particular degree of confidence in the electronic identification means issued to the person, while reducing or avoiding the risk of misuse or undue alteration of identity.

Notwithstanding the analysis of the elements referred to each of the levels of assurance, it is necessary to remember that these levels differ according to the risk of use of the electronic identification in a specific service; that is, depending on the probability of occurrence of a threat, with a qualitatively or quantitatively determinable harmful impact.

The levels of assurance must be specified later, as provided in section 3 of Article 8 itself, in the following terms: "by 18 September 2015, taking into account relevant international standards and subject to paragraph 2, the Commission shall, by means of implementing acts, set out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified for electronic identification means for the purposes of paragraph 1".

In this way, the European legislator seeks the cooperation of the EU Commission for the practical implementation of the aforementioned levels of security, using the indirect referral technique, and which is substantiated by an implementing act thunder the examination procedure. However, the European legislator lays down essential content for these minimum technical specifications, standards and procedures, which, according to the second paragraph of Article 8 (3) of the eIDAS Regulation "shall be set out by reference to the reliability and quality of the following elements:

(a) the procedure to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means;

(b) the procedure for the issuance of the requested electronic identification means;

(c) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party;

(d) the entity issuing the electronic identification means;

(e) any other body involved in the application for the issuance of the electronic identification means; and

(f) the technical and security specifications of the issued electronic identification means".

This implementing act is 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 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS Security Regulation).

According to Recital (2) of the eIDAS Security Regulation, "determining the minimum technical specifications, standards and procedures is essential in order to ensure common understanding of the details of the assurance levels and to ensure interoperability when mapping the national assurance levels of notified electronic identification schemes against the assurance levels under Article 8 as provided by Article 12 (4) (b) of Regulation (EU) Nº 910/2014".

Thus, its purpose is twofold: on the one hand, to detail the criteria for the levels of security to obtain a common understanding of them; on the other, to facilitate the mapping between the levels of the Member State systems with the levels defined in the eIDAS Regulation.

It is interesting to note, first, that the eIDAS Security Regulation considers what is established in the international standard ISO/IEC 29115:2013, although it does not refer to any specific content of the same, because it "differs from that international standard, in particular in relation to identity proofing and verification requirements, as well as to the way in which the differences between Member State identity arrangements and the existing tools in the EU for the same purpose are taken into account" in accordance with its Recital (3). In addition, the eIDAS Security Regulation also considers the results of the STORK project, as mentioned in its Recital (4).

Secondly, according to Article 1(2) of the eIDAS Security Regulation, "the specifications and procedures set out in the Annex shall be used to specify the assurance level of the electronic identification means issued under a notified electronic identification scheme by determining the reliability and quality of following elements:

(a) enrolment, as set out in section 2.1 of the Annex to this Regulation pursuant to Article 8 (3) (a) of Regulation (EU) Nº 910/2014;

(b) electronic identification means management, as set out in section 2.2 of the Annex to this Regulation pursuant to Article 8 (3) (b) and (f) of Regulation (EU) Nº 910/2014;

(c) authentication, as set out in section 2.3 of the Annex to this Regulation pursuant to Article 8 (3) (c) of Regulation (EU) Nº 910/2014;

(d) management and organisation, as set out in section 2.4 of the Annex to this Regulation pursuant to Article 8 (3) (d) and (e) of Regulation (EU) Nº 910/2014".

The notion is that the Regulation we are examining will determine, for each of these elements, one or more specifications and/or procedures, which will help Member States to rely on the electronic identification means.

First, section 2.1 of the Annex to the eIDAS Security Regulation refers to the registration in the electronic identification system, in relation to which it determines criteria for the application and registration; the proof and verification of the identity (of natural person, of juridical person); and the link between the means of electronic identification of physical and legal persons. This section contains the appropriate controls for the registration of a new user in an electronic identification system, often also called "registration phase", as in the STORK QAA framework.

Secondly, section 2.2 of the Annex to the eIDAS Security Regulation refers to the management of electronic identification means, establishing criteria referring to the characteristics and design of electronic identification means; to the expedition, delivery and activation thereof; suspension, revocation and reactivation thereof; and to the renewal and replacement of these same means. In this case, an approach to management processes organised around the life cycle of the means of electronic identification, or credentials, is adopted, which will require corresponding adaptations to each technology.

Thirdly, section 2.3 of the Annex to the eIDAS Security Regulation refers to authentication, in relation to which essentially establishes requirements related to the authentication mechanism, through which the natural or legal person uses the means of electronic identification for Confirm its identity to the user side. That is, in this phase is where the person uses his credential to claim his identity to the service he intends to access, using the corresponding technical protocol, so it should be noted that this process only allows to rely on the identification data of the person, and does not assert anything about the suitability of such data for the purposes of the service to which the person us granted access.

Finally, section 2.4 of the Annex to the eIDAS Security Regulation concerns the management and organisation of participants providing a service related to electronic identification in a cross-border context, including certain general provisions; publication of notices and user information; information security management; preservation of information; facilities and staff; technical controls; and compliance and audits.

The detailed requirements for each of this section might be consulted in the eIDAS Security Regulation itself. It is also worthwhile to mention that the

eIDAS Cooperation Network has issued a specific Guidance for the application of the levels of assurance which support the eIDAS Regulation[9].

4.3.4. The exclusive attribution of the electronic identification data and means

As a specification of the alignment requirement with a predetermined level of security, Article 7 (d) and (e) of the eIDAS Regulation require the guarantee of exclusive attribution of electronic identification data and means to the person concerned. In the first case, it is required that "the notifying Member State ensures that the person identification data uniquely representing the person in question is attributed, in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3), to the natural or legal person referred to in point 1 of Article 3 at the time the electronic identification means under that scheme is issued".

We can recall the identification data are those that allow the identification of the person, such as in the case of an electronic certificate, or an identity card contained in a database.

This guarantee must be offered in the terms of the implementing act that defines the levels of security, which we will present later, and must be offered at the moment in which the means of identification are issued; it is a requirement of what is known as the user "registration", and it is very significant that this obligation is imposed on the State –and with the corresponding liability– and not on the entity that issues the electronic identification means, something that accounts for the fundamental importance of digital identity.

In the second case, though, it is required that "the party issuing the electronic identification means under that scheme ensures that the electronic identification means is attributed to the person referred to in point (d) of this Article in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8 (3)" of eIDAS Regulation. In this case, it is the party that issues the electronic identification means who must offer this guarantee –and assume the corresponding liability– something that is understandable given that it is the entity that takes charge of the operation of the system, having to do it with the minimum mandatory security measures.

The identification data are defined in the 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 of the European Parliament and of the Council on electronic identification and trust services for

[9] Available at https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Guidance+documents.

electronic transactions in the internal market (the eIDAS Interoperability Regulation). This is known as the Minimum Data Set (MDS).

In this sense, Article 11 of the eIDAS Interoperability Regulation authorises the use of various attributes for the representation, in an electronic identification means used in a cross-border context, of the identity of a natural or legal person (section 1), or of a natural person who represents a legal person (section 2), specifying that data shall be transmitted based on original characters and, where appropriate, also transliterated into Latin characters (section 3).

The purpose of this rule is to agree on the minimum mandatory contents to be used for the description of a natural or legal person, in a cross-border context. Given that the different identity numbers or codes assigned by the authorities of the Member States –which will be employed by the identity providers of those Member States– may be incomprehensible to service providers in other Member States, or that there may be legal issues for the cross-border use of an identity code, as they are of exclusive use within the Member State, it is necessary to establish rules for the assignment of specific identifiers for cross-border authentication, or for the use of previous identifiers for cross-border transactions. I.e., in Germany it is not allowed to use the national identification number outside Germany, and thus it is necessary to assign a new identifier.

In this sense, section 1 of the annex to the eIDAS Interoperability Regulation imposes the obligation to use the following attributes for the identification of a natural person: a) surname or current surnames; b) current name or names; c) the date of birth and d) a unique identifier drawn up by the issuing Member State in accordance with the technical specifications for cross-border identification purposes and as constant as possible over time.

Likewise, the following additional attributes are authorised: a) name or names and surname or surname of birth; b) place of birth; c) current address and d) sex; being understood that whenever the necessary prior consent is available, except in those cases where the legislation excludes it.

Technical specifications have been established in the STORK projects and then in the CEF eID, for cross-border identification, based on a set of principles that seek to reconcile the different legal sensitivities of Member States with regard to the use of identifiers.

4.3.5. The availability of an online authentication mechanism

Article 7 (f) of the eIDAS Regulation requires that "`the notifying Member State ensures the availability of authentication online, so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form`" when the said person needs access to a service offered online by that party.

In our opinion, this obligation is essential for the operation of the electronic identification system, since the relying against which the person is to be identified needs to be able to verify that the person is who she claims to be,

according to the technological system used, and therefore is imposed on the corresponding identity provider, to which the State must transfer this legal obligation.

However, the obligation under this heading should also be understood as referring to the need for the State to establish and guarantee the overall operation of the electronic identification system, as well as one or more nodes of the interoperability architecture for electronic identification, all subject to an electronic public service regime reserved to the competent public authority in each Member State.

Again, this is an electronic public service, with a marked instrumental nature, facilitating the provision of other finalist public services or the performance of electronic administrative procedures, especially from the perspective of relationship with the citizen; but also in support of the realisation of private sector transaction, and thus it can eventually overcome the wards of so-called e-Government, affecting market development.

The relying party must access this process of cross-border authentication online, and therefore, if it is not available, access to the service offered by the relying party is simply interrupted. Consequently, it is configured as a mandatory service and, as we have seen, is regulated by public law, regardless of the ownership of the electronic identification device issued –and the corresponding authentication process–, or also the ownership of the service which is accessed through the aforementioned authentication.

According to the second paragraph of this paragraph (f), the cross-border authentication shall be provided free of charge when it is carried out in relation to a service online provided by a public sector body, a requirement which is aptly intended to avoid the complex and problematic Invoicing for the consumption of the service between the different Member States of the European Union, and from which we can also infer to the contrary that a fee for the use of this service may be established in other cases –as in the same paragraph is to be understood when it states that for relying parties other than public sector bodies the notifying Member State may define terms of access to that authentication.

That the process of cross-border authentication is free when used for access to electronic public services implies, on the other hand, that the use of the electronic identification means for such authentication must also be free; that is to say, both the use of the electronic identification means (such as the electronic National ID, or a qualified certificate, or a password) and the technical platform implementing the authentication process must be free of charge, regardless of the ownership of the electronic identification means. Thus, in case the identification means is offered by a private company, free usage will be a condition required for recognition. This condition may make commercially uninteresting for private providers offering the service to its customers, at least for the cross-border authentication when accessing public services.

Finally, in order to maximise the potential use of electronic identification means in cross-border online authentication, the second paragraph of this numeral requires that "Member States shall not impose any specific disproportionate technical requirements on relying parties intending to carry out such authentication, where such requirements prevent or significantly impede the interoperability of the notified electronic identification schemes".

This provision refers to the relying parties in the system, which will be, mainly, public sector bodies of the Member States other than the one in whose territory the electronic identification means has been issued, but in the end, it protects the citizens having the aforementioned means, who are interested in being able to authenticate themselves to e-government or other services on the territory of another Member State.

What is to be considered as a disproportionate technical requirement, and under what circumstances does it prevent or significantly impede interoperability, is a factual issue to be resolved on a case-by-case basis, but imposition of software installation or use by the citizens are a good candidate. We are referring to additional technical conditions different from those which form part of the interoperability framework provided for in the Regulation itself, even if formally compatible with it. It is true that the very existence of the eIDAS interoperability framework, and its subsequent application by the Member States, can provide elements that help to objectify these circumstances, reinforcing their relevance as a public soft law instrument.

4.3.6. The need for prior cooperation

Article 7 (g) of the eIDAS Regulation requires the Member State aiming to notify the European Commission of an electronic identification system to send to the other Member States a description of the system at least six months prior to such notification (pre-notification procedure).

The purpose of this action is to inform the other Member States of the European Union about the system envisaged to be notified, for the purposes of cooperation between them, as provided for in the Regulation, which is aimed at the interoperability and security of the identification system subject to notification; and to facilitate the peer review process of the pre-notified system.

The eIDAS Regulation does not precisely define the content of this description of the system, but we can understand that it will be the same description provided for in Article 9 (1) (a) thereof, as part of the contents of the notification to be sent to the European Commission.

This is clear from Article 13 of Commission Implementing Decision (EU) 2015/296 of 24 February 2015, which obliges the Member State to send to the Cooperation Network the draft notification form with the contents provided for in Article 9 (1) (a) of the eIDAS Regulation.

The eIDAS Cooperation Network has published specific guidance on the pre-notification form[10].

4.3.7. The guarantee of interoperability of electronic identification means

Finally, Article 7 (h) of the eIDAS Regulation requires that, in order to be notified, an electronic identification system must comply with the provisions of the interoperability framework provided for in Article 12 (8) thereof, approved by the aforementioned eIDAS Interoperability Regulation.

Interoperability is one of the key elements of the regulatory approach to electronic identification, and in this sense it is reflected in article 12 (1) of the eIDAS Regulation, which determines that "the national electronic identification schemes notified pursuant to Article 9 (1) shall be interoperable" with each other, an obligation in relation to which in section 2 of article 12 it is foreseen that "an interoperability framework shall be established" (for electronic identification).

The interoperability framework for electronic identification, of a sectoral nature, must meet, under section 3 of article 12 of the eIDAS Regulation, the following criteria: "(a) it aims to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State; (b) it follows European and international standards, where possible; (c) it facilitates the implementation of the principle of privacy by design; and (d) it ensures that personal data is processed in accordance with Directive 95/46/EC".

The first criterion of the interoperability framework refers to its necessary technological neutrality, so that it does not prevent the use of the various technical solutions for electronic identification that are applied in the Member States, both with respect to the existing means of identification and the authentication processes in which they are used.

Therefore, the interoperability framework should not force the Member State to modify its domestic technological options –allowing the citizen to continue using the identification system that it already has– but it should limit itself to the adoption of the technology strictly necessary to extend the use of this system to cross-border transaction, and always with the minimum restrictions on the citizen, particularly in respect to the need to use software applications[11]. Note,

[10] Available at https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Guidance+documents.

[11] Recital (3) of the eIDAS Interoperability Regulation indicates that "where a Member State or the Commission provides software to enable authentication to a node operated in another Member State, the party which supplies and updates the software used for the authentication mechanism may agree with the party which hosts the software how the operation for the authentication mechanism will be managed. Such an agreement should not impose disproportionate technical requirements or costs (including support, responsibilities, hosting and other costs) on the

however, that this is an informative criterion, and that it refers only to the fact that the system aspires to be neutral, without being legally required in any case, more a guideline than a true legal rule.

The second criterion looks after basing the interoperability framework, to the extent possible, on international and European standards[12], instead of being created *ad hoc*, an approach that also facilitates interoperability, given that there is a technological heritage created and adopted by the industry that can be reused, reducing costs and implementation times.

The third criterion aims to promote that the interoperability framework applies the important principle of "privacy by design", in line with GDPR, by virtue of which, and especially in this case, "`the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed`" (article 25(2)), in spite of other measures.

Finally, the fourth criterion comes to require that personal data be treated in accordance with regulatory regulations. We would not be in this case before a principle, but before a true legal obligation, also included in article 5 of the eIDAS Regulation, which orders that "`processing of personal data shall be carried out in accordance with Directive 95/46/EC`", a reference that, at present, must be made to GDPR, regardless of the corresponding legislation approved at the national level.

These two obligations denote the enormous importance of the protection of personal data in electronic identification, especially given its structure in a network of nodes[13]. Indeed, if a network of unique points is installed (in each State) through which all cross-border authentications by the Administration are mediated, the risk of monitoring the activity, interests, etc., of citizens and the creation of behavioural profiles is evident, by requiring the registration of metadata about the operations[14] or the inspection of the operational messaging,

---

`hosting party`"; probably in a reference to the middleware and intermediary software initially created in the framework of the STORK projects and, after maintained in the CEF eID community.

[12] The eID component is based on internationally accepted standards such as SAML, which, however, does not enjoy the legal consideration of an international or European technical standard, but rather a technical specification for ICTs, because it has not been approved by an international standardization body, nor by a European standardization organisation (cf. Regulation (EU) No. 1025/2012).

[13] Indeed, the electronic identification interoperability architecture is a good example of a control architecture to which it refers (Moles Plaza, 2004), which could allow the State to obtain valuable personal information from citizens.

[14] For example, imagine that the operator of this infrastructure records the authentications of the users in order to determine their options for political participation, using the metadata of the platforms they access.

a risk that may be unacceptable from a social point of view[15], especially in light of the debates raised in the thread of different surveillance programs –secret and without judicial control– of citizens by some governments. To reduce this risk, an electronic identification interoperability framework should take the most restrictive approach possible with regard to the processing of personal data.

Likewise, this interoperability framework will consist in the following, according to section 4 of Article 12 of the eIDAS Regulation: "(a) a reference to minimum technical requirements related to the assurance levels under Article 8; (b) a mapping of national assurance levels of notified electronic identification schemes to the assurance levels under Article 8; (c) a reference to minimum technical requirements for interoperability; (d) a reference to a minimum set of person identification data uniquely representing a natural or legal person, which is available from electronic identification schemes; (e) rules of procedure; (f) arrangements for dispute resolution; and (g) common operational security standards".

Article 1 of the eIDAS Interoperability Regulation states that "this Regulation lays down technical and operational requirements of the interoperability framework in order to ensure the interoperability of the electronic identification schemes which Member States notify to the Commission", adopting a technologically neutral approach that allows new technical systems to be adopted in the future.

With respect to the objective scope, Article 2 (1) of the eIDAS Interoperability Regulation defines a node as "a connection point which is part of the electronic identification interoperability architecture and is involved in cross-border authentication of persons and which has the capability to recognise and process or forward transmissions to other nodes by enabling the national electronic identification infrastructure of one Member State to interface with national electronic identification infrastructures of other Member States"; from a subjective perspective, Article 2 (2) of the eIDAS interoperability Regulation defines a node operator as "the entity responsible for ensuring that the node performs correctly and reliably its functions as a connection point". These definitions are provided to the end of establishing the corresponding interoperability obligations for and between them.

This node usually corresponds to one of the main components of the system that facilitates cross-border authentication, which in the case of STORK is the Pan European Proxy Server or PEPS, partially adopted as an eID component of the

[15] In this sense, the analysis of (Martin, van Brakel, & Bernhard, 2009, p. 217) regarding the national identity system of the United Kingdom is very illustrative.

Connecting Europe Facility, but it may also be implemented as a middleware, without a central authority acting as a delegated authentication IdP.

Entering the normative content of the eIDAS Interoperability Regulation, firstly, two references to the security levels of electronic identification means are contained. The first of these appears in Article 3, which establishes that "minimum technical requirements related to the assurance levels shall be as set out in Commission Implementing Regulation (EU) 2015/1502" (the eIDAS Security Regulation), in a purported development of the provision contained in Article 12 (4) (a) of the eIDAS Regulation, according to which the interoperability framework must contain "a reference to minimum technical requirements related to the assurance levels under Article 8"; development that is not going to be carried out in this Regulation but in that of security measures, something that is certainly criticisable in terms of legislative technique.

Secondly, and also in relation to security, Article 4 of the eIDAS Interoperability Regulation establishes that "the mapping of national assurance levels of the notified electronic identification schemes shall follow the requirements laid down in Implementing Regulation (EU) 2015/1502" (the eIDAS Security Regulation), provision that supposedly complies with the requirement contained in Article 14 (2) (b) of the eIDAS Regulation, under which the interoperability framework must contain "a mapping of national assurance levels of notified electronic identification schemes to the assurance levels under Article 8"; that is, a correlation between the security level of a system in the notifying Member State and the eIDAS Regulation.

As can be seen, Article 4 of the eIDAS Interoperability Regulation once again refers this question entirely to what is determined in the eIDAS Security Regulation.

The second sentence of Article 4 of the eIDAS Interoperability Regulation is of greater interest, which provides that "the results of the mapping shall be notified to the Commission using the notification template laid down in Commission Implementing Decision (EU) 2015/1984". This Decision, which regulates the trusted lists that we will analyse in greater detail later, establishes in its Annex II a form for the notification of the information on the body responsible for the establishment, maintenance and publication of the national trusted lists, and the details relating to the place where said lists are published, the certificates used to sign or seal the trust lists and any modification thereof (Article 4 (1) of the Decision, which complies with Article 22 (3) of the eIDAS Regulation).

This notification is used, in the trust services regulation, for the publication, by the Commission, of a compiled list with the previous information, so that it is easy to locate the list of trust services of a specific supervisor. But its use for reporting the mapping of security levels of electronic identification systems is quite difficult to understand, unless the will of the European executive has been

to establish that the results of this correlation are, in effect, contained in a trusted list, but exclusively related to identification systems.

If this is the case the content of said trust list should be adapted, based on the European standards in the matter, since the content provided in Annex I of the eIDAS Trusted Lists Decision is not appropriate for this mapping, since there is no syntax or semantics to represent the "result of" the aforementioned correlation. The opposite case would be even worse, since it would force defining the document with the mapping from scratch, and in a misaligned way of the trusted lists, something that would make this approach even more difficult to understand.

Nor does the rule clarify who should make this mapping, or notify it to the European Commission, but it can be imagined that it will be the notifying Member State, in accordance with the provisions of Articles 7 and 9 of the eIDAS Regulation, and the analysis that the eIDAS Cooperation Decision previously carried out. This has been the adopted practice.

Secondly, the eIDAS Interoperability Regulation dedicates two articles to establishing minimum technical requirements for interoperability, taking this notion in a strict sense, which refer to the nodes of the electronic identification interoperability architecture and the format of the messages for the communication.

Regarding the nodes, Article 5 of the eIDAS Interoperability Regulation limits itself to stating that the nodes in one Member State shall be able to connect with nodes of other Member States (section 1); that the nodes shall be able to distinguish between public sector bodies and other relying parties through technical means (section 2); and that a Member State implementation of the technical requirements set out in the Regulation shall not impose disproportionate technical requirements and costs on other Member States in order for them to interoperate with the implementation adopted by the first Member State (section 3), a rule we have previously referred to.

It is an extremely sparse regulation, which of course only facilitates interoperability from a very high-level perspective, so its concretion must take place through subsequent technical specifications.

For its part, in relation to the format of messages for communication –that is, for communication between nodes for the purposes of cross-border authentication–, Article 8 of the eIDAS Interoperability Regulation requires that "`the nodes shall use for syntax common message formats based on standards that have already been deployed more than once between Member States and proven to work in an operational environment`", a rule that lead almost inexorably, in my opinion, to the exclusive adoption of the results of STORK/CEF eID specifications as the interoperability framework, and the need that, for its replacement by another framework, it must first be implemented and tested repeatedly and successfully in various Member States.

In any case, the eIDAS Interoperability Regulation establishes rules referring to the syntax to be used, in the sense that it "shall allow: (a) proper processing of the minimum set of person identification data uniquely representing a natural or legal person; (b) proper processing of the assurance level of the electronic identification means; (c) distinction between public sector bodies and other relying parties; (d) flexibility to meet the needs of additional attributes relating to identification", requirements that again strongly refer to the technical, syntactic and semantic protocol basis of STORK/CEF eID, which is SAML 2.0, but that can be perfectly projected to any other technical system, notably those known as self-sovereign or self-managed identity systems that make use of distributed ledger technology-based systems.

Third, the eIDAS Interoperability Regulation determines the minimum set of person identification data uniquely representing a natural or legal person. In this sense, its Article 11 authorises the use of various attributes for this representation, when used for the authentication in a cross-border context to act on her own behalf (section 1), or when a natural person acts on behalf of a legal person (section 2), specifying that "data shall be transmitted based on original characters and, where appropriate, also transliterated into Latin characters" (section 3).

The purpose of this rule is to agree on the mandatory minimum content to be used to describe a natural or legal person, in the cross-border authentication context. Given that the different numbers or identity codes assigned by the authorities of the Member States –which will be used by the identity providers of those States– may be incomprehensible to service providers in other Member States, or there may be legal barriers for the cross-border use of an identity code, as it is for exclusive use within the Member State, it is necessary to establish rules for assigning specific identifiers for cross-border authentication, or for using pre-existing identifiers in cross-border transactions.

In this sense, section 1 of the annex to the eIDAS Interoperability Regulation imposes the obligation to use the following attributes to identify a natural person: (a) current family name(s); (b) current first name(s); (c) date of birth; (d) a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time.

Likewise, the use of the following additional attributes is authorised: (a) first name(s) and family name(s) at birth; (b) place of birth; (c) current address; (d) gender; as long as the necessary prior consent is obtained, except in those cases where the regulations exempt it.

For its part, section 2 of the annex to the eIDAS Interoperability Regulation imposes the obligation to use at least the following attributes for the identification of a legal person (a) current legal name; (b) a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time.

Likewise, the use of the following additional attributes is authorised, as appropriate: (a) current address; (b) VAT registration number; (c) tax reference number; (d) the identifier related to Article 3(1) of Directive 2009/101/EC of the European Parliament and of the Council; (e) Legal Entity Identifier (LEI) referred to in Commission Implementing Regulation (EU) No 1247/2012; (f) Economic Operator Registration and Identification (EORI) referred to in Commission Implementing Regulation (EU) No 1352/2013; (g) excise number provided in Article 2(12) of Council Regulation (EC) No 389/2012.

It may be striking that, for both individuals and legal entities, a need to use a unique identifier is foreseen, which must be in accordance with the technical specifications for cross-border identification purposes, with the remaining personal identifiers being optional, depending on the needs and, especially, on the applicable legal context. Likewise, this identifier should be as constant as possible over time, which facilitates multiple cross-border operations, but will also allow a greater degree of potential citizen traceability.

Fourth, the eIDAS Interoperability Regulation establishes common operational security standards, referring to data privacy and confidentiality; to the integrity and authenticity of the data for communication between the nodes; to the management of metadata and security information; and, finally, to information security and security standards; while, fifthly, the eIDAS Interoperability Regulation contains provisions for the settlement of disputes.

Thus, and this is really relevant in the context of this study, Articles 12 and 13 (2) of the eIDAS Interoperability Regulation set out the main governance rules:

- Where it is justified by the process of implementation of the interoperability framework, the Cooperation Network established by Implementing Decision (EU) 2015/296 may adopt opinions pursuant to Article 14 (d) thereof on the need to develop technical specifications.

- Pursuant to the opinion referred to in paragraph 1 the Commission in cooperation with Member States shall develop the technical specifications as part of the digital service infrastructures of Regulation (EU) No 1316/2013.

- The Cooperation Network shall adopt an opinion pursuant to Article 14 (d) of Implementing Decision (EU) 2015/296 in which it evaluates whether and to what extent the technical specifications developed under paragraph 2 correspond to the need identified in the opinion referred to in paragraph 1 or the requirements set in this Regulation. It may recommend that Member States take the technical specifications into account when implementing the interoperability framework.

- The Commission shall provide a reference implementation as an example interpretation of the technical specifications. Member States may apply this reference implementation or use it as a sample when testing other implementations of the technical specifications.

- In case of any dispute concerning the interoperability framework than cannot be resolved by the concerned Member States through negotiation, the Cooperation Network established in accordance with Article 12 of Implementing Decision (EU) 2015/296 shall have competence in the dispute in accordance with its rules of procedure

4.4. The legal effect of notified electronic identification means

4.4.1. The main legal effect: cross-border recognition by public sector bodies

From the perspective of the substantive legal effects of electronic identification systems[16], the eIDAS Regulation focuses precisely on their mutual recognition within the territorial scope of application of the standard, so that the right to use these systems is extended to the rest of States of the European Union. This is derived from article 6.1 of the eIDAS Regulation, when it establishes that "when an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State" that meets the requirements and conditions provided for in the Regulation, and the corresponding implementing acts, "shall be recognised in the first Member State for the purposes of cross-border authentication for that service online".

This recognition does not occur immediately, but is deferred over time, and more specifically, within a maximum period of one year[17] from the publication of the list of identification systems by the European Commission[18].

For its part, Article 6 (2) of the Regulations also determines that electronic identification systems that do not meet these requirements and conditions may also be recognised by other States, although on a fully voluntary basis.

This legal effect of cross-border recognition of electronic identification is guaranteed only in relationships between individuals and public sector bodies (Dumortier, 2016, p. 11), which according to Article 3(7) of the eIDAS Regulation, are defined as "state, regional or local authority, a

[16] Although our interest is focused on the legal dimension of these media, their relevance is greater, since electronic identification is considered one of the fundamental elements of "digital sovereignty", which can be defined as "having complete knowledge and individual control or about who can access what data and where such data is transferred" (Posch, 2017, p. 77), who believes that electronic identification should be the basis for remote access to data in the Cloud.

[17] Nothing, of course, prevents the aforementioned recognition from occurring previously, which will depend on technological, budgetary or simply political factors.

[18] For systems notified before the first publication of the list of identification systems, as provided for in article 9.2 of the eIDAS Regulation, given that the systems subsequently notified will be published within two months after notification, as provided in section 3 of the same article.

body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate"; in an evident sample of the connection of this institution with the policies of the European Union in the electronic administration strategies of the Member States.

Secondly, it is necessary to point out the possibility that national law may establish its own substantive, additional, legal effects in relation to one or more electronic identification systems. And among these effects it is perfectly possible to declare the equivalence of an electronic identification system with a written signature. Although it is not an optimal possibility, since it would collide with the signature or qualified electronic seal regulation, it cannot be dismissed. It will happen, however, that this legal effect of equivalence will not enjoy cross-border recognition, unlike the institution of the qualified electronic signature provided for in the eIDAS Regulation; thus, probably this type of means of identification will be subject to both regulations.

As just indicated, for this legal effect of cross-border recognition to occur with respect to electronic identification systems, the three conditions legally provided for in article 6 (1) of the eIDAS Regulation must concur simultaneously.

First, the electronic identification means must have been issued under an electronic identification system included in a list published by the Commission, in accordance with the provisions of Article 9 of the eIDAS Regulation, for which it must have been previously notified by the Member State.

Secondly, the level of security of this electronic identification means must correspond to a level of security equal to or greater than the level of security required by the public sector body to access said online service in the first Member State, provided that the security level of said electronic identification means corresponds to a substantial or high level of security.

Third, the public body in question must require a substantial or high level of security in relation to access to this online service, a provision that surprisingly excludes the possibility that a person with a better than required system can use it For example, it could happen with a Belgian citizen who intends to use her electronic ID to access a service in another Member State that only requires a password (even a low quality one), due to the low sensitivity of the service.

This is a restriction contrary to logic –it seems that the principle that "who can do more, can do less" should apply– and that it can only be understood, in my opinion, from a budgetary point of view; that is, in order not to compel that Member State to incorporate any cross-border authentication to that service, but it certainly will be something to be decided by each Member State according to its public procedure legislation.

In any case, other legal instruments at the EU level will concrete specific uses of electronic identification means in cases where it may not be clear the application of public procedural law. This is the case with Article 13b of Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law, added by Directive (EU) 2019/1151 of the European Parliament and of the Council of 20 June 2019 amending Directive (EU) 2017/1132 as regards the use of digital tools and processes in company law (not yet in force), ordering that "Member States shall ensure that the following electronic identification means can be used by applicants who are Union citizens in the online procedures referred to in this Chapter: (a) an electronic identification means issued under an electronic identification scheme approved by their own Member State; (b) an electronic identification means issued in another Member State and recognised for the purpose of cross-border authentication in accordance with Article 6 of Regulation (EU) No 910/2014".

Nonetheless, under section 4 of Article 13b, "where justified by reason of the public interest in preventing identity misuse or alteration, Member States may, for the purposes of verifying an applicant's identity, take measures which could require the physical presence of that applicant before any authority or person or body mandated under national law to deal with any aspect of the online procedures referred to in this Chapter, including the drawing up of the instrument of constitution of a company". To avoid this provision deactivates in practice the possibility of online procedures, the same article adds that "Member States shall ensure that the physical presence of an applicant may only be required on a case-by-case basis where there are reasons to suspect identity falsification, and that any other steps of the procedure can be completed online".

4.4.2. A secondary legal effect: the use of electronic identification systems for legal-private transactions

Although its main objective is to facilitate cross-border access to public services, the truth is that the eIDAS Regulation also encourages the use of electronic identification systems by private users, for cross-border authentication operations in access to its services; that is, for authentication in front of companies and other private organisations, with respect to transactions under private law.

In this sense, Recital 17 of the eIDAS Regulation says that "Member States should encourage the private sector to voluntarily use electronic identification means under a notified scheme for identification purposes when needed for online services or electronic transactions", because "the possibility to use such electronic identification means would enable the private sector to rely on electronic identification and authentication already largely used in many Member States

at least for public services and to make it easier for businesses and citizens to access their online services across borders".

In effect, having access to a large number of people already identified with strong legal procedures would facilitate the transactions of private user parties, who are certainly increasingly subject to greater identification requirements with respect to their customers, especially depending on the sector. Therefore, it is increasingly important to be able to determine the real identity of the people they engage with, without incurring in excessive costs, especially the greater the geographical distance between the parties is.

Some examples of this possibility have already been identified in EU legislation and other EU legal instruments:

- Article 24 (1) (b) of the eIDAS Regulation authorises qualified trust service providers, when issuing a qualified certificate, "to verify the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued […] remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'". This provision in currently in force, since the eIDAS Regulation for trust services entered into application 1 July 2016.

- Article 13 (1) (a) of the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, modified by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018, orders that "customer due diligence measures shall comprise: […] identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities"[19]. This provision

[19] A good national example implementing this possibility can be found in Article 19 (1) of *Decreto legislativo 21 novembre 2007, n. 231, Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo*

must be considered currently in force, since the deadline for the transposition of the Directive was 10 January 2020.

- Article 5 (1) (a) of Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market, expressly authorises the possibility of using an electronic identification means to verify the state of residence of a subscriber to an online content service, at the time of the conclusion or renewal of the contract (provided that the said electronic identification means offers such information which is optional, or if it is used in combination with an additional mechanism such as an internet protocol (IP) address check, to identify the Member State where the subscriber accesses the online content service). This provision in currently in force, since the Regulation entered into application 1 April 2018.

We can also cite non-legislative instruments, such as Commission Recommendation 2014/478/EU of 14 July 2014 on principles for the protection of consumers and players of online gambling services and for the prevention of minors from gambling online, whose number 20, following the request made by the European Parliament, by means of Resolution of 10 September 2013 on online gambling in the internal market, to introduce mandatory third-party identification controls, encourages Member States to adopt electronic identification systems in the registration process.

As can be easily verified, in all these cases the use of some of the electronic identification systems offered or recognised by the Member States under the eIDAS Regulation would be consistent, at least in the case of systems with a level of assurance substantial or high.

The key point is that Recital 17 of the eIDAS Regulation says that "in order to facilitate the use of such electronic identification means across borders by the private sector, the authentication possibility provided by any Member State should be available to private sector relying parties established outside of the territory of that Member State under the same conditions as applied to private sector relying parties established within that Member State"; that

del sistema finanziario a scopo di riciclaggio dei proventi di attivita' criminose e di finanziamento del terrorismo nonche' della direttiva 2006/70/CE che ne reca misure di esecuzione (modified by Article 2 of *Decreto legislativo 25 maggio 2017, n. 90, Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attivita' criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006*), authorises the use of identification systems without personal physical presence, including qualified certificates, provided that they comply with national regulations –contained in Article 64 of *Decreto legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale*–, o that have been notified under Article 9 of the eIDAS Regulation with level of assurance high, or when the certificate corresponds to a digital signature associated to an electronic document, according to Article 24 of the *Codice dell'amministrazione digitale*.

is, "with regard to private sector relying parties, the notifying Member State may define terms of access to the authentication means", including to "inform whether the authentication means related to the notified scheme is presently available to private sector relying parties".

As we have seen previously, article 7 (f) of the eIDAS Regulation establishes that "for relying parties other than public sector bodies the notifying Member State may define terms of access to that authentication", a provision that refers, as we already know, to the use of the infrastructure provided by the State to enable the authentication process; including the electronic identification interoperability nodes, or the direct access to the eID in the middleware approach.

In this sense, we must ask ourselves what kind of conditions can be established by the Member State, given that they must be in accordance with the reporting principles of Union law. And, in this sense, it must be understood that any condition to be established must be, at least, objective, reasonable and non-discriminatory, including, where so decided, any cost[20].

For the application of this specific conditions, there may be the need to identify this type of relying parties, so that the specific conditions of access can be applied[21].

5. THE LEGAL REGIME OF ELECTRONIC SIGNATURES AND ELECTRONIC SEALS

5.1. Electronic signatures and seals

The eIDAS Regulation, as previously done by the DFE, legally institutionalises the electronic signature, in a concept that the eIDAS Regulation exclusively reserves for the performance of legal acts by individuals, as well as the electronic seal, intended for legal entities.

Article 3 (10) of the eIDAS Regulation defines the electronic signature as "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", in a definition which is slightly different from that originally contained in the eSign Directive, reinforcing the finalist approach of the definition, since the important thing will be that the aforementioned data is used precisely for this intention of signing, while in the previous regulation the functional aspect of the signature as an data origin authentication system was emphasised.

[20] (Brugger, et al., 2014) have analysed this issue with respect to the STORK project.

[21] Cf. https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Terms+of+access+to+notified+eID+schemes+for+non-public+sector+-+Identification+of+relying+parties.

In effect, according to article 2 (1) of the eSign Directive, the electronic signature was defined as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication", a kind of credential that electronically supported identification and authentication (Alonso Ureba & Alcover Garau, 2000, p. 192). It should be noted that only the authentication technologies that referred to electronic data (Martínez Nadal, 2009, págs. 73-74) constituted an electronic signature, and only these, not paper data (Illescas Ortíz, 2001, pág. 91), nor those that only referred to the authentication of entities (COM (2010) 120 final, page 4).

This definition of the signature in the eSign Directive corresponds, in general terms, with the most basic function that can be preached from a written signature, which is simply to indicate to whom a communication or a document authenticated by it can be attributed.

However, the new definition seems to disregard the requirement of identification/authentication. Obviously, it is necessary to be able to effectively identify the signatory, before or after the production of a signature, in order to benefit from its evidentiary value (Merchán Murillo, 2016, pág. 32).

At least in a superficial reading, it is a definition that seems to implicitly require using some type of key to sign, something that is not especially neutral in technological terms, and that is somewhat strange when certain technologies are used, such as the electronically captured handwritten signature, in which there is no key to use. In this case, the data in electronic format that the signer uses to sign include those that represent the dynamics of the handwritten signature (a modality of behaviour-based biometry), such as speed, pressure, or inclination. These data constitute an electronic signature only when they are used by the signer to sign, and not in other cases.

On the other hand, regarding what the expression “to sign” means (Fraenkel, 1992, p. 7), it is a question that must be analysed under national law, since the eIDAS Regulation says nothing about it (Dumortier & Vandezande, 2012a, p. 5) (Dumortier & Vandezande, 2012a, p. 5).

In this sense, it is clear that the handwritten signature fulfils various typical social functions (Chou, 2015, p. 84), which have normally been legally

institutionalised by legislation[22] or jurisprudence[23], so any technology that allows such compliance should be considered as an electronic signature, in spite of the convenience of slightly modifying the definition of this institution in the sense of making it more neutral, for example, in line in English law.

From this point of view, it happens that, as we have already seen when analysing the concept of electronic signature in the eSign Directive, one of the functions of the electronic signature may be simply the attribution of the message to an identified person, but without her making of any declaration of will –this would happen, for example, with the signing of a postcard sent to a relative–; while another socially typical function will be the provision of contractual consent, for which specific conditions will be required (Couto Calviño, 2007, págs. 7-8).

Any of the typical social functions of the handwritten signature only make sense in relation to a written document (Fraenkel, 2008, p. 23) –in particular, the most legally important typical social function occurs when the document incorporates a declaration of will or another, which produces legal effect–, so any electronic signature must also be projected on a durable electronic medium that incorporates said writing.

Likewise, it must be remembered that, even if the most important typical social function of the signature (handwritten and, therefore, electronic) is to link a declaration to a person, normally for the purposes of the declaration of will, there is no obligation to put the signature on any medium (paper or another durable medium, including an electronic one) that contains a private-legal regime (a clause) binding for the parties, since there are indeed cases in which a simple durable medium will be enough, without having to incorporate any signature (Madrid Parra, 2001, págs. 187-188).

This will be, therefore, a matter that will remain in the scope of the formal requirements imposed by national law, as confirmed by the CJEU in its Judgment of November 9, 2006, issued in case C -42/15, Home Credit Slovakia, in which it states that "Article 10 (1) and (2) of Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC, read in conjunction with Article 3(m), thereof, must be interpreted as meaning that: […] – it does

[22] For example, article 1316-4 of the French Civil Code, incorporated by article 4 of *Loi No. 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique* –currently, article 1367 of the French Civil Code, after the reform carried out by article 4 of the *Ordonnance nº 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations*–, says that the signature necessary for the perfection of a legal act identifies its author, and who expresses his consent to the obligations derived from said act. Therefore, in French law a technology that does not guarantee these two properties simply cannot be considered as an electronic signature for the purposes of the perfection of legal acts, although it certainly could be for other purposes. Additionally, said norm (also maintained after the aforementioned Civil Code reform) indicates that when the signature is electronic, it consists of a reliable identification process that guarantees its connection with the act to which it is attached.

[23] This would be the case in Spain, according to the Judgment of the Supreme Court of November 3, 1997 (Anguiano Jiménez, 2015).

not preclude a Member State from providing in its national legislation, first, that a credit agreement falling within the scope of Directive 2008/48 which is drawn up on paper must be signed by the parties and, second, that the requirement that the agreement be signed applies to all the details of that agreement referred to in Article 10(2) of that directive".

Therefore, in the absence of a formal requirement, the use of an electronic signature of any kind will simply not be required (De Miguel Asensio, 2015, pág. 1000), without prejudice that the parties may decide to use it or replace it with another source of evidence electronic, such as an electronic record of the performance generated by an intervening third party, as an "airplane black box" (Dumortier, 2004, p. 281).

As a relevant novelty in relation to the eSign Directive, article 3 (25) of the eIDAS Regulation defines the electronic seal as "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". The usefulness of the seal is given by these two elements, which refer to the computer security services of data origin authentication and data integrity.

This is a mechanism that is somewhat similar to the electronic signature, but for use by legal entities (Muñoz Soro, 2003, pág. 134), as deduced from Recital 59 of the eIDAS Regulation, which indicates that "electronic seals should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity"; while, according to Recital 65, "in addition to authenticating the document issued by the legal person, electronic seals can be used to authenticate any digital asset of the legal person, such as software code or servers".

While, in the case of electronic signature, the signatory is "a natural person who creates an electronic signature" (Article 3 (9)) of the eIDAS Regulation), in the case of the electronic seal, the creator of the seal is "a legal person who creates an electronic seal" (Article 3 (24)) of the eIDAS Regulation).

As can be seen, a very relevant difference between the two concepts is that the electronic signature is built in relation to the written signature, so it should be possible to use an electronic signature where the legislation refers to a written signature –so the electronic signature is considered equivalent to the written signature–,in the case of the electronic seal, this approach is not applied; rather, the eIDAS Regulation defines what the seal is for, instead of referring to the use of the "physical seal", and which use is regulated in a number of cases.

5.2. Advanced electronic signatures and seals

Article 3 (11) of the eIDAS Regulation defines an advanced electronic signature as "an electronic signature which meets the requirements set out in Article 26"; that is, "(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".

As can be seen from its definition, the advanced electronic signature is technically ideal to fulfil the typical social purpose of the written signature previously explained, including the identification of the signatory as the author of the document, the will to be bound and the link with the text contained in the document, usually based on the use of certain technologies.

Article 3 (26) of the eIDAS Regulation defines an advanced electronic seal as "an electronic seal, which meets the requirements set out in Article 36"; that is, "(a) it is uniquely linked to the creator of the seal; (b) it is capable of identifying the creator of the seal; (c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and (d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable".

As can be seen from both definitions, the creation of the advanced electronic signature and seal requires the use of creation data, which must be subject to a different degree of control by the owner, since the relationship of the signature or seal with its holder depends on it (Mason, 2017, p. 152). Electronic signature creation data is, according to Article 3 (13) of the eIDAS Regulation, "unique data which is used by the signatory to create an electronic signature". The eIDAS Regulation also refers to the electronic seal creation data as "unique data, which is used by the creator of the electronic seal to create an electronic seal", in its Article 3 (28).

In both cases, it is the most critical aspect of the system, since the unauthorised possession or access to the signature creation data allows to impersonate the signatory or the seal creator, respectively; a reason for which the signature or seal creation data must be able to be protected against misuse by third parties, something that had traditionally been interpreted as meaning the exclusive possession of a private key only by the signatory, although the eIDAS Regulation considers a broader approach to adapt to new technological options, even authorizing the management, by third parties – significantly, by qualified trust service providers–, of the creation data, under certain conditions, provided that they are under the sole control of the signatory. On the other hand, the data for the creation of the advanced electronic seal must be under the control of the legal entity, but it does not have to be a sole control, showing one of the main differences between both institutions.

In this sense, it is also necessary to clarify that the creation of the advanced electronic signature or seal occurs using a device. It is defined in Article 3 (22) of the eIDAS Regulation as "configured software or hardware used

to create an electronic signature", while Article 3 (31) of the eIDAS Regulation defines the electronic seal creation device as "configured software or hardware used to create an electronic seal".

These definitions connect the creation of the electronic signature or seal with the application (that is, with the use) of the signature or seal creation data, so that the possessor of the device is really the person who really controls the process of creating the signature or the seal, whether or not it is the subscriber of the corresponding certificate.

For this reason, the signature or seal will be attributed to the signer or creator of the seal if an unauthorised person cannot use the corresponding creation data, which justifies the need to have control over the use of signature or seal activation data, something is provided for in the definition of an advanced electronic signature or seal, with the difference that this control must be exclusive in the case of electronic signature, and not in the case of the electronic seal.

It is also necessary to refer to Article 3 (40) of the eIDAS Regulation, which refers to the electronic signature or seal validation data, which defines as "data that is used to validate an electronic signature or an electronic seal" (by third-party recipients communications and signed documents), instead of "verification", which was the term used by Annex IV of the eSign Directive, a change that has no practical effect, but that in both cases points to the use of asymmetric key technologies, such as digital signatures.

This second definition of electronic signature and seal, incremental in requirements over the more general one of simple electronic signature and seal, requires a technology that allows identifying and attributing data to the person who uses the mechanisms to produce the signature or seal, and unlike the handwritten signature, the technology appropriate to create an advanced electronic signature or seal must guarantee the integrity of the document, so that subsequent modifications thereof are detectable.

Again, it is an orientation that aims to be neutral from a technical perspective, allowing various technologies to receive the legal status of advanced electronic signature and seal, despite the fact that it seems that the European legislator regulates with a certain technology in mind (COM (2006) 120 final, p. 4), which is none other than digital signature based on asymmetric key cryptography based on electronic certificate; that is, the so-called PKI or public key infrastructure. In this sense, neutrality is more oriented to the different digital signature technologies than to other different technologies, an opinion not shared by (Sorge, 2014, p. 135).

Indeed, is quite evident the equivalence between the private key (technical concept) and the signature or seal creation data (legal concept), as well as between the public key (technical concept) and the signature or seal validation data (legal concept), supporting the equivalence between the digital signature (technical concept) and the advanced electronic signature or the advanced

electronic seal (legal concept), although this requires the use of a certain technical syntax.

In any case, and at least from a purely theoretical perspective, the advanced electronic signature and seal can, however, correspond to a digital signature, or not, and in the first case, be based on a certificate, or not, without This affects its legal value, but whenever a technology is used that allows compliance with all the requirements of the signature or advanced electronic seal, something that is not always easy.

5.3. Qualified electronic signatures and seals

Finally, article 3 (12) of the eIDAS Regulation contains a third definition of an electronic signature, which it calls qualified, and which it conceptualises as "an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures".

It is, again, an incremental definition of requirements, which incorporates two additional elements to the advanced electronic signature –the qualified electronic signature creation device and the qualified electronic signature certificate, to which we will refer later in detail– in order to guarantee that the qualified electronic signature technology produces its typical effect; that is, it is suitable for a natural person to identify herself and sign.

Note that both the signing device and the signing certificate must be qualified, as a measure of prior control that guarantees their suitability and, therefore, that the electronic signature is indeed qualified.

In this way, the concept of qualified electronic signature will serve to denote a subset of electronic signature technologies as a legal institution, to which specific legal effects will be associated, "providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union", in words of Recital (2) of the eIDAS Regulation.

From this legal conceptualization, it is possible to criticise that the qualification must necessarily refer to these two elements –qualified certificate and qualified creation device–, because it supposes a technological commitment that violates the principle of technological neutrality; on the contrary, qualification should be abstract, as happens in most trust services, because otherwise innovation is discriminated,.

For its part, and again in a clear analogy with the qualified electronic signature, Article 3 (27) of the eIDAS Regulation defines the qualified electronic seal as "an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal"; again,

the considerations made in relation to the qualified electronic signature are applicable, but for use by legal entities.

As we have advanced, one of the elements required to obtain a qualified electronic signature or seal –which as we have already seen is directly equivalent to the written signature of the natural person, or directly attributable to the legal person that generates it, respectively– is the qualified device for creating said signature or seal.

This qualified device is defined in Article 3 (23) of the eIDAS Regulation, with respect to a qualified electronic signature, as "an electronic signature creation device that meets the requirements laid down in Annex II", while Article 3 (32) of the same Regulation, in respect to qualified electronic seal, defines it as a "an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II". Obviously reiteratively, Article 29 (1) of the eIDAS Regulation provides that "qualified electronic signature creation devices shall meet the requirements laid down in Annex II", provision applicable mutatis mutandis to qualified electronic seal creation devices pursuant to the provisions of article 39 (1) of the same Regulation.

In this sense, regarding qualified electronic signature devices, Recital (56) of the eIDAS Regulation indicates that "this Regulation should lay down requirements for qualified electronic signature creation devices to ensure the functionality of advanced electronic signatures", giving a good account of the purpose and orientation of said requirements.

Annex II of the eIDAS Regulation, applicable to both qualified signature creation devices and qualified seal creation devices, is the one that really establishes the requirements that these products must meet, which largely refer to the creation data signature or seal, in various relevant provisions.

First, section 1 (a) of Annex II of the eIDAS Regulation requires that "the confidentiality of the electronic signature [or seal] creation data used for electronic signature [or seal] creation is reasonably assured", a completely logical requirement, since if this signature or seal creation data is known by third parties, then said third parties can use them to produce signatures or seals instead of the legitimate parties.

Second, Annex II of the eIDAS Regulation determines in its section 1 (b) that qualified devices must guarantee that "the electronic signature [or seal] creation data used for electronic signature [or seal] creation can practically occur only once", recognizing the impossibility of offering this guarantee in an absolute way; indeed, the guarantee of uniqueness of the creation data can be obtained as randomly as possible using very large numerical spaces, but even in this case it is difficult to ensure that said data is unique, especially when different providers generate creation data using various mechanisms.

Third, Annex II of the eIDAS Regulation determines in its section 1 (c) that qualified devices must guarantee that "the electronic signature [or seal] creation data used for electronic signature [or seal] creation cannot, with reasonable assurance, be derived and the electronic signature [or seal] is reliably protected against forgery using currently available technology", in an implicit reference to the properties of cryptographic algorithms used in support of qualified electronic signatures and seals.

Fourth, an explicit reference to the protection of creation data is contained in Annex II of the eIDAS Regulation when its section 1 (d) provides that these devices must guarantee that "the electronic signature creation data used for electronic signature [or seal] creation can be reliably protected by the legitimate signatory [or seal creator] against use by others".

As a novelty in relation to the eSign Directive, the eIDAS Regulation regulates, in the case of a qualified electronic signature and seal, the possibility that a qualified provider of trust services can generate and manage signature or seal creation data on behalf of the signatory or seal creator, respectively.

In relation to qualified devices for creating a signature or seal, the eIDAS Regulation has meant a radical change of orientation with respect to the eSign Directive, since its article 30 (1) establishes that "conformity of qualified electronic signature creation devices with the requirements laid down in Annex II shall be certified by appropriate public or private bodies designated by Member States", making this certification, which was understood as optional, mandatory.

It is a rule that must be directly related to Article 29 (2) of the eIDAS Regulation, which indicates that "the Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices", with the legal effect that "compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards"; acts that "shall be adopted in accordance with the examination procedure referred to in Article 48 (2)"; and Article which is also applicable to qualified devices for creating a seal by virtue of the provisions of Article 39 (1) of the eIDAS Regulation.

The legal consequence of this modification is that, from July 1, 2016, the start date of application of article 30 (1), a device cannot be marketed as qualified without prior certification; which, as indicated in section (3) of article 30 of the eIDAS Regulation, "shall be based on one of the following: (a) a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in the list established in accordance with the second subparagraph; or (b) a process other than the process referred to in point

(a), provided that it uses comparable security levels and provided that the public or private body referred to in paragraph 1 notifies that process to the Commission. That process may be used only in the absence of standards referred to in point (a) or when a security evaluation process referred to in point (a) is ongoing", provision that is completed with the mandate that "the Commission shall, by means of implementing acts, establish a list of standards for the security assessment of information technology products referred to in point (a). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48 (2)".

This article offers two options: a stricter one, which is the preferable one for the European legislator, and which consists in the use, as until now, of specific functional safety methodologies for products, mainly Common Criteria, for which Europeans standards are being generated; and a more flexible one, which authorises certification using other methodologies, including those established *ad hoc*, but that can only be used in the absence of European standards under the first indent, or while a product is in the evaluation process under those standards; all this according to the recent Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30 (3) and 39 (2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market[24].

With regard to the contents of the aforementioned Decision 2016/650, it should be noted that it is issued under Article 30 (3) and 39 (2) of the eIDAS Regulation, without any mention being made of Articles 29 (2) and 39 (1) of the Regulations; and this despite the fact that both "standards for the evaluation of the security of information technology products" and "standards relating to qualified electronic signature creation devices" (applicable *mutatis mutandis* to the qualified electronic seals creation devices) are referenced therein.

Among the first, which in effect would be those of Articles 30 (3) and 39 (2), we find the references to the Evaluation criteria for IT security[25] and the Methodology for IT security evaluation [26].

[24] This Decision has derogated Commission Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council.

[25] ISO/IEC 15408-1:2009 – Information technology – Security techniques – Evaluation criteria for IT security – Part 1, ISO/IEC 15408-2:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 2 and ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 3.

[26] ISO/IEC 18045:2008: Information technology – Security techniques – Methodology for IT security evaluation.

However, among the latter we find the CEN EN 419 211 standard, parts 1 to 5, successor to CEN CWA 14169, which was referenced in Decision 2003/511/EC precisely as a standard that enjoys general recognition for electronic signature products with the effect of presumption of compliance. Logically, this rule should have been referred, therefore, not to the legal basis of articles 30 (3) and 39 (2) of the eIDAS Regulation, but for the purposes of articles 29 (2) and 39 (1) of the Regulation, since it could be the case that a qualified product that has obtained the corresponding certification is considered not to be protected by the legal presumption of compliance with the legal requirements established in Annex II of the eIDAS Regulation.

Second, Decision 2016/650 makes use of the two possibilities provided for in Article 30 (3) of the eIDAS Regulation, by establishing, on the one hand, "standards for the security assessment of information technology products that apply to the certification of qualified electronic signature creation devices or qualified electronic seal creation devices according to point (a) of Article 30(3) or 39(2) of Regulation (EU) No 910/2014, where the electronic signature creation data or electronic seal creation data is held in an entirely but not necessarily exclusively user-managed environment", and, on the other, authorise the certification of qualified electronic signature creation devices or qualified electronic seal creation devices, when a qualified provider of trust services manages the electronic signature creation data or the electronic seal creation data. on behalf of a signer or a creator of a seal, which "shall be based on a process that, pursuant to Article 30(3)(b), uses security levels comparable to those required by Article 30(3)(a) and that is notified to the Commission by the public or private body referred to in paragraph 1 of Article 30 of Regulation (EU) No 910/2014"; that is, any evaluation process equivalent to the Common Criteria and the protection profiles of the CEN EN 419 211 standard, at the discretion of the designated certification body, which is the one that must make the decision about the methodology to be used and communicate it to the European Commission[27], as has happened in the case of Spain and Italy, for example[28].

Furthermore, Article 31 (2) of the eIDAS Regulation provides that "the Commission shall establish, publish and maintain a list of certified qualified electronic signature creation devices", based on the information that the Member States must send to it (provided for in Article 30 (1) of the eIDAS Regulation); a rule that clearly seeks to establish

[27] The eIDAS Regulation does not clarify whether the products certified under this second option will only be considered qualified devices in the State where they have been certified or, on the contrary, such products may be marketed in other States of the Union as qualified devices. In our opinion, it should be understood that said products will enjoy the benefit of free movement provided for in Article 4 (2) of the eIDAS Regulation.

[28] Cf. https://ec.europa.eu/futurium/en/content/list-alternative-processes-notified-commission-accordance-article-303b-and-392-eidas.

an administrative mechanism for administrative publicity that provides certainty to the providers and users of trust services, especially to the parties that trust, currently available at the European Commission's eIDAS Observatory[29].

Finally, it is imperative to note that Recital 56 of the eIDAS Regulation mentions that "this Regulation should not cover the entire system environment in which such devices operate. Therefore, the scope of the certification of qualified signature creation devices should be limited to the hardware and system software used to manage and protect the signature creation data created, stored or processed in the signature creation device", due to what "the scope of the certification obligation should exclude signature creation applications".

5.4. The legal effect of electronic signatures and seals

From the perspective of the legal effects, any electronic signature or seal, regardless of its classification as "ordinary" or "simple", "advanced" or "qualified" serve the same objective of attributing the content of the document to the natural or legal person, and therefore are potentially valid and, depending on the case, perfectly acceptable[30].

In this sense, Recital (22) of the eIDAS Regulation says that "in order to contribute to their general cross-border use, it should be possible to use trust services as evidence in legal proceedings in all Member States"; and for its part, Recital (49) of the eIDAS Regulation indicates that "this Regulation should establish the principle that an electronic signature should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic signature".

In short, the eIDAS Regulation establishes a legal norm of non-discrimination of the electronic signature different from the qualified electronic signature, which also extends to the unqualified electronic seal. This is shown in Article 25 (1) of the eIDAS Regulation, when it establishes that "an electronic signature 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 for qualified electronic signatures", while, in relation to the electronic seal, article 35 (1) of the eIDAS Regulation indicates that "an electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an

[29] https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds.

[30] Cf. (Caprioli, 2014, p. 102) or (Madrid Parra, 2001, p. 230).

electronic form or that it does not meet the requirements for qualified electronic seals".

Consequence of all this is that we must start from the potential validity of all electronic signature technology (Chou, 2015, p. 85) and electronic seal, because the legally relevant thing is to be able to attribute, from and evidential perspective, a content to a natural or legal person, according to the circumstances of the case, with a specific situation that varies depending on the solemnities and the forms required for the production of each legal act.

Different question of the potential validity will be that of the specific legal effects of non-qualified electronic signatures or electronic seals, which remains in the hands of each national legislator[31].

The real difference between a simple electronic signature or seal, an advanced electronic signature or seal, or a qualified electronic signature or seal does not reside in its legal validity or admissibility, except in those acts subject to formal requirements, and not even in its potential effectiveness[32], but in the set of technical requirements necessary to achieve or even legally guarantee specific legal effects, in particular, by way of legal assumptions, which reverse the burden of proof, contained in the eIDAS Regulation and those that are can be established at the national level (Recital (22) of the eIDAS Regulation).

However, it should be noted, with respect to legal validity, that the use of any non-qualified electronic signature may be restricted by applicable regulations, imposing the use of the qualified electronic signature or a specific type of non-qualified electronic signature. Infringing the legal duty to use a legally required type of signature will undoubtedly affect the validity of the electronic signature, due to the breach of a formal requirement, in spite of the fact that, even in this case, said signature may become effective in a judicial procedure.

From the point of view of effectiveness, and with respect to the qualified electronic signature, article 25 (2) of the eIDAS Regulation establishes that "a qualified electronic signature shall have the equivalent legal effect of a handwritten signature", while with respect to the qualified electronic seal, Article 35 (2) of the eIDAS Regulation determines that "a qualified electronic seal shall enjoy the presumption

[31] Recital (22) of the eIDAS Regulation recognised that "it is for the national law to define the legal effect of trust services, except if otherwise provided in this Regulation", while Recital (49) of the eIDAS Regulation says that "it is for national law to define the legal effect of electronic signatures, except for the requirements provided for in this Regulation according to which a qualified electronic signature should have the equivalent legal effect of a handwritten signature".

[32] Because if it is admissible as evidence, it will potentially produce legal effects, even if the national legislator does not regulate any specific legal effect for these instruments, or regulate an effectiveness of the unskilled electronic signature different from the equivalence with the written signature of a natural person, or a different efficacy of the unqualified electronic seal than the presumption of origin and data integrity of a document or communication of a legal person. And in this context, what is established by sectoral regulations or the parties' will be particularly relevant.

of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked".

In both cases, it is a typical legal effect, which seeks to generate legal certainty for users of qualified electronic signature or seal systems, which do not therefore need to regulate the operation of the electronic signature or seal system, nor obtain a prior authorisation to use them, in their relations with third parties.

In summary, we have two levels that characterise the effectiveness of the electronic signature: the legal rule of non-discrimination, according to which the party who is interested in the effectiveness of a valid electronic signature has the right to have sufficient evidence, which determine if the electronic signature was reliable enough to impute the act to the person who produced it; and the rule of equivalence, which does not eliminate the need for this test, but reduces it considerably, by presuming the special suitability of a certain technology (which can be subsumed in the legal concept of a qualified electronic signature) to act substantively as if was the handwritten signature of that person, effectively *erga omnes*.

While the legal rule of non-discrimination allows the existence of atypical electronic signatures, the substantive effects of which will be defined by the parties, being able to "serve to sign [in that particular case]", the equivalence rule establishes a typical electronic signature that provides security legal to the parties that decide to use it, due to its suitability to "serve to sign [in any case]". And given the need to admit the use of non-qualified electronic signatures in certain areas, it is observed that in effect the Member States establish unique typical effects for these non-qualified signatures, limited to their jurisdiction.

Member States can not only establish legal effects with regard to non-qualified electronic signatures, but can also do so in relation to qualified electronic signatures, provided that such effects go beyond the typical effect defined in the eIDAS Regulation, such as will happen in the case of the establishment of a presumption of authenticity of the qualified electronic signature[33].

In the case of the electronic seal, something similar would happen with the electronic signature, although with the difference that there is no legally described equivalence effect, as in the electronic signature; that is to say, that the typical effect of the seal is, as we have seen, to prove the authenticity of the origin of the data and its integrity, and not be equivalent to any previously existing artefact, such as the “physical seal of a legal person”.

Given the absence of this effect of "equivalence with", reasonable doubts can be generated about the acts for which an electronic seal can be used (regardless

[33] This is the case in the case of German procedural legislation, when the qualified electronic signature has been validated in accordance with article 32 of the eIDAS Regulation, as shown in section § 371a (1) of the German Code of Civil Procedure (*Zivilprozessordnung – ZPO*). With respect to the German regulation before eIDAS Regulation, see (Wolf & Zeibig, 2015, p. 36).

of whether it is ordinary, advanced or qualified), except when we find ourselves before the substantive legal requirement that a legal person must offer a guarantee of authenticity of the origin of the data and the integrity of the content, as is the case, for example, in the case of electronic invoices. Neither does it seem unreasonable to resort to the use of the electronic seal in those cases where there is a rule that provides for the use of a (physical) seal of a legal person. One example is the usage of electronic seals by public sector bodies to authenticate their electronic documents.

However, although we know that for the eIDAS Regulation, the electronic seal must serve as proof that an electronic document has been issued by a legal entity, providing certainty about the origin and integrity of the document –Recital (59)– and to authenticate any digital asset of the legal entity, for example, computer programs or servers –Recital (65)–, therefore it cannot be inferred that it can be used by the legal entity for all legally binding actions, especially in accordance with the rules of representation of the different types of legal entities.

In this regard, it is surprising that Recital (58) of the eIDAS Regulation establishes that "when a transaction requires a qualified electronic seal from a legal person, a qualified electronic signature from the authorised representative of the legal person should be equally acceptable", probably to prevent that the existence of the seal could negatively affect the representation, in the sense of negatively discriminating the actions of the representative of the legal entity in question.

It seems that for the European legislator an electronic seal could be used for any action of a legal person, but it must be remembered that the Regulation does not affect Union or national law related to the conclusion and validity of contracts or other legal obligations or of procedure related to the form, so we analyse each specific case to find out whether or not it is possible to use a seal for a certain legal act.

Again, Member States can determine in their legislation the legal effects produced by electronic seals, following two types of regulations: those that may regulate effects of non-qualified electronic seals in some concrete cases, and, unlike the qualified electronic signature, those that authorise the use of the qualified electronic seal for certain transactions, such as, for example, in the field of relations between legal entities and public sector entities, for public sector bodies issuance of electronic legal acts[34], in the case of electronic invoicing, or even to formalise legally binding actions for the legal person without the necessary intervention of a natural person acting of its behalf[35].

[34] This is the case, e.g., of the Spanish public sector regime legislation, that allows a Public Administrativo to issue legal acts in an automated form, using an electronic seal.

[35] This possibility is considered perfectly natural by (Gobert, 2015, p. 39) and has been adopted in Belgium.

In the event that Member States do not establish specific rules regarding the effects of electronic seals, or authorising their use in those cases where representation by a natural person is legally required, it will also be necessary to attend to what the parties agree, within self-regulation scope, or to the intrinsic usefulness of the seal, which for example could be used for the authentication of communications sent by legal persons to third parties, including the accreditation of identity when accessing to electronic repositories, or even for the formalization of general terms and conditions[36].

To the main legal effect that we have just explained, the IDAS Regulation adds a second legal effect, identical in relation to both institutions, when Article 25 (3) mandates that "a qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States", and Article 35 (3), that "a qualified electronic seal based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic seal in all other Member States".

It is a cross-border recognition effect that justifies the very existence of the eIDAS Regulation, which is oriented to the Digital Single Market, as we already know, and which is limited to qualified electronic signatures or qualified electronic seals that are based on qualified certificates issued in the Member States.

Two considerations need to be made regarding this provision. The first of these is that the eIDAS Regulation does not establish any rule regarding the cross-border recognition of signatures or electronic seals that are not qualified, so that such recognition will be subject to the provisions of the national legislature, in application of the applicable legislation. to the case, being able to enter the game of autonomy of the will of the parties when the applicable legal framework allows it.

Second, it is surprising that cross-border recognition is limited to a qualified electronic signature or a qualified electronic seal based on a qualified certificate because, as we have seen, a signature or a seal can only be qualified when based on a qualified certificate, because it is a constitutive element of the legal concept.

[36] In relation to the latter case, the Judgment of the Court of Justice (Third Chamber) of 25 January 2017, in the case BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG v Verein für Konsumenteninformation (C-375/15), interprets that an Internet site can constitute a durable means when it allows the user of payment services to store the information that is sent to him personally in such a way that this information can be consulted later for a period of time appropriate to its purpose and reproduced without changes, provided that any possibility of unilateral modification of its content by the payment service provider or by any other professional entrusted with the management of the website is excluded, assurances that the advanced electronic seal undoubtedly offers as, in any case, does the qualified electronic seal.

For this reason, this provision is only understood from the point of view that said qualified certificate has been issued in a Member State, and not in a third State, something that would support the position that qualified electronic signatures or seals based on certificates issued in States that are not members of the Union do not necessarily enjoy the effect of cross-border recognition as qualified signatures or seals, in line with the former German law[37].

Perhaps due to the displacement of the national legislation operated by the eIDAS Regulation, it has been considered necessary to foresee at the European level a standard such as that contained in Article 25 (3), in relation to the electronic signature, and in Article 35 (3), in relation to the electronic seal, but said rule could potentially conflict with the provisions of Article 14 of the eIDAS Regulation, by virtue of which, for all trust services, the possibility of declaring its equivalence is provided by recognition by agreement between the Union and the third country or international organisations.

In this case, we must understand that the qualified electronic signature based on a qualified certificate issued in a third country with an agreement must also be recognised as a qualified electronic signature in all other Member States, because otherwise the undesirable result of not applying Article 14 of the eIDAS Regulation. See, to this end, Article 24 (4) (ter) of the Italian CAD[38].

The eIDAS Regulation has established a series of rules for the cross-border admission of electronic signatures and seals (Polanksi, 2015, p. 778), which will affect the freedom of the Member States to regulate the conditions of use of these systems of electronic evidence in the relationships established with them.

Although it is not the first time that Union law establishes criteria to facilitate the cross-border admission of electronic signatures[39], it is the first time that a general rule has been established.

First, according to Articles 27 (3) and 37 (3), Member States shall not request for cross-border use in an online service offered by a public sector body an electronic signature por seal at a higher security level than the qualified electronic signature or seal. It is a rule clearly aimed at guaranteeing the cross-border transactions of Union citizens, who in their states of residence will typically obtain, at most, a qualified electronic signature or seal system. In spite of what has just been indicated, as is logical, this regime also applies to

[37] Article 162a (1) of the German Civil Code (BGB), before reformed by Article 11 (27) of the *eIDAS-Durchführungsgesetz* of 18th July 2017, which has suppressed this reference. See Article 23 of *Signaturgesetz* of 16 May 2001, and (Bierekoven, Bazin, & Kozlowski, 2004, pp. 7-8).

[38] As drafted by *Decreto legislativo n.º 179*, of 26th August 2016.

[39] Car. Commission Decision of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (notified under document C(2011) 1081); or Article 7 (6) of Regulation (EC) No 1896/2006 of the European Parliament and of the Council of 12 December 2006 creating a European order for payment procedure.

signatures and seals produced by public sector entities, which must be admitted by public sector entities from the other Member States.

As an example of a signature or electronic seal with a higher level of security than the qualified one, we can cite the mandatory imposition of a qualified electronic time stamp on the content of the signed document, or an electronic signature certificate with attributes –as in the case of legal or voluntary representation– or an attribute certificate, in addition to the qualified electronic signature certificate. This provision does not preclude the possibility of European legislation to impose additional content requirements for qualified certificates, of course[40].

Second, Articles 27 (2) and 37 (2) of the eIDAS Regulation order that if a Member State requires an advanced electronic signature or seal based on a qualified certificate to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures or seals based on a qualified certificate and qualified electronic signatures or seal in at least the formats or using methods defined in the implementing acts referred to in paragraph 5; while Articles 27 (1) and 37 (1) of the eIDAS Regulation mandate that if a Member State requires an advanced electronic signature or seal to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures or seals, advanced electronic signatures or seals based on a qualified certificate for electronic signatures or seal, and qualified electronic signatures or seals in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.

As can be seen in both cases, what the European legislator seeks is, again, to ensure that, at least, advanced electronic signature or seal that are available to users in their own Member State can be used when a different Member State imposes an obligation to use them. Non-advanced electronic signatures or seals, on the contrary, could be excluded for cross-border uses.

These formats and methods have been set by Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS AdES Formats Decision), that essentially refers to XAdES, CAdES, PAdES and ASiC baseline profiles, defined in ETSI TS 103

[40] This is the case with qualified certificates of payment service providers under Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (PDS2). To this end, see Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

171 v.2.1.1, ETSI TS 103 173 v.2.2.1, ETSI TS 103 172 v.2.2.2 and ETSI TS 103 174 v.2.1.1; or to the use of equivalents methods described in the same Decision.

Article 2 (1) of the eIDAS AdES Formats Decision mandates that "Member States requiring an advanced electronic signature or an advanced electronic signature based on a qualified certificate as provided for in Article 27(1) and (2) of Regulation (EU) No 910/2014, shall recognise other formats of electronic signatures than those referred to in Article 1 of this Decision, provided that the Member State where the trust service provider used by the signatory is established offers other Member States signature validation possibilities, suitable, where possible, for automated processing". This is an interesting possibility because it mandates the cross-border recognition (by public sector bodies) of new signature or seal formats, allowing innovative possibilities that were not forecasted when approving the Decision, such as linked data signatures used for the authentication of a verifiable credential.

Article 2 (2) of the eIDAS AdES Formats Decision sets out the requirements with respect to the signature validation possibilities, that shall:

"(a) allow other Member States to validate the received electronic signatures online, free of charge and in a way that is understandable for non-native speakers;

(b) be indicated in the signed document, in the electronic signature or in the electronic document container; and

(c) confirm the validity of an advanced electronic signature provided that:

(1) the certificate that supports the advanced electronic signature was valid at the time of signing, and when the advanced electronic signature is supported by a qualified certificate, the qualified certificate that supports the advanced electronic signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I of Regulation (EU) No 910/2014 and that it was issued by a qualified trust service provider;

(2) the signature validation data corresponds to the data provided to the relying party;

(3) the unique set of data representing the signatory is correctly provided to the relying party;

(4) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;

(5) when the advanced electronic signature is created by a qualified electronic signature creation device, the use

of any such device is clearly indicated to the relying party;

(6) the integrity of the signed data has not been compromised;

(7) the requirements provided for in Article 26 of Regulation (EU) No 910/2014 were met at the time of signing;

(8) the system used for validating the advanced electronic signature provides to the relying party the correct result of the validation process and allows the relying party to detect any security relevant issues".

6. THE LEGAL REGIME OF TRUST SERVICES

6.1. The eIDAS characterisation of trust services

According to Article 3 (16) of the eIDAS Regulation, a 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".

This Article does not properly contain a definition or concept of trust service, but rather an enumeration of information society services which, precisely because they are included in the closed list, are considered to be "trustworthy".

Before entering the presentation, necessarily succinct in this study, of the trust services, it is necessary to indicate that this name of "trust service" contained in the eIDAS Regulation constitutes an evolution and, at the same time, a semantic extension on the name of the "certification service" used in the eSign Directive. It is an expression based on the fact that these services provide confidence in the business processes in which they are used, largely thanks to the legal effects associated with said services.

Thus, according to Recital (2) of the eIDAS Regulation, it "seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union", for which it is necessary to

go beyond the regulation of electronic signature, which did not offer "a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions".

The eIDAS Regulation, therefore, pursues the creation of a uniform law for the internal market, providing harmonised legal norms in relation to various services, which in fact already operated on similar technical standards, and offers the possibility of coordinating the different bases laws for electronic government and digital society globally, although it also poses important challenges (Borges, 2012).

This notion of "trust service", also referred to as "reliable service" or "trusted service", is not an invention of the eIDAS Regulation, but rather has been used for a long time by market agents, as well as by scholars.

For example, (Ølnes, 2001) defines trust as the perception of absence of vulnerabilities and, after distinguishing between technical and organisational trust, offers a taxonomy of reliable services attending to some characteristics of such services, such as type of service, quality of service, evidence management, user community, trust model, legal aspects and communications pattern.

(Baldwin, Shiu, & Cassasa Mont, 2002) refer to trusted services as e-commerce enablers and indicate the existence of trusted services widely installed in paper processes, considering that service providers are experts managing risks related to the services they offer, and provide a list of services candidates to enter this qualification: identity, authorisation, anonymity, qualification and trust recommendation, guarantee of delivery of communications, generation of auditable receipts, storage and notarisation. These authors also refer to the existence of certain services of trustworthy components, which are meaningless to end users, but which are used in other trusted services, including key storage services, archiving services and date and time stamp services.

For (Dumortier & Vandezande, 2012b), trust in e-commerce operations works in a similar way to a black box: the user is confident that the machine will record all processes and maintain sufficient evidence to be able to reproduce what really happened; an approximation they consider that may be more effective than the use of electronically signed documents. In their opinion, and regardless of the definition or concept of trust, it always consists of an internal state of the user evoked by the reliability characteristics of the technology, being an informed acceptance of the vulnerability.

In short, we could conceptualise trusted services as those technologies that can be trusted, modifying the user's perception regarding the vulnerability of a process to which they are incorporated. For this, the user must be able to recognise a trust service, in fact, as secure and reliable enough. To do this, the approach of the eIDAS Regulation is the creation of a reinforced level of services of trust, which is significant in the sense that the trust in these services seems to be born from the fact that they are legally regulated, rather than only in their own technical characteristics.

In this sense, Article 3 (17) of eIDAS Regulation provides the notion of a qualified trust service, defining it as "a trust service that meets the applicable requirements laid down in this Regulation", which differentiates two "reliance levels":

- The non-qualified trust service level, which is not practically regulated, and does not receive any particular legal recognition; and in which case, the user must construct his own internal state of trust with respect to the service. For example, a person can recognise a password from your financial institution as being secure enough, but not a cloud storage service.

- The qualified trust service level, which is highly regulated, and receives a particular recognition of legal effects, something which should be an incentive to its adoption, a promise that has not always been fulfilled due to several inhibitors, as shown by (Roβnagel, 2006), (Srivastava, 2011) or (Dumortier & Vandezande, 2012a). In this case, this explicit legal recognition is the one that allows the user to recognise the service as reliable, so we can assume that these services will be developed earlier and in greater volume than those that do not enjoy this condition.

It should also be noted that the eIDAS Regulation contains a closed list of trusted services in order to delimit the scope of the uniform European regulation but that Member States may define other trust services as well as maintain (or introduce) national provisions, in accordance with Union law, concerning trust services of confidence, provided that such services are not fully harmonised by this Regulation, considerations which show the central objective of the regulation, which is none other than to guarantee the free movement of these services in the internal market, by means of a minimum set of harmonised standards.

One consequence of this model is the more than possible divergence in the catalogue of trust services in the different jurisdictions of the European Union, as the business sector is constantly generating new services, based on technological innovation. For instance, Belgium has regulated a national trust service, consisting in a secure document archive, with a specific legal effect, both as non-qualified and qualified service.

Regarding the closed list of trust services, it derives from the definition of the qualified trust service that we have just seen and, by virtue of which, only one service can be qualified in relation to which the eIDAS Regulation has established specific requirements. It follows that, in reality, we have two lists of trust services, since not all trust services can be subject to qualification.

More specifically, the nine trust services typified in the eIDAS Regulation that may be subject to qualification are the following:

- Three services for the issuance of qualified electronic certificates, for the electronic signature of a natural person, the electronic seal of a legal person and the authentication of websites, given that Article 28 and

Annex I of the eIDAS Regulation, Article 38 and the Annex III of the eIDAS Regulation, and Article 45 and Annex IV of the eIDAS Regulation establish, respectively, the corresponding requirements.

- A service for the issuance of qualified electronic time stamps, given that Article 42 of the eIDAS Regulation establishes the corresponding requirements.

- A qualified electronic registered delivery service, since Article 44 of the eIDAS Regulation establishes the corresponding requirements.

- Two qualified services for the validation of qualified electronic signatures and qualified electronic seals, since Article 33 and Article 40 of the eIDAS Regulation establish, respectively, the corresponding requirements, applying Article 33 *mutatis mutandis* in the case of the seal.

- Two qualified services for the preservation of electronic signatures and qualified electronic seals, since Article 34 of the Regulation and Article 40 of the eIDAS Regulation establish, respectively, the corresponding requirements, applying Article 34 *mutatis mutandis* in the case of the seal.

On the other hand, non-qualified trust services include, in addition to the non-qualified versions of the nine services contained in the previous list, also the following, since they are expressly cited in the definition of trust service contained in the eIDAS Regulation:

- A remote electronic signature (ordinary and advanced) and electronic seal (ordinary and advanced) creation service.

- A validation service for electronic signature, electronic seal and website authentication certificates.

- A service for the preservation of signature and electronic seals certificates.

It does not seem reasonable that this differentiation should exist, at least from a theoretical point of view, given that, in the double-level logic established in the eIDAS Regulation, any trust service should be potentially qualified. However, it is true that, if no specific requirements are established for a trust service, there is no basis for this qualification, at least in the current legal definition, which is ultimately the fulfilment of minimum conditions in support of the quality, security and trustworthiness of the service.

This differentiation can ultimately lead to consistency problems in the market, causing confusion for users. For example, with this legal interpretation, it is perfectly imaginable that a trust service provider offers the (non-qualified) service for the creation of an electronic/advanced remote signature or seal, where appropriate generating or managing the corresponding signature or seal

creation data, while the provision of the same service, but in relation to the electronic qualified signature or seal, will be reserved to any of the qualified provider, because only those who manage the corresponding creation data can allow the creation of the signature or seal.

One possibility, more than reasonable, is that the provider that issues the qualified electronic signature certificate or qualified electronic seal certificate is also the one that offers the service of generation or management of the corresponding creation data, given that said provider is precisely responsible, vis-à-vis third parties, for the usage of a qualified device, but a model is also imaginable in which another qualified trust service provider performs this generation or management of the qualified signature or seal creation data , as in the case of a provider that offers qualified signature or seal validation or preservation services.

Apparently, in this construction, it does not fit that the regulation of the identification evidence has not been classified as a typical trust service (Kennedy & Millard, 2016, p. 102), since it is not expressly included in the definition of these services, but in reality this is not entirely true.

First, it happens that there are harmonised trust services in the eIDAS Regulation that have, among their typical legal effects, that of allowing electronic identification. This is the case of the issuance of certificates of electronic signature of a natural person, a trust service harmonised by the eIDAS Regulation, which confirms the identity of said natural person; and in the same way it happens with the certificate of electronic seal of legal person, which confirms its identity. Therefore, these trust services, which can be subject to qualification, allow electronic identification, at least in connection with said electronic signature or electronic seal.

Similarly occurs with the authentication –which actually fulfils the identification function– of the websites, which is dealt with in the eIDAS Regulation, unlike the electronic identification of individuals, as a harmonised trust service, including with qualification.

Secondly, the reason why electronic identification is not treated as a trust service in the eIDAS Regulation is its consideration as a national prerogative (Recital (12) of the eIDAS Regulation), which allows its maintenance by the State as a public service, without being obliged to authorise its provision by private operators, and less as an economic activity. But it does not follow from this that this decision cannot be taken at the national level, such as in Italy, that publishes in their trusted list the “identity verification service”, that allows citizens to use the national service card[41] to authenticate themselves over the network, offered by qualified trust service providers, with the exception of the Ministry of Interior, issuer of the national identity card.

[41] Cf. https://www.agid.gov.it/index.php/en/piattaforme/national-service-card.

In any case, what happens is that the electronic identification of people –not of websites– actually has various applicable legal regimes, which are fully alternative, and which can even coexist in the same Member State, and can be treated as a public service, as a trust service, or even as a third type of private service, depending on what each Member State decides.

All this explains, in fact, that the regulations contained in the eIDAS Regulation are not applicable to electronic identification except in terms of their cross-border recognition between the Member States, which certainly implies establishing a typical legal effect for these systems, "to serve for cross-border access to public and, eventually, private services", but nothing more.

From this perspective, the regulation of electronic identification contained in the eIDAS Regulation presents a different extension to the regulation of trust services, because it only regulates its dimension of cross-border use, while the regulation of trust services refers to both the cross-border use of services, such as the regime for its provision and its substantial legal effects.

6.2. The eIDAS regulatory model for trust services

As we have pointed out, and in contrast to the eSign Directive, where the provision of certification services was not subject to any kind of previous licence, the eIDAS Regulation opts for a regulatory orientation of prior administrative authorisation in relation to the provision of qualified trust services – (Gobert, 2015, p. 27) or (Rico Carrillo, 2015, pág. 8)–, while maintaining the *ex post* supervision model for non-qualified services.

Indeed, Article 21 (1) of the eIDAS Regulation sets out that a provider, who does not have a qualification, to begin its activity relating to qualified services, must submit to the supervisory body a notification of his intention together with a conformity assessment report issued by a conformity assessment body, whereas Article 17 (3) (a) (4) (g) stipulates that the national body will carry out prior supervision and the award of the qualification, and that the service cannot be started until such qualification has been obtained (Article 21 (3)), and it has been publicly disseminated through the mechanism provided for in Article 22 of the eIDAS Regulation (the Trusted List). Although with a somewhat obscure terminology, this is an administrative authorisation, which must be granted under the relevant administrative procedure, within the national legislation framework.

In addition, the qualified provider of trusted services must pass a conformity assessment at least every two years and send it to the supervisor, as determined by Article 20 (1) of the Regulation, as well as accept any audit performed by the supervisor, or additional assessments of conformity that it imposes on it, pursuant to the provisions of paragraph 2 of Article 20 of the eIDAS Regulation.

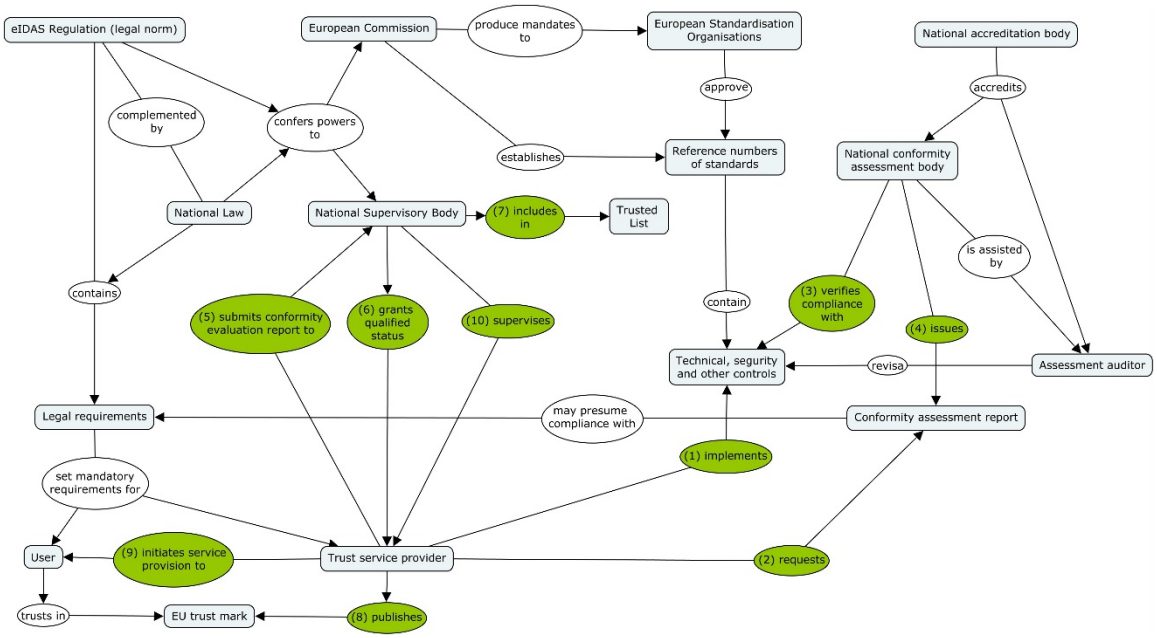

Figure 14. eIDAS Regulatory model conceptual map (Alamillo Domingo, 2019a)

As seen in the Figure, technical standards play a significant role (Nguyen, 2018), sometimes being applicable in a voluntary basis (i.e. the policy and security requirements set forth by ETSI standards), while in other cases they become mandatory (e.g., in the case of the so-called qualified electronic signature or seal devices, according CEN standards).

It is also interesting to note that qualified trust services have a strict liability regime contained in Article 13 (1) of the eIDAS Regulation. In its virtue, "`trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation`" (subparagraph 1), and "`the intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider`" (subparagraph 3); while in the case of non-qualified trust services, "`the burden of proving intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph`" (subparagraph 2).

This new regulatory approach is a clear exception to the approach of the e-Commerce Directive, which in its Article 4 prohibits the subjection of information society services to prior authorisation or any other requirement with equivalent effect, and Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, which limits the possibility of restricting access to and authorisation only in certain circumstances.

That doesn't mean that the rest of the regulation of the information society services do not apply. On the contrary, any provision in that regulation that doesn't conflict with the trust services regulation will be applicable to a DLT/Blockchain based trust service.

The legal regime of qualified trust services included in the eIDAS Regulation has been partially developed by the following implementing acts:

- Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services (Text with EEA relevance). This implementing act is relevant for the EBSI project because it allows a provider to easily prove that it is issuing qualified certificates, facilitating the adoption of the derived identities by relying parties. According to Article 23 (1) of the eIDAS Regulation, "after the qualified status referred to in the second subparagraph of Article 21(2) has been indicated in the trusted list referred to in Article 22(1), qualified trust service providers may use the EU trust mark to indicate in a simple, recognisable and clear manner the qualified trust services they provide".

- Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance). This implementing act is also relevant for the EBSI project because these formats have the legal admissibility granted in relationships with public sector bodies.

- Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance).

- Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30 (3) and 39 (2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance).

6.3. Issuance of electronic signature/seal/website digital certificates

Public key certificates have been regulated as a specific trust service by the eIDAS Regulation, differentiating three types of certificates, according to its use: natural persons certificates used in connexion of their electronic signatures,

legal persons certificates used in connexion of their electronic seals, and website certificates.

In the eIDAS Regulation, the digital certificate is always treated as an electronic proof of identity, whether a natural person or a legal entity, and regardless of whether the certificate is used to support an electronic signature, an electronic seal or a domain name on the Internet.

Article 3 (14) of the eIDAS Regulation refers to the electronic signature certificate as "an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person", and Article 3 (15) thereof, to the qualified certificate as "a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I".

Similarly, in the case of the electronic seal, Article 3 (29) defines the electronic seal certificate as "an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person", whereas Article 3 (30) refers to the qualified certificate as "a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III".

For its part, Article 3 (38) of the eIDAS Regulation defines the certificate of website authentication as "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", defining Article 3 (29) the website authentication qualified certificate as "a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV".

This "identification" (of the natural or legal person), which is the main purpose of digital certificates, is issued in respect of various legal purposes provided for by the eIDAS Regulation, mainly to support the signature or advanced electronic seal at a later stage by confirming the identity of the person concerned, and for the authentication of websites; this means that the websites can be identified on or from the connections made to them. The three certificate types are used, in some way or another, to "authenticate" the identity of the natural or the legal person, with additional attributes when needed.

To underpin the confidence of relying parties, the eIDAS Regulation establishes a set of minimum standards covering the content of each of these certificates and the minimum obligations of providers issuing them, defining the relevant trust services for issuing certificates.

The question that may arise, although only in relation to the use of electronic signature or electronic seal certificates, is whether they can be used so that the natural or legal person identified in the certificate can be electronically

identified in a process that does not require the electronic signature or the electronic seal, as for example in the case of access to a web page with informative content that requires the necessary prior authentication; that is, if these certificates serve, in addition to signing or sealing, to authenticate themselves, normally in an access control process. Or, in other words, if they can be used in an entity authentication service.

This is a doubt that the eIDAS Regulation does not solve directly, simply because it is not applicable to the decisions that Member States make in domestic authentication processes –usually in the field of electronic administration, although not exclusively– and, therefore, this possibility will depend on what the national law establishes in this regard, as for example happens in Spain or France. But what is certain is that a State may notify the use of electronic signature or seal certificates as an identification system for cross-border purposes, in which case the answer will, of course, be affirmative.

In view of this possibility, it would certainly seem strange that a qualified certificate supporting a qualified electronic signature could not be used for any other process where electronic identification and authentication are required, where appropriate based on the autonomy of the parties' will, in spite of the existence of legal exceptions that are duly justified.

On the other hand, the eIDAS Regulation does not regulate the use of electronic certificates that cannot, at least, be used to validate electronic signatures or seals, so a certificate that is issued only to identify a person –but not for the creation of the signature or the electronic seal– would be outside the harmonised regulation, and would, as we already know, be subject to regulation at the national level, or event be accepted simply on the basis of the autonomy of the parties' will, as is the case with other electronic identification systems.

An example of a trust service for certificate issuance used exclusively for electronic identification is found in Italian Law, without qualification under the eIDAS Regulation, but with recognition as such a trust service at national level, and advertised on the Italian trusted list. It is the authentication certificate (of entity) incorporated to the national service card (*Carta Nazionale dei Servizi*[42]), a document issued in computer support intended to allow telematic access to the services provided by Public Administrations –including the submission of

[42] Regulated by *Decreto del Presidente della Repubblica 2 marzo 2004, n. 117, Regolamento concernente la diffusione della carta nazionale dei servizi, a norma dell'articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n. 3*; its current legal definition is contained in Article 1 (1) (d) of *Decreto Legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale (CAD)*, and Article 64.2-novies, incorporated by Article 50 (1) (e) of *Decreto Legislativo 26 agosto 2016, n. 179*, authorises access through this card to the services offered electronically by Public Administrations, just as with the *carta d'identita' elettronica* and the novel system SPID.

applications and writings[43]– with the particularity that said certificate is issued by qualified trust service providers on behalf of the card issuing Administration.

The eIDAS Regulation does not establish any specific legal effect in relation to the use of the electronic certificate, even when it is qualified, surely due to its accessory nature to the processes it supports, and in spite of the definition itself. It is clear from the certificate that the certificate confirms the identity of a person, be it a natural person (a signatory), a legal person (a seal creator), or a person (natural or legal) controlling a specific website.

What does not exist in the eIDAS Regulation is, therefore, a functional equivalence rule with any institution used for the proof of identity in face-to-face or distance relationships supported on paper. More specifically, the eIDAS Regulation does not authorise the substitution of a personal identity mechanism –such as a national identity document, on physical support– by an electronic certificate, not even in the case of qualified electronic signature, so the national law is unchanged in this regard, always except for the possibility that a rule of the Union establishes this rule in some specific case.

For this reason, it will be the European Union or national regulations or, when possible, the autonomy of the parties' will, which will enable this possibility, where appropriate. And, consequently, it cannot necessarily be assumed, in general, that "where a law orders the use of an identity document, a certificate of natural or legal person may be used", which would be the embodiment in this case of the rule of the functional equivalent.

Another thing, however, is that a State decides to recognise a certificate as an identification system in accordance with the eIDAS Regulation, making it effective cross-border through the online authentication system guaranteed by the notifying State.

[43] Article 65.1.b) del *CAD* already foresaw this possibility in its initial drafting. In its current wording, it also refers to the SPID system.

Part 3. Legal scenarios related to SSI & eIDAS

In this part we introduce some general legal considerations and a collection of identified legal scenarios, with respect to SSI and the eIDAS Regulation. Whether possible, scenarios are aligned with the current or proposed architectural and procedural considerations discussed in the EBSI eIDAS Bridge and EBSI ESSIF projects.

We have adopted an evolutionary approach, defining very-short term scenarios, short-term scenarios and mid- to long-term scenarios:

- Very short-term scenarios may be implemented with the current eIDAS Regulation, without the need to produce legal changes:
    - Use of notified eIDAS eID means and qualified certificates to issue verifiable credentials.
    - eIDAS Bridge: increasing verifiable credentials' legal value and cross-border recognition.
    - Use current eID nodes to issue a SAML assertion based in verifiable credentials/presentations.
- Short-term scenarios may be implemented with the current eIDAS Regulation, by applying a technologically neutral interpretation of it. There may be a need to slightly modify implementing acts or approve technical specifications:
    - Use of Verifiable IDs as eIDAS electronic identification means.
    - Issuance of qualified certificates based on a specific DID method and verifiable credential.
- Mid- to long-term scenarios require legal modification of the eIDAS Regulation:
    - Extend the eIDAS notification mechanism to Verifiable Attestations: enhanced Trusted Issuers management.
    - Regulate the issuance of Verifiable Attestations as a new trust service.
    - Regulate Identity Hubs as a new trust service, in support of SSI-based TOOP.
    - Regulate delegated key management as an independent trust service.
    - Regulate a specific type of DLT/node as a trust service.

Some very-short term scenarios may be affected, or even superseded, by short-term scenarios. For example, when the scenario "Use of verifiable credentials/presentations as eIDAS eID means" if adopted, the scenario "Use current eID nodes to issue a SAML assertion based in verifiable credentials/presentations" may be abandoned. In another example, if the scenario "Issuance of qualified certificates based on a specific DID method

and verifiable credential" is adopted, the scenario "eIDAS Bridge: increasing verifiable credentials' legal value and cross-border recognition" would slightly change.

7. GENERAL LEGAL CONSIDERATIONS

As a pre-requisite, according to SSI design principles (see section 2 of this report), the person must have obtained a DID, using a valid method, without any critical dependency of a third party. This does not preclude the need to be authorised for accessing a DLT permissioned network by a node, if it does not affect the subject's autonomy (i.e. because the subject can access though any node she decides in any moment).

As per today, EBSI ESSIF is limited to natural persons. Thus, we consider out of scope of this section the considerations of legal persons as subjects/holders of verifiable credentials. Of course, to be able to cover the full scope of the current eIDAS Regulation, the particularities of these subjects should be analysed.

Also, the use of verifiable credentials in support of natural persons acting on behalf of legal persons, under eIDAS Regulation, should be further studied.

Recommendation/s:

[Recommendation 1] Consider extending the EBSI ESSIF use cases to legal persons, to cover full adherence to eIDAS subjective scope.

[Recommendation 2] Define precise semantics for verifiable credentials/presentations in support of natural persons acting on behalf of legal persons, under eIDAS Regulation.

7.1. Regarding the legal value of verifiable credentials and their presentations

Verifiable credentials, as introduced in section 2 of this report, must be considered as electronic documents. As such, they benefit from the provision of Article 46 of the eIDAS Regulation, by virtue of which "`an electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form`".

In application of the non-discrimination principle, this rule ensures the possibility of a verifiable credential to be admitted as evidence in legal proceedings, prohibiting its denial just because of being in electronic form.

But it doesn't mean that a verifiable credential has any specific recognition for any particular purpose. This is quite evident in the case of a verifiable credential, because a verifiable credential does not have fully defined semantics.

On the contrary, each class of verifiable credential can have well-defined semantics if they are properly designed by its issuer, possibly according to a specific governance framework. This could be the case for EBSI ESSIF. In this project we have three potential subclasses of verifiable credentials:

- Verifiable credentials to be used as electronic identification means under eIDAS (provisionally called “Verifiable IDs”).

  A Verifiable ID is defined, provisionally, as “a special form of a «verifiable credential» an entity can put forward as evidence of whom he/she/it is (comparable with a passport, physical IDcard, drivers-license, social security card, member-card…)”.

  The Verifiable ID could be modelled to have precise legal semantics defined by reference to the concepts of the eIDAS Regulation, although it might be better to model it as a verifiable presentation subclass (instead of as a verifiable credential subclass), as we’ll discuss later.

  Regarding this definition, we have to note that is functional, in the sense that it seems to be a verifiable credential designed with the purpose of being appropriate to be used as a notified eIDAS electronic identification means, at least in the EBSI ESSIF current ecosystem, benefiting from the legal effect of notified eIDs, significantly the recognition of these Verifiable IDs for accessing public services in different Member States, as explained in section 4.4.1 of this report.

  This approach would benefit from the potential extension of notified Verifiable IDs to private sector parties, as we’ve introduced in section 4.4.2 of this report.

- Verifiable credentials for the management of legal authorisations and mandates (provisionally called “Verifiable Mandates”), especially in support of the SSI management procedures such as providing access to an Identity Hub.

- Verifiable credentials for conveying any other identity attributes (provisionally called “Verifiable Attestations”). In this case, it is more difficult to establish a legal semantics for any possible Verifiable Attestation, because in reality it depends on the attributes. A proposal, which we’ll discuss later, could be to build generic legal semantics around the concepts of legal acts such as a certification, a testimony, a self-declaration, etc.

However, it is possible to define specific legal aspects of the general verifiable credential class, as long as they apply to all subclasses of credentials, including the subject’s identity proofing when issuing any verifiable credential, verifiable credential’s authentication using an advanced electronic seal based on a qualified issuer certificate (eIDAS Bridge) or the governance of verifiable credential’s issuers (Trusted Issuers).

It is also interesting to analyse the legal semantics of “presenting” a verifiable credential to a third party, from the perspective of the legal act it implies by the subject, and the pertinent liability.

Recommendation/s:

[Recommendation 3] Define, at the verifiable credential class level, all legal properties and procedures that are common to any verifiable credential subclass.

[Recommendation 4] Define precise legal semantics for any verifiable credential and any corresponding verifiable presentation.

7.2. Legal assessment of DIDs, DID Documents and DID control keys

Verifiable credentials use the (optional) property "id" to "to unambiguously refer to an object, such as a person, product, or organisation. Using the id property allows for the expression of statements about specific things in the verifiable credential".

Although it is, in strict sense, non-mandatory, many implementations of verifiable credential systems (including EBSI ESSIF V1) rely on Decentralised Identifiers (DIDs), defined as "a portable URL-based identifier, also known as a DID, associated with an entity. These identifiers are most often used in a verifiable credential and are associated with subjects such that a verifiable credential itself can be easily ported from one repository to another without the need to reissue the credential. An example of a DID is did:example:123456abcdef" (Verifiable Credentials Data Model 1.0). According to 1.2. Technical specification ESSIF - ESSIF DID Modelling[44], properties of DIDs are 1. decentralised, 2. persistent, 3. cryptographically verifiable, and 4. resolvable.

An important concept related to a DID is the DID Document, defined in the W3C DID specification as "a set of data describing the DID subject, including mechanisms, such as public keys and pseudonymous bio-metrics, that the DID subject can use to authenticate itself and prove their association with the DID. A DID document might also contain other attributes or claims describing the subject". This document "typically express verification methods (such as public keys) and services that can be used to interact with a DID controller", according to a DID method ("a definition of how a specific DID scheme can be implemented on a specific distributed ledger or network, including the precise methods by which DIDs are resolved and deactivated and DID documents are written and updated").

From a legal perspective, in an SSI environment, DIDs are identifiers that autonomously created and managed by users, typically with the support of a DLT/Blockchain system. Their legal consideration may depend on the type of entity: i.e. if the user creating a DID is a natural person, the DID will be considered as a pseudonym (constituting personal data) and, therefore, a data that must be compliant with GDPR, as applicable to any party. On the contrary,

[44] https://ec.europa.eu/cefdigital/wiki/display/EBP/1.2.+Technical+specification+ESSIF+-+ESSIF+DID+Modelling.

if the DID is created by a legal person, for itself or for a thing it owns, it will probably be considered as an asset property of the legal person.

According to the W3C DID specification, "these new identifiers are designed to enable the controller of a DID to prove control over it and to be implemented independently of any centralised registry, identity provider, or certificate authority". Thus, generally speaking, a DID is under the control of its "owner", or a third party duly authorised, because of the existence of a mechanism to assure that control, that must be associated to the DID. Although the control mechanism may vary between different DID methods, in many implementations it is based in public key cryptography, such as in the case of EBSI ESSIF v1. This is recognised in section § 3.3 of the W3C DID specification: "a DID document can express cryptographic keys and other verification methods, which can be used to authenticate or authorise interactions with the DID subject or associated parties. The information expressed often includes globally unambiguous identifiers and public key material, which can be used to verify digital signatures. Other information can be expressed, such as status information for the key (for example, whether it is suspended or revoked), or other attributes that enable one to determine whether it is a hardware-backed cryptographic key. Regarding cryptographic key material, public keys can be included in a DID document using, for example, the publicKey or authentication properties, depending on what they are to be used for. Each public key has an identifier (id) of its own, a type, and a controller, as well as other properties that depend on the type of key it is".

Moreover, under section 5.3 of the W3C DID specification "public keys are used for digital signatures, encryption and other cryptographic operations, which in turn are the basis for purposes such as authentication (see Section § 5.4 Authentication) or establishing secure communication with service endpoints (see Section § 5.6 Service Endpoints). In addition, public keys may play a role in the authorisation mechanisms for DID CRUD operations (see Section § 7.2 DID Operations), defined by DID method specifications.

Also, the controller property "which identifies the controller of the corresponding private key, MUST be a valid DID", to expressly indicate the entity that effectively controls the DID and, therefore, may execute (and has ultimate responsibility) the operations described in the DID document.

The legal consideration of the key pair used to control a DID must be exactly the same as the DID it helps controlling, to maintain the logical and legal construct of the SSI. Precisely this is mandated under the SSI principles that were introduced in section 2 of this report, and the DID design goals considered in the W3C specification, at least with respect to natural persons.

We can assume that, from a legal perspective, the DID control key is mainly used for entity authentication purposes, with the objective of cryptographically proving that a DID controller (typically, the DID subject herself) is associated with a DID. Thus, this functionality is supporting the usage of Verifiable IDs as "electronic identification means" in the sense of the eIDAS Regulation (as will further analysed in section 9.1 of this report).

But the same key pair could also be used for a different purpose, which is to provide proof of the integrity of the DID document by the DID subject or the DID controller, if different from the DID subject. As the W3C DID specification is extensible, one could imagine additional features, such as using the DID Document to convey additional information with legal value: i.e. a declaration by a natural person acting as a DID subject that delegates its DID to a different person (DID controller). In this case, from a legal perspective this key could be considered to be as electronic signature or seal creation data. In this case, the eIDAS Regulation would be eventually applicable: i.e. if this proof is to be considered as an advanced or qualified electronic signature.

Which are the legal semantics of this "signature/seal"? As stated in Article 3 (10) of the eIDAS Regulation, 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". The concept of "signing" is not defined in the eIDAS Regulation, but in national Laws (or, more frequently, in jurisprudence), but it is generally accepted that signing is strongly related with providing consent.

The fact is that we can perfectly imagine the use of the DID to perform a legal act, in the sense of concluding a contract, and not only for authenticate the subject. This could be the case, i.e., of the issuance of a Verifiable Mandate by the subject. We'll analyse some of the implications of this possibility in section 10.4 of this report.

Recommendation/s:

[Recommendation 5] Define the legal semantics for DID key usage in connexion with any verifiable credential subclass.

[Recommendation 6] Define key management policies aligned with the legal semantics of DID usages.

8. LEGAL ASSESSMENT OF VERY SHORT-TERM SCENARIOS

8.1. Use of notified eIDAS eID means and qualified certificates to issue verifiable credentials

Description: This scenario considers the utilization of a notified eID for the validation or proofing of the identity attributes that are to be included in any assertion associated to a DID. Moreover, this would be a scenario in which an electronic identification means notified in accordance with the eIDAS Regulation is used to proof the information that will be included in an ESSIF Verifiable ID. This case is described in 2.3. Technical specification ESSIF – Obtaining VC using eIDAS-AuthN[45].

[45] https://ec.europa.eu/cefdigital/wiki/display/EBP/2.3.+Technical+specification+ESSIF+-+Obtaining+VC+using+eIDAS-AuthN.

The scenario considers also the possibility of using a qualified certificate for electronic signature for the same purpose. As we introduced in section 6.3 of this report, the main purpose of a qualified certificate is to confirm the identity of the signatory.

In this section we'll only analyse the legal issues with respect to the identity proofing procedure with respect to ESSIF Verifiable IDs. This analysis could also be applicable for the issuance of a Verifiable Attestation, although in this case it seems more reasonable to use an identity proofing procedure based on a Verifiable ID.

In any case, our analysis considers the need for this verifiable credential (alone of combined with other credentials) to be eligible for notification as an eIDAS electronic identification means. If that would not be the case, self-regulation could be used to establish different rules, but then the value of reusing the eIDAS trust framework would disappear.

Discussion:

From a legal perspective, there could be three classes of subjects: natural persons, legal persons, and natural persons representing legal persons (Article 3 (3) of eIDAS Regulation). The third class is really representing a special kind of relationship (a power of representation) that may be included in a verifiable credential, and thus it will not be considered now.

Under Article 7 of the eIDAS Regulation, for an electronic identification scheme to be eligible for notification, that:

- The notifying Member State ensures that the person identification data uniquely representing the person in question is attributed, in accordance with the eIDAS Security Regulation, to the natural or legal person at the time the electronic identification means under that scheme is issued (Article 7 (d) of the eIDAS Regulation), and

- The party issuing the electronic identification means under that scheme ensures that the electronic identification means is attributed to the person in accordance with the eIDAS Security Regulation (Article 7 (e) of the eIDAS Regulation).

The requirements for identity proofing are, therefore, detailed in the eIDAS Security Regulation, and they are more or less strict depending on the desired level of assurance (as introduced in section 4.3.3 of this report). We will assume that the minimum acceptable level of assurance for a Verifiable ID (or another verifiable credential) is substantial.

The following requirements apply to any identity proofing procedure for natural persons fulfilling level of assurance substantial or high:

- The person can be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity.

- The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid. An authoritative source include that is nationally trusted to provide valid data, such as identity cards, public registries or a private sector service provider register.

- It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.

- The procedure must adhere to one of the following alternatives:

    - The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity; and the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person; and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence.

    - An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it; and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents.

- An issuer is exempt of perform of repeating the identity proofing and verification processes for level substantial, if one of these alternative conditions are met:

    - Where procedures used previously by a public or private entity in the issuer’s Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance, confirmed by a conformity assessment body.

    - Identity proofing and verification is based in a valid notified electronic identification means having the assurance level substantial or high.

    - Identity proofing and verification is based in a valid electronic identification means having the assurance level substantial or high, confirmed by a conformity assessment body.

      In both cases, the issuer will need to take into account the risks of a change in the person identification data.

- In addition to the previous requirements, if the Verifiable ID level of assurance should be high, there exist two possibilities:

    - Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source; and the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source.

    - Where the applicant does not present any recognised photo or biometric identification evidence, the very same procedures used at the national level in the Member State of the entity responsible for registration to obtain such recognised photo or biometric identification evidence are applied.

- An issuer is exempt of perform of repeating the identity proofing and verification processes for level high, if one of these alternative conditions are met:

    - Where procedures used previously by a public or private entity in the issuer's Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance level, confirmed by a conformity assessment body, and steps are taken to demonstrate that the results of the earlier procedures remain valid.

    - Identity proofing and verification is based in a valid notified electronic identification means having the assurance level high.

    - Identity proofing and verification is based in a valid electronic identification means having the assurance level high, confirmed by a conformity assessment body.

      In both cases, the issuer will need to take into account the risks of a change in the person identification data and take steps to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid.

The remote procedure considered in 2.3. Technical specification ESSIF – Obtaining VC using eIDAS-AuthN can be considered legally appropriate, because is based in one of the exceptions (using a valid notified electronic identification means, or a valid non-notified electronic identification means whose equivalence has been confirmed).

Of course, during this procedure, the issuer (eventually, with the collaboration of the corresponding Member State) will have to proof all the identity attributes as needed for the purpose of use of the verifiable credential. In the case of a Verifiable ID, this include at least all the attributes in the minimum data set (see

section 4.3.7 of this report), but in the case of a different credential it may be limited to a subset of this data.

Imagine, por instance, that an issuer wants to issue a Verifiable Attestation to a subject, such as her profession. To do it without verifying the subject's identity may be a significant legal risk. One possibility would be to request the presentation of a Verifiable ID (according to the eIDAS Regulation, even a non-notified one), while another possibility would be just to apply the identify proofing procedure again.

The notion of using a notified (or non-notified) electronic identity means to remotely, cross-border) issue a new electronic identity implies, indeed, that the issuer of the Verifiable ID must connect to the corresponding eIDAS node, through the eIDAS-Connector, using the proxy or the middleware integration model. If the issuer is part of an electronic identification scheme, it will the a public authority or a private entity acting on behalf of the Member State, and therefore will be covered by the principal legal effect of the eIDAS Regulation (see section 4.4.1 of this report), but in any other case, the issuer will not necessarily have a legal right to consume the electronic identification means (see section 4.4.2 of this report). It may also happen that the Member State who owns or operates the corresponding electronic identification schemes authorises its use to private verifiable credentials' issuers but with strict limitations or by paying a fee (see section 4.4.2 of this study), preventing the development of the SSI market.

In any case, assuming the issuer is able to consume a particular user's electronic identification means according to the eIDAS Security Regulation, it will receive an assertion with the proofed identity attributes corresponding to that user (the minimum data set), with a certain level of assurance. From this perspective, the main advantage of using this approach is that the verifiable credential inherits the level of assurance of the eIDAS electronic identification information, allowing a person to get different Verifiable IDs and leveraging their use in the space of decentralised transactions, gaining real privacy.

The possibility of issuing Verifiable IDs (or other verifiable credentials) using qualified certificates as identity proofing mechanism[46] may also be considered legally feasible, using two arguments. First, if the issuer of the Verifiable ID is the qualified TSP that issued the qualified certificate, it could be covered by the exemption of reusing the identity proofing procedure applied to issue the qualified certificate, which is obviously a procedure used previously for a purpose other than the issuance of electronic identification means). Due to the strict conditions required for this process under Article 24 (1) of the eIDAS Regulation, it is highly probable that the conformity assessment body considers it equivalent with the requirements set forth in the eIDAS Security Regulation.

[46] A different possibility would be to consider a specific type of Verifiable Credential, based on a specific DID method, as an electronic signature or seal certificate, as we'll see later on.

Second, if the issuer of the Verifiable ID is not the qualified TSP that issued the qualified certificate, it could consider that the qualified certificate constitutes an authoritative source with respect of the subject's identity. This could be based on the subject producing an advanced or qualified electronic signature on the Verification ID application form. The main issue in this case is the possibility of the qualified TSP prohibiting this use, or rejecting its own liability on the grounds of an unauthorised, incompatible or abusive certificate usage. Thus, the relationship between the issuer of the Verifiable ID and the qualified TSP should be investigated on a case-per-case basis.

Independently of using an electronic identification means or a qualified certificate as part of the issuance process, the issuer must apply additional controls in the identity proofing procedure to reach level of assurance high, and also additional controls to issue the verifiable credential with an eIDAS level of assurance, as we'll see later on.

One of the most important is to ensure that the Verifiable ID is issued to the legitimate controller of a DID. This implies the need for the subject to perform two authentication procedures:

- First, an eIDAS delegated (dynamic) authentication, to recover the minimum data set; or a cryptographic authentication using her private key associated to the qualified certificate.

- Second, and only if the first authentication succeeded, a DID authentication process, to check that the person claiming DID ownership really has access to the private key used to control that DID.

If both authentication processes are correctly performed, the issuer will be able to issue the verifiable credential (as in the ESSIF proposed use case) or to derive an identity into the SSI system (as in the Qualified ID derivation concept proposed by (Abraham, Theuermann, & Kirchengast, 2018), refined in (Abraham, Hörandner, Omolola, & Ramacher, 2019), with the incorporation of Zero Knowledge Proofs.

As we'll see later, the issuer of a Verifiable Credential should be liable for issuing a Verifiable Credential with assured identity attributes, it will need to store information to defend itself in case of a legal claim. That would even be mandatory, for example, in the case of issuing Verifiable IDs to be used in the context of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, modified by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018, especially when the Verifiable ID issuer acts as a third-party on behalf of the obliged subject.

Recommendation/s:

[Recommendation 7] Develop detailed guidance for remote and presential identity proofing procedures for issuing verifiable credentials.

[Recommendation 8] Develop guidance for conformity assessment bodies, with respect to equivalent assurance confirmation, both for non-notified electronic identification means and qualified certificates.

[Recommendation 9] Develop detailed guidance for collection and storage of identity proofing material for evidential purposes.

8.2. eIDAS Bridge: increasing verifiable credentials' legal value and cross-border recognition

Description: This scenario uses qualified certificates for electronic signatures of seals to authenticate verifiable credentials with increased legal value. This case is described in 4.1. Technical specification ESSIF – eIDAS bridge for VC-eSealing[47].

Qualified certificates are regulated under articles 28 (natural persons) and 38 (legal persons) of the eIDAS Regulation, and they confirm the identity of the natural person or the legal person. They may also contain other identity attributes, such as mandates.

This scenario has been conceived as a transitory one, until a solution for managing trusted issuers completely on the SSI system, with the same legal recognition, is available.

Discussion:

The basic idea of the eIDAS Bridge is to enhance the legal certainty of any class of verifiable credential, by incorporating the issuer's advanced or qualified electronic signature (if the verifiable credential issuer is a natural person) o seal (if the verifiable credential issuer is a legal person).

As explained in section 5.4 of this report, the eIDAS Regulation defines the legal effect of qualified electronic signatures and qualified electronic seals, leaving to Member States the definition of legal effect with respect to non-qualified electronic signatures or seals.

- A qualified electronic signature shall have the equivalent legal effect of a handwritten signature (Article 25 (2) of the eIDAS Regulation). Thus, using an electronic signature will only make sense when the verifiable credentials incorporates a legal act by a natural person issuing the

[47] https://ec.europa.eu/cefdigital/wiki/display/EBP/4.1.+Technical+specification+ESSIF+-+eIDAS+bridge+for+VC-eSealing.

credential. For example, a Public Notary could issue a verifiable credential containing a notarial power of representation.

- A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked (article 35 (3) of the eIDAS Regulation). As already explained in this report, using an electronic seal in a transaction, such as issuing a verifiable credential, may need an explicit legislation authorising such a use or, the least, that this possibility does not conflict with the national legislation.

  As an example, in the Diploma use case, a University can issue a Verifiable Attestation with the diploma of a subject. Whether this verifiable credential may be issued directly by a legal person and, thus, an electronic seal can be used to authenticate it (confirming also the identity of the University) depends exclusively in national Law.

  It would be convenient to regulate the use of electronic seals for the issuance of verifiable credentials or, alternatively, create a rule in the European level, mandatory for all Member States, to allow using an electronic seal for any legal act that requires the intervention of a representative, in line, for example, with Belgian legislation.

Both in the case of the electronic signature and seal, instead of using the qualified versions thereof, it could be acceptable to use advanced electronic signatures and seals based in qualified certificates.

In all cases, the electronic certificates must be issued by a qualified TSP in compliance with the corresponding legal requirements, and the solution must comply with the legal requirements applicable to an advanced or qualified electronic signature or seal (see sections 5.2 and 5.3 of this report, respectively).

Among (many) other considerations, key management is particularly relevant, as the solution could make use of different keys: one possibility could be to use the DID control key; another one, to generate a key pair specifically for this electronic signature or seal creation (this second possibility has been adopted in the project). If the key pair used to sign or seal is to be managed by a third party, for instance because a server wallet or another remote signature/seal is used, then it is necessary to comply with the legal restrictions set forth by the eIDAS Regulation, at least with respect to qualified electronic signatures and seals, including the usage of qualified remote signature/seal creation devices managed by qualified trust service providers (with respect to this problematic, see section 10.4 of this report).

From a technical perspective, this electronic signature or seal is attached to the verifiable credential in form of a linked data signature, a special class of a linked data proof, according to a specific syntax[48]. This format is currently not included

[48] See https://w3c-ccg.github.io/ld-proofs/#linked-data-signatures.

in the eIDAS AdES Formats Decision, but it could be considered as another format if the conditions of Article 2 are met, thus benefiting from the legal effect defined in Article 27 and 37 of the eIDAS Regulation, when used verifiable credentials in the context of public procedures. Thus, it would be convenient to set specific guidance for ensuring compliance to the requirements set forth in the said Decision.

In any case, this linked data proof is verified using the issuer's qualified certificate; which must be resolvable and accessible to any relying party. To this end, the DID document of the issuer is updated with information to identify an online repository where the certificate is published (called an identity hub), and also a new attribute asserting the level of assurance of the key[49].

Any person receiving a verifiable credential is able to lookup the DID, and then resolve the DID to get the DID Document; with the DID document, it is possible to access the qualified certificate contained in this repository.

Moreover, this technique allows any person to lookup for any DID and recover a qualified certificate associated with it, thus confirming the identity of the subject owning that DID (this is a re-identification technique). In the case of natural persons acting as verifiable credentials issuers, this could generate privacy issues, and could be considered against the very SSI principles. In the current version of EBSI, only electronic seals are used, but it will be a need to allow natural persons issuers. To do it in alignment with GDPR, we anticipate the need to design and implement access restrictions to identity hubs storing qualified certificates (see section 10.3 of this report).

The main benefit of this approach is that using qualified certificates in support of qualified electronic signatures or seals provide legal confirmation of identity and a legal basis for attributing a verifiable credential to an issuer leveraging the current eIDAS Regulation, which right now is technically developed around hierarchical PKI.

While it is true that the legal semantics of this authentication may vary depending of the verifiable credential subclass, there is a common legal ground to all electronic signature and seal that increases the trustworthiness of any signed or sealed document.

But it does not provide any confirmation of authority to issue a particular claim with respect to a subject, so additional measures are needed to this end, for each type of verifiable credential subclass: the main measure is to create a trusted issuer mechanism (see sections 9.1 and 10.1 of this report, with respect to Verifiable IDs and Verifiable Attestations, respectively).

49

While this trusted issuer mechanism is not fully developed, a possibility could be to incorporate this information in the qualified certificate, in form of a set of attributes.

Recommendation/s:

[Recommendation 10] Regulate the use of electronic seals for the issuance of verifiable credentials or, alternatively, create a rule in the European level, mandatory for all Member States, to allow using an electronic seal for any legal act that requires the intervention of a representative, in line, for example, with Belgian legislation.

[Recommendation 11] To extend the eIDAS concept to natural persons issuing verifiable credentials, the use of identity hubs with proper access controls, under the self-management of the subject, should be made mandatory.

[Recommendation 12] Consider authorising at the European level the use of advanced electronic signatures and seals based in qualified certificates for the authentication of verifiable credentials, to facilitate the early adoption of SSI.

[Recommendation 13] Develop detailed guidance, according to Article 2 of the eIDAS AdES Formats Decision, to ensure that Linked Data Signatures used for signing or sealing verifiable credentials are mandatorily recognised by Member States, in the context of Articles 27 and 37 of the eIDAS Regulation.

8.3. Use current eID nodes to issue a SAML assertion based in verifiable credentials/presentations

Description: This scenario considers the possibility to incorporate, to a current regular eIDAS node, the capability to accept verifiable presentations as a form of user authentication. It is a transitory scenario, whilst the scenario described in section 9.1 is not implemented.

Discussion:

This scenario is interesting as a kind of “fast-track” procedure for the interoperable adoption of the SSI technology in relations with public sector bodies, but it does not leverage the innovations and privacy enhancements of SSI technologies.

The DID method should adopt a minimal set of requirements related to the DID control mechanism, to ensure its alignment with the eIDAS Security Regulation, and the verifiable credential/verifiable presentation should include the minimum data set as per eIDAS Interoperability Regulation.

These requirements are developed in sections 8.1 and 9.1 of this report, to which we refer to avoid redundancy.

The scenario may be valuable to start exploring the application of the eIDAS provisions to an SSI solution, especially the eIDAS Security Regulation and the different models of verifiable presentations that can be applied to represent the minimum data set mandated by the eIDAS Interoperability Regulation in real cross-border transactions; while reducing the operational exposure of the eIDAS network.

The protocol for the communication in the network of eIDAS identification nodes would not change, and the assertion issued by the node would be fully conformant with the current eIDAS technical specifications, just as with other authentication mechanisms. Thus, this scenario would allow Member States to notify real SSI solutions, used in their Member States, to be used for accessing (at least) pubic services in other Member States, by using the currently implemented network.

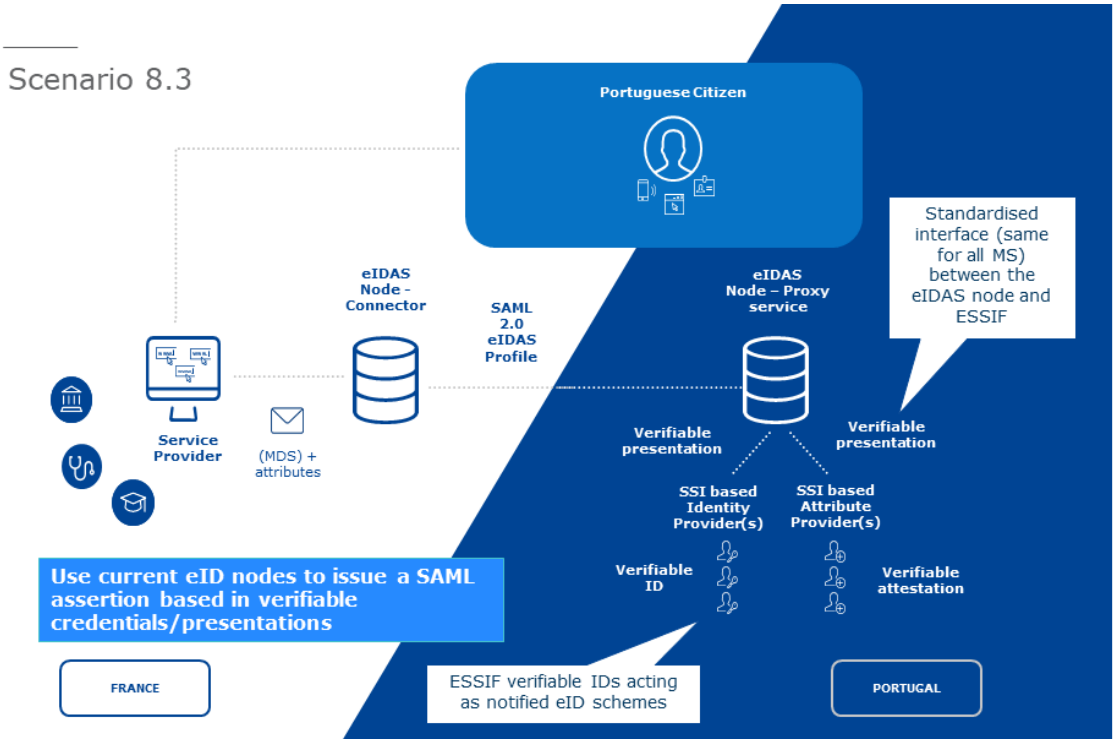

Figure 15. Use current eID nodes to issue a SAML assertion based in verifiable credentials/presentations

It would be convenient, to foster the adoption of this scenario, the intervention of the eIDAS Cooperation Network.

Recommendation/s:

[Recommendation 14] Produce specific additional guidance for the assessment of how notified electronic identification means using SSI-based verifiable presentations with the current eIDAS eID profiles meet eIDAS interoperability and security requirements.

9. LEGAL ASSESSMENT OF SHORT-TERM SCENARIOS

9.1. Use of Verifiable IDs as eIDAS electronic identification means

Description: eIDAS is considered an appropriate regulatory framework to embody specific SSI systems, such as EBSI ESSIF Verifiable IDs proposal, aligned with assurance level substantial (or high, depending on the user device and setup).

Although electronic identification under eIDAS Regulation is today clearly aligned with federated identity management (SAML-based) infrastructures, nothing in the eIDAS or its implementing acts should prevent the usage of an SSI system as an electronic identification means from end to end.

Thus, this scenario considers a Verifiable ID as an eIDAS compliant electronic identification means, enabling –at least– transactions with public sector bodies and Public Administrations and, if so decided by issuers in the framework of the notified electronic identification scheme, also with private sector entities, for AML/CFT and other uses.

Discussion:

As discussed in section 7.1 of this report, the legal value of a Verifiable ID depends on the legal framework applicable to its issuance, including any condition applicable to the issuer and to the process.

As already introduced (see section 4 of this report), the eIDAS Regulation constitutes a very relevant legal framework for the admissibility and usage of electronic identification means in the context of public sector bodies procedures, but it is limited to cross-border scenarios, and does not regulate the domestic legal value of any electronic identification means. In any case, it is interesting to evaluate if the Verifiable ID proposed in EBSI ESSIF can be considered as an electronic identification system under eIDAS (as explained in section 4.1 of this report), to benefit from the recognition legal effect regulated in Article 6 of the eIDAS Regulation.

This system is formed by a technical and organisational architecture, including a DLT system, a wallet and a collection of server applications, communication services, external database providers, etc. As artefacts or components of the electronic identification means, we must cite the DID and its DID Document and the Verifiable ID and its corresponding verifiable presentation.

The pair DID-Verifiable Presentation (containing a Verifiable ID) could be considered as the “electronic identification means” (article 3 (2) of the eIDAS Regulation defines it as “a material and/or immaterial unit containing person identification data and which is used for authentication for an online service”).

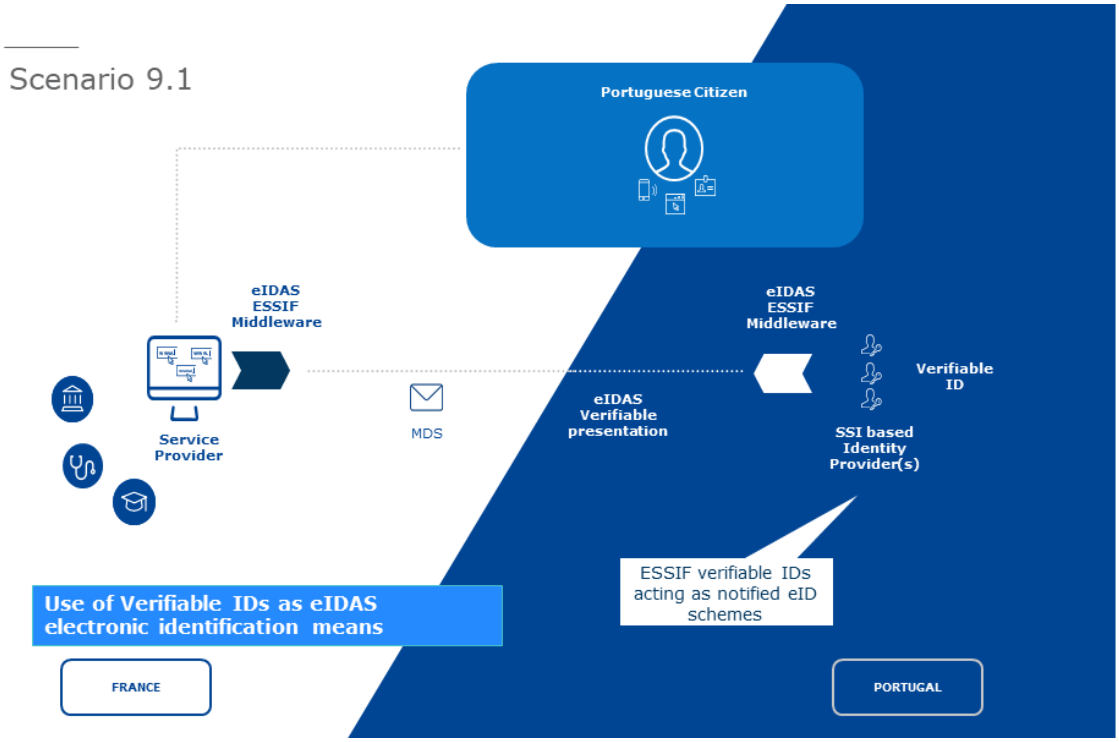

Figure 16. Use of Verifiable IDs as eIDAS electronic identification means

The DID referenced in the Verifiable ID is used for authentication (as defined in Article 3 (5) of the eIDAS Regulation), by using the private key controlling the DID, and then producing a Verifiable Presentation, to be shared with the relying party using an Identity Hub.

In fact, that means we must evaluate if EBSI ESSIF Verifiable IDs fulfil the eligibility criteria for notification of electronic identification schemes regulated in Article 7 of the eIDAS Regulation (for an explanation of the different eligibility criteria, refer to section 4.3 of this report), and some additional legal obligations:

Requirement	Evaluation
Article 7 (a)	A Verifiable ID issued by a Member State, under a mandate of the Member State or independently of a Member State but recognised by that Member State, would qualify as an electronic identification mean to be notified (see section 4.3.1 of this report).
Article 7 (b)	To be notifiable, a Verifiable ID must be previously admitted to access at least one service which is provided by a public sector body and which requires electronic identification in the notifying Member State (see section 4.3.2 of this report).

Requirement	Evaluation
Article 7 (c)	The EBSI ESSIF scheme must comply with the security measures (see section 4.3.3 of this report, and specific analysis below).
Article 7 (d) and (e)	For a Verifiable ID to be notifiable, the notifying State must ensure the exclusive attribution of person identification data to the credential subject, in accordance to the eIDAS Security Regulation; and the issuer of the Verifiable ID must ensure its exclusive attribution to the credential subject, also in accordance to the eIDAS Security Regulation (see section of this report). Regarding the security measures, see the specific analysis below.
Article 7 (f)	For a Verifiable ID to be eligible for notification, the notifying State must ensure ensures the availability of authentication online, so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form (see section 4.3.5 of this report). It is possible, in our opinion, to comply with this requirement for an SSI solution taking the middleware to middleware approach currently used in the installed eIDAS infrastructure. Of course, it will be needed to define the corresponding technical specifications, aligned with the eIDAS Interoperability Regulation.
Article 7 (g)	This requirement does not present significant particularities regarding SSI schemes (section 4.3.6 of this report), except for the need to adapt the current instruments used in the pre-notification process.
Article 7 (h)	The EBSI ESSIF scheme must comply with the interoperable requirements of Article 12 (1) of the eIDAS Regulation (see section 4.3.7 of this report). It is anticipated that there will be a need to approve specific interoperability specifications in support of EBSI ESSIF, alongside with the current SAML-based eID specifications. These new specifications should be used for the implementation and testing of SSI solutions, at least in two Member States, and the approved by the competent bodies, including the Cooperation Network and the Commission.

As noted, the SSI solution must ensure compliance with eIDAS Security Regulation. We will assume that the minimum acceptable level of assurance for a Verifiable ID (or another verifiable credential) is substantial. Some of the requirements are evaluated in the following table:

Section	Evaluation
§ 2.1	See section 8.1 of this report.
§ 2.2.1	The wallet managing the keys controlling the subject's DID implements at least two authentication factors from different categories, and is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs. This requirement also applies in case of a remotely managed wallet (see section 10.4 of this report), by applying the same protection measures that are used for advanced electronic signatures. Additionally, for level of assurance high, the Verifiable ID implements protections against duplication and tampering as well as against attackers with high attack potential. This feature may be based in the eIDAS Bridge for eSealing the verifiable credential (see section 8.2 of this report). Also, for level of assurance high, the Verifiable ID is designed so that it can be reliably protected by the person to whom it belongs against use by others. To this end, the wallet must implement security measures granting sole control of the DID-controlling keys. This requirement also applies in case of a remotely managed wallet (see section 10.4 of this report), by applying the same protection measures that are used for qualified electronic signatures.
§ 2.2.2	After issuance, the Verifiable ID is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs. For level of assurance high, the activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs. In both cases, the requirements are referred to the DID and its corresponding keys, with respect to their binding to a specific subject. Thus, this measure is associated with

Section	Evaluation
	the identity proofing mechanism introduced in section 8.1 of this report.
§ 2.2.3	The possibility of suspending or revoking an electronic identification means can be implemented with respect to the verifiable credential. The fact that the issuer cannot suspend or revoke the subject's DID seems irrelevant from a legal perspective. The issuer may adopt measures to prevent unauthorised suspension, revocation and/or reactivation. The issuer may adopt measures to ensure that reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met.
§ 2.2.4	The issuer must ensure that, taking into account the risks of a change in the person identification data, renewal or replacement meets the same assurance requirements as initial identity proofing and verification or is based on a valid electronic identification means of the same, or higher, assurance level. Additionally, for level of assurance high, where renewal or replacement is based on a valid electronic identification means, the identity data is verified with an authoritative source. These measures are associated with the identity proofing mechanism introduced in section 8.1 of this report.
§ 2.3.1	The release of person identification data (that is, transmitting the minimum data set to the relying party) must be preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication. This requirement may be fulfilled by using the DID control key in the authentication process, before sending or giving access to the verifiable presentation containing the Verifiable ID. Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline. This requirement may be fulfilled implementing the proper controls in the Identity Hub used for giving access to the verifiable presentation (see section 10.3 of this report).

Section	Evaluation
	The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms (in the case of level of assurance high, the attacker will have a high attack potential). This control may be fulfilled by using string cryptographic algorithms for DIDs keys, communication protocols used for DID authentication, Verifiable ID protection, such as by its sealing (see section 8.2 of this report), and communications and access controls with the Identity Hub (see section 10.3 of this report).

A novel approach, which could be better aligned with the SSI principles, would be to design a special type of a verifiable presentation transporting a set of verifiable credentials, or using verifiable credentials that support selective disclosure (i.e. based in partially blinded signtures).

In the first case, instead of including the Minimum Data Set in a verifiable credential (currently called Verifiable ID), a subject could receive a set of verifiable credentials with different identity attributes (e.g., a verifiable credential with the first name, a different verifiable credential with surname/s, a different verifiable credential with the birth date, etc.). When required to access an electronic service in a different Member State, the subject would create a verifiable presentation containing at least all verifiable credentials needed to share the Minimum Data Set, plus any other verifiable credential related to additional data. This verifiable presentation would be standardised as a "Verifiable Presentation for eIDAS authentication".

The advantage of this approach is that it allows reusing the verifiable credentials for other use cases, that simply do not require the subject to disclose so much personal information. This approach could be considered more aligned with the SSI principles, although a similar result can be achieved by implementing ZKP techniques.

Following the SSI logic, strongly attained to the fact that "identity is contextual" (see section 1 of this report), a well-designed scheme should allow different verifiable credentials' issuers, even if it increases complexity.

Thus, for the definition of our "Verifiable Presentation for eIDAS authentication" we could consider the following cases:

- A single verifiable credential with all the minimum data set, issued by an IdP. This is the current case in EBSI ESSIF v1.

- A set of verifiable credentials with subsets of identity attributes, that collectively assert all the minimum data set, issued by an IdP.

- A set of verifiable credentials with subsets of identity attributes, that collectively assert all the minimum data set, issued by different IdPs.

Finally, 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, potentially 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.

Recommendation/s:

[Recommendation 15] Define and approve new technical specifications for eIDAS eID SSI profile based in SSI-based verifiable presentations, according to Article 12 of the eIDAS Interoperability Regulation.

[Recommendation 16] Produce specific additional guidance for the assessment of how notified electronic identification means using SSI-based verifiable presentations with the new eIDAS eID SSI profile meet eIDAS interoperability and security requirements.

[Recommendation 17] Extend the notification procedure to include the trusted issuers ledger management.

[Recommendation 18] Consider the design of a "Verifiable Presentation for eIDAS authentication", that combines a set of verifiable credentials to present the Minimum Data Set to relying parties; considering the participation of one or multiple issuers.

9.2. Issuance of qualified certificates based on a specific DID method and verifiable credential

Description: This scenario considers the possibility to consider a specific DID method plus a specific type of verifiable credential as a "qualified certificate", both for natural and for legal persons, based on a technologically neutral, wide,

interpretation of the eIDAS Regulation (more specifically, of the "certificate" definition).

As qualified certificates confirm the identity of the subject (signatory or seal creator), this specific combination of a DID method and a verifiable credential would benefit from the legal effect defined for qualified certificates, and would also support advanced and qualified signatures and advanced qualified electronic seals in blockchain transactions.

This type of credential would also qualify as a Verifiable ID, when including the minimum data set.

Moreover, this approach would facilitate transitioning from PKI to DPKI and SSI systems, while maintaining and even fostering a valuable market and reusing a convenient and proven supervisory and liability regime.

Discussion:

As explained in section 6.3 of this report, a "'certificate for electronic signature' means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person". A similar definition exists for certificate for electronic seal.

Essentially, the eIDAS Regulations refers to a public key certificate, that binds a public key with a name and other relevant attributes. Annex I of the eIDAS Regulation contain the mandatory attributes for a certificate.

The following table maps an electronic signature certificate required contents with the SSI artefact where each information should be contained:

Content requirement	Artefact
An indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature.	Subject's verifiable credential
A set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and:	Issuer's verifiable credential, accessible in the identity hub[50].

[50] The subject's verifiable credential contains the issuer's DID. By resolving the issuer's DID it is possible to get the issuer's DID document, that contains the URL of the identity hub.

Content requirement	Artefact
- for a legal person: the name and, where applicable, registration number as stated in the official records, - for a natural person: the person's name.	
At least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated.	Subject's verifiable credential
Electronic signature validation data that corresponds to the electronic signature creation data.	Subject's DID document
Details of the beginning and end of the certificate's period of validity.	Subject's verifiable credential
The certificate identity code, which must be unique for the qualified trust service provider.	Subject's verifiable credential
The advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider.	Subject's verifiable credential
The location where the certificate supporting the advanced electronic signature or advanced electronic seal (of the issuing qualified trust service provider) is available free of charge.	Issuer's DID document, pointing to the issuer's identity hub
The location of the services that can be used to enquire about the validity status of the qualified certificate	Subject's DID document
Where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing	Subject's DID document

What most closely resembles a traditional public key certificate is a DID document that associates a public key with a subject. In the current eIDAS, it could be argued that this concept can only be assimilated if the DID private control key is used to sign or create stamps, or to authenticate websites.

The current definition of certificate refers to "an attestation". If understood as a single file, a X.509 certificate fits perfectly well in the definition (unsurprisingly…) but it may prevent the use of the SSI model, where we have decentralised public key infrastructure supported by the DID controlled by the private key corresponding to the public key declared in the DID document, and the identity data contained in a verifiable credential specifically designed for this purpose.

On the contrary, if we read the eIDAS Regulation from a purely technologically neutral view, an attestation could be interpreted as two or more bounded different files. The idea is that a qualified certificate, in this view, would be an attestation composed of (1) a subject's DID Document, (2) an issuer's DID Document, (3) an issuer's Verifiable ID and (4) a subject's verifiable ID.

This verifiable credential could be designated as a "SSI eIDAS qualified certificate", to differentiate it from PKI eIDAS qualified certificates.

The subject's DID method should define all details with respect to key management. One possibility could be to reuse the DID control key to sign, while another possibility would be to use a different key pair, specifically for electronic or seal signature, like in the eIDAS Bridge (see section 9.2 of this report). As the a DID document may be updated by a party different from the subject, duly authorised, the qualified TSP issuing the SSI eIDAS qualified certificate could grant the signature or seal validation data.

Additionally, the DID method should define specific attributes to register the quality of the signature or seal key, as the qualified TSP need to know this information when issuing the verifiable attestation. Depending on the implementation, this information should be generated by the wallet, according to the security environment or by the TSP, in case the key is created and managed remotely (see section 10.4 of this report).

Obviously, if the keys are managed using a qualified (even remote) electronic signature or seal creation device, the SSI eIDAS qualified certificate will support qualified signatures or seals.

Also, if the SSI eIDAS qualified certificate contain the Minimum Data Set, it will be also eligible for notification as an electronic identification means (see section 9.1 of this report).

One of the major innovations of SSI consists in DPKI. According to (Reed & Slepak, 2015), "the goal of DPKI is to ensure that, unlike PKIX, no single third-party can compromise the integrity and security of the system as whole", because "trust is decentralized through the use of technologies that make it possible for geographically and politically disparate entities to reach consensus on the state of a shared database". Thus, for these authors, "DPKI focuses primarily on decentralized key-value datastores, called blockchains, but it is perfectly capable of supporting other technologies that provide similar or superior security properties".

With DPKI, traditional cryptographic trust anchors are transformed. As explained in the TADIM Report (Alamillo Domingo & Curry, 2019), IETF has extensive experience in the treatment of cryptographic trust anchors, especially in PKI. IETF RFC 5280, the Internet X.509v3 profile technical specification for the Internet, refers to trust anchors in the context of the validation of certification paths, as part of the certification validation procedure, but it does not define what a trust anchor is. According to IETF RFC 5914 (Trust Anchor Format), "a trust anchor is an authoritative entity represented by a public key and associated data. The public key is used to verify digital signatures, and the associated data is used to constrain the types of information or actions for which the trust anchor is authoritative".

Moreover, according to IETF RFC 5934 (Trust Anchor Management Protocol – TAMP), "a trust anchor contains a public key that is used to validate digital signatures". This specification differentiates three types of trust anchors: apex trust anchors, management trust anchors and identity trust anchors. The latter "are used to validate certification paths, and they represent the trust anchor for a public key infrastructure", being "most often used in the validation of certificates associated with non-management applications". IETF RFC 6024 states that "a trust anchor represents an authoritative entity via a public key and associated data. The public key is used to verify digital signatures, and the associated data is used to constrain the types of information for which the trust anchor is authoritative. A relying party uses trust anchors to determine if a digitally signed object is valid by verifying a digital signature using the trust anchor's public key, and by enforcing the constraints expressed in the associated data for the trust anchor".

In the IETF model, trust anchors are used as "roots" of hierarchical PKIs, thus supporting chains of trust: i.e. an end-entity digital signature is verified with the end-entity's public key included in a certificate signed by a Subordinate Certification Authority (CA); the Subordinate CA signature is verified with the Subordinate CA's public key included in a certificate issued by a Root CA; this Root public key is a typical example of a Trust Anchor.

Trust anchor collections may be, and usually are, represented by a Trust Anchor List, conforming to the syntax defined in IETF RFC 5914, with the aim i.e. to publish them to applications (trust anchor stores) used by relying parties when validating a digital signature. This Trust Anchor List is typically signed to protect and authenticate the information contained within. In many cases, trust stores as those provided by browsers.

One possibility could be to adapt this notion, which was created in the context of hierarchical PKIs to the specificities of a Decentralised PKI. As SSI is based on DPKI, each user is her own root of trust; therefore, cryptographic trust anchor stores are substituted by the DLT implementing the DPKI.

In the trust services regulatory framework explained in section 6.2 of this report, the eIDAS Regulation use the concept of a Trusted List –an XML according to a XSD vocabulary– to publish the trust points (such as Root CA self-signed certificates), also known as service digital identifiers. Note that the Trusted List

for each Member State is periodically issued by the corresponding supervisory body.

It would be needed to adapt this Trusted List model to the SSI world, by implementing this mechanism by using a Trusted Issuer Ledger, storing information about trusted issuers[51], without the need for a chain of trust[52].

The ledger governance rules should consider the possibility of managing the lifecycle of qualified trust services by supervisory bodies. In a first moment, the trusted issuer ledger would not substitute the trusted list, but complement it. To transform the scheme, Article 22 of the eIDAS Regulation should be modified, and of course, the eIDAS TL Decision should be withdrawn.

Implementing this proposal technically and legally would allow to deploy a fully comprehensive SSI scheme, both for identification and signing/sealing, even for qualified electronic signatures and seals.

Recommendation/s:

[Recommendation 19] Promote a common interpretation of the certificate definition, in the sense of understanding the expression "an attestation" may be referred to the combination of a verifiable credential and one or more DID documents ("SSI eIDAS qualified certificate").

[Recommendation 20] Provide guidance for the definition of DID methods for the issuance and lifecycle of SSI eIDAS qualified certificates including those to be also admitted as Verifiable IDs.

[Recommendation 21] Develop a governance framework for a trusted issuers ledger for qualified trust service providers, considering the possibility of managing the lifecycle of qualified trust services by supervisory bodies of Member States.

[Recommendation 22] Modify Article 22 of the eIDAS Regulation and withdraw Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists.

[51] See 4.3. Technical specification ESSIF - Description of Trusted Issuer Referential/Ledger (https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=167937331).

[52] This is already the case for several trust services different from issuing certificates, such as qualified electronic registered delivery service, which is represented in the Trusted List as an end-entity X.509v3 certificate (usually a certificate for electronic seal). In this case, the Trusted List is not needed for establishing a chain of trust, as happens with a hierarchical PKI.

10. LEGAL ASSESSMENT OF MID- TO LONG-TERM SCENARIOS

10.1. Extend the eIDAS notification mechanism to Verifiable Attestations: enhanced Trusted Issuers management

Description: This scenario presents the opportunity to extend Chapter II of the eIDAS Regulation to schemes for the self-managed sharing of identity attributes (e.g. ESSIF Verifiable Attestations), leveraging the legal infrastructure to create a general, abstract, framework for this process. Sectorial legal norms would define the rules associated to the content (thus fostering the reusable building block concept).

Discussion:

As discussed in section 4 of this report, eIDAS constitutes a common legal framework for electronic authentication in a cross-border transaction, providing a trust framework for federated identity management that can be easily adapted to SSI (see sections 8.1, 8.3 and 9.1 of this report), by defining verifiable credentials/presentations specialised in identification, such as EBSI ESSIF Verifiable IDs.

eIDAS does not cover identity management in a wide sense, but just electronic identification. Thus, it is not immediately applicable to the issuance and sharing of other verifiable credentials/presentations (EBSI ESSIF Verifiable Attestations). This is reasonable from the perspective of the legal regime of the content of these credentials (e.g. a diploma), but it makes difficult using them in a cross-border scenario, because of the existence of multiple, sectoral, regulations.

One possibility to solve this problem is to extend the legal approach and governance rules already existing in the eIDAS Regulation, to regulate a general framework for the lifecycle of verifiable credentials/presentations used for purposes different to electronic authentication.

The current legal approach in the eIDAS Regulation is very concrete and detailed: it contains legal definitions related to electronic identification (electronic identification scheme, electronic identification means, personal identification data) and authentication; defines processes, levels of assurance, interoperability and governance rules. In short, a full legal trust framework for cross-border authentication, an important part of identity management.

Our proposal, in this scenario, is to create a parallel trust framework for issuing and sharing other identity attributes. This objective cannot be accomplished in the same way as the current approach for electronic identification, because the semantics and rules of these other identity attributes are quite different. Although they identify a person, in a very wide sense, they are not used for identification and authentication.

Let's take the EBSI v1 User Journey as an example[53], that considers the issuance of Bachelor and Master Diplomas, in form of Verifiable Attestations. In the first case, the subject (in the user journey, she's called Eva) onboards (getting a Verifiable ID from the Federal government of Belgium) and gets a Bachelor diploma (a Verifiable Attestation issued by the competent authority, which in this specific case is the regional government of Flanders). When she applies to a Spanish university, she's requested to produce a verifiable presentation that includes her Verifiable ID, the Verifiable Attestation of the Diploma and specific data related to this verifiable presentation (its purpose, including GDPR and other terms & conditions acceptance).

As seen, when Eva is requested by the Spanish university to produce and share (directly or by giving access to her identity hub[54]) a verifiable attestation, she's authenticating herself by presenting a strict electronic identification means (in form of a Verifiable ID issued by the competent authority) but also a very relevant additional information as the Bachelor diploma (in form of a Verifiable Attestation issued by the competent authority).

While the eIDAS Regulation provides a strong legal framework with respect to the part of this authentication process enabled by the electronic identification means, it does no regulate at all the other part of this authentication process, consisting in presenting the Diploma.

It could be argued that there is no need for a regulation dealing with presenting attestations, because there already exists sectoral legislation that covers the legal value and legal effects of the credentials. Such is the case of Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications, which "establishes rules according to which a Member State which makes access to or pursuit of a regulated profession in its territory contingent upon possession of specific professional qualifications (referred to hereinafter as the host Member State) shall recognise professional qualifications obtained in one or more other Member States (referred to hereinafter as the home Member State) and which allow the holder of the said qualifications to pursue the same profession there, for access to and pursuit of that profession", and also "establishes rules concerning partial access to a regulated profession and recognition of professional traineeships pursued in another Member State" (a novelty included by Directive 2013/55/EU of the European Parliament and of the Council of 20 November 2013 amending Directive 2005/36/EC on the recognition of professional qualifications and Regulation (EU) No 1024/2012

[53] Scope of EBSI v1: Eva´s User Journey, available at https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=150471697.

[54] 4.4. Technical specification ESSIF - Identity Hub, available at https://ec.europa.eu/cefdigital/wiki/display/EBP/4.4.+Technical+specification+ESSIF+-+Identity+Hub. See also section 10.3 of this report.

on administrative cooperation through the Internal Market Information System ('the IMI Regulation')).

According to Article 2 (2) of Directive 2005/36/EC, "each Member State may permit Member State nationals in possession of evidence of professional qualifications not obtained in a Member State to pursue a regulated profession within the meaning of Article 3 (1) (a) on its territory in accordance with its rules". Other possibilities exist, but this general case is enough for our example.

Article 3 (b) of the same Directive defines 'professional qualifications', as "qualifications attested by evidence of formal qualifications, an attestation of competence referred to in Article 11, point (a) (i) and/or professional experience", while number (c) defines 'evidence of formal qualifications' as "diplomas, certificates and other evidence issued by an authority in a Member State designated pursuant to legislative, regulatory or administrative provisions of that Member State and certifying successful completion of professional training obtained mainly in the Community". Again, other possibilities are considered in this legal instrument, but we don't need to analyse them to our ends.

Evidence of professional qualifications is required with respect to the declaration to be made in advance, if the service provider first moves from one Member State to another in order to provide services (Article 7), for instance.

In this sense, Article 13 (1) second paragraph of Directive 2005/36/EC says that "attestations of competence or evidence of formal qualifications shall be issued by a competent authority in a Member State, designated in accordance with the laws, regulations or administrative provisions of that Member State". In some cases, more than one document is needed, such as in the case of Article 21 (1) of the same Directive, according to which, "each Member State shall recognise evidence of formal qualifications as doctor giving access to the professional activities of doctor with basic training and specialised doctor, as nurse responsible for general care, as dental practitioner, as specialised dental practitioner, as veterinary surgeon, as pharmacist and as architect […] and shall, for the purposes of access to and pursuit of the professional activities, give such evidence the same effect on its territory as the evidence of formal qualifications which it itself issues", adding that "such evidence of formal qualifications must be issued by the competent bodies in the Member States and accompanied, where appropriate, by the certificates listed in […]".

As seen, whether a Verifiable Attestation is an evidence of professional qualifications depend on the Law applicable to the issuance of the corresponding document. This means that national law must authorise or, at

least, not prevent the use of a Verifiable Attestation as a valid evidence of professional qualification.

For instance, according to Spanish Royal Decree 1002/2010, of 5th August, on issuance of official university diplomas, mandates that the original diploma is exclusively issued following certain specifications regarding its text, format and procedure set forth in the regulation. It is worth noting several potential issues for transforming these diplomas into Verifiable Attestations:

- Official university diplomas are valid in the national territory (Article 3 (3); and Article 4 of Royal Decree 1393/2007, of 29th October). Does it mean they don't have legal effect in a cross-border transaction? Clearly, that would be against Directive 2005/36/EC, and their usage it is not being limited.

- Official university diplomas must be produced in a special paper support (Article 16). There's no possibility of issuing an official university diploma in electronic support.

- Official university diplomas must be issued by the University Rector. In a strict interpretation, this means the personal signature of the Rector, although in practice the full printing process is automated.

Universities may issue the Diploma supplement, both in paper support (Article 5 of the Royal Decree 22/2015, of 23rd of January) and in electronic support (Article 6 of the same regulation). In the latter case the Diploma supplement will be available in the University website. Its purpose is to "provide sufficient independent data to improve the international transparency and fair academic and professional recognition of qualifications (diplomas, degrees, certificates etc.). It is designed to provide a description of the nature, level, context, content and status of the studies that were pursued and successfully completed by the individual named on the original qualification to which this supplement is appended". This document could be more easily issued in form of a Verifiable Attestation, but it does not substitute the diploma itself.

Article 4 of Royal Decree 1002/2010 regulates the National Registry of Official University Graduates, in which the official university diplomas are registered prior to their issuance. This public, administrative, register provides access to the diploma's information contained therein, in accordance to the transparency legislation applicable in Spain. A certification issued by the register would have the same legal effect as presenting an electronic, authentic, copy of the diploma itself.

This simple example shows the complexity of transforming the classical certifying documents normally issued by Public Administration. To facilitate a quick transformation into Verifiable Attestations, a new equivalence rule could be proposed, in the sense of authorising the use of a Verifiable Attestation according to the (new) eIDAS Regulation whenever a legal norm requires a document certifying an identity attribute for a natural or a legal person.

As explained in the eIDAS Bridge, the use of electronic seals should be authorised in those cases where a signature is requested, for the sole purposes of the electronic form of this credential.

From another perspective, with respect to the competent authorities, following again our example (partially), Annex V to Directive 2005/36/EC contains lists of the evidence of formal qualifications of doctors of medicine, nurses responsible for general care, dental practitioners, veterinary surgeons, midwives, pharmacists and architects. This list is updated following notifications from Member States of amendments to their legislative, regulatory and administrative provisions on the issuing of evidence of the formal qualifications in question, when the Commission considers that the amended provisions comply with the conditions set out in Title III, Chapter III of Directive 2005/36/EC.

Thus, this list contains relevant information for determining the public or private entities with authority to issue the corresponding documents. Thus, they should be recognised as trusted issuers of the pertinent Verifiable Attestations, while the Commission should act as the manager of the lifecycle of these trusted issuers, in accordance with the ledger governance rules. Note that the trusted issuers ledger would only reflect the authoritative information from the Annex, instead of substituting it. This process would support, as in the case of Verifiable IDs, the "notification procedure" currently in place for electronic identification means. This procedure should be maintained to ensure that "notified" Verifiable Attestations have been properly managed as they will be admissible in cross-border public sector transactions, at the least.

As can easily be imagined, the complexity of creating a scheme for the issuance, deliverance and sharing of each set of identity attributes regulated under sectoral legislation might be an enormous task. While there may be important differences regarding the number of attributes and their syntax and semantics, it is nonetheless the truth that Verifiable Attestations could be standard scheme for these identity management process.

- Verifiable Attestations can be a common format for containing arbitrary sets of attributes, thanks to a minimum set of properties that identified issuers, subjects, dates of validity, etc.

- By using the eIDAS Bridge[55], Verifiable Attestations can be legally authenticated by using electronic seals or, when needed, electronic signatures.

- The existence of an enhanced trusted issuers ledger provides an easy way to decide which Verifiable Attestations may be trusted, without the need to understand the enormous complexity of determining who is authorised to issue a specific credential. If a specific credential is issued

[55] Initial

by a body registered in the trusted issuer ledger, it can be trusted without the need to perform any more checks.

- Verifiable Attestations may incorporate a common set of processes, such as issuance, revocation, access or sharing with third parties that facilitates the transformation of the current documents that certify identity attributes to legally valid credentials, enabled for cross-border procedures with anyone.

- Verifiable Attestations may incorporate a common, baseline, logic with respect to any set of identity attributes contained therein, in terms of legal acts. At least there should be Verifiable Attestations that legally certify the identity attributes and others that declare data with a lower level of legal guarantees, depending on the legal powers of the issuer.

- Verifiable Attestations may be combined with Verifiable IDs to form specific verifiable presentations crafted for particular procedures, both for public sector bodies and for private companies, without the need to centralise the information in data siloes, reducing GDPR management complexity and risk.

- Verifiable Attestations eligible for notification would also include those issued by qualified trust service providers (see scenario 10.2).

These conditions would allow to extend the existing trust framework embodied in the eIDAS Regulation for electronic identification, to regulate a common framework for identity data sharing under the control of natural or legal persons, sustained by a ledger conceived as a public good.

This new regulatory approach would also support the new data sharing economy, and a better compliance with GDPR. It would also complement The Once Only Principle by facilitating the identity attributes sharing between public authentic sources and private sector parties, due to its self-sovereign foundational design.

It would be convenient to establish a legal effect for this service, to ensure the legal validity and acceptance of these Verifiable Attestations. As explained in section 7.1 of this report, verifiable credential are electronic documents and, as such, they already benefit from the non-discrimination rule set forth by Article 46 of the eIDAS Regulation, but attaining a specific legal semantics to these credentials would increase their value for real transactions.

Also, following the current approach of eIDAS Regulation with respect to notified electronic identification means (including those that are based in qualified certificates), notified Verifiable Attestations should be mandatorily admitted by Member States public sector bodies.

Recommendation/s:

[Recommendation 23] Propose modifying Chapter II of the eIDAS Regulation with the necessary Articles to extend the existing trust framework embodied in the eIDAS Regulation for electronic identification, to include a common framework for identity data sharing under the control of natural or legal persons, sustained by a ledger conceived as a public good.

[Recommendation 24] Create a legal rule, based in the equivalence principle, to authorising the use of a Verifiable Attestation according to the (new) eIDAS Regulation whenever a legal norm requires the presentation of a document certifying a natural or a legal person identity attribute.

[Recommendation 25] Member States should be mandated to admit notified Verifiable Attestations, substituting the paper or electronic documents (such as diplomas) containing the identity attributes.

[Recommendation 26] Create a specific legal rule authorising the use of an advanced or qualified electronic seal for the issuance of Verifiable Attestations, whenever the Law applicable to the form of the document mandates the use of a signature.

[Recommendation 27] Define a governance framework for a trusted issuers ledger providing verifiable attestations, considering the possibility of managing the lifecycle of these issuers by Member States with the intervention of the European Commission.

10.2. Regulate the issuance of Verifiable Attestations as a trust service

Description: Following the legal logic of qualified certificates deployed as a DID method plus a verifiable credential under specific rules, it could be possible to define a new trust service, oriented to the issuance of verifiable credentials containing identity attributes (other than foundational identity attributes contained in VCs issued as qualified certificates).

Discussion:

This scenario is very similar to 10.1. The main difference is that scenario 10.1 is mainly oriented to cover Verifiable Attestations issued by public sector bodies, according to public procedure legislation, while in this scenario we consider the possibility of other entities, public or private, acting as issuers of Verifiable Attestations.

Main benefits include leveraging all the common rules, the supervisory framework and the liability model set up in Chapter III of the eIDAS Regulation (a legal trust anchor) for issuing identity attributes in a separated instrument (the Verifiable Credential).

In this sense, the current eIDAS Regulation authorises that "`qualified certificates for electronic signatures [or seals] may include non-mandatory additional specific attributes.`

`Those attributes shall not affect the interoperability and recognition of qualified electronic signatures [or seals]`" (Articles 28 (3) and 38 (3) of the eIDAS Regulation). If it is legally acceptable to issue a qualified X.509 certificate with additional attributes, under the liability regime of the current eIDAS Regulation, it should also be possible to issue these additional attributes in a separate artefact (the Verifiable Attestation). This could be implemented using the same interpretation proposed in scenario 9.2 of this report –considering the qualified certificate (SSI eIDAS qualified certificate) is formed by a Verifiable ID and one or more Verifiable Attestations issued by the same entity, of course–, but Verifiable Attestations may also be issued to a subject that already has an SSI eIDAS qualified certificate.

One of the foundational bases of SSI consider that identity is a social construct, formed by multiple relationships conforming a graph, that conform a wide conception of digital identity. In that view, it does fully make sense to promote that any entity issues verifiable credentials, especially if they are ensured by a legal regime.

A lot of cases exist where it is convenient to issue Verifiable Attestations as an independent trust service, such as customer due diligence evidential identity information, allowing the possibility of reusing the very costly Know Your Customer processes.

Is there a need to establish a legal effect for this trust service? As we already know (see section 6.3 of this report), a qualified certificate for electronic or seal signature does not have a specific legal effect. While its definition clearly states that it "confirms at least the name or the pseudonym of that person" (in the case of a natural person, or "the name of that person" (in the case of legal persons), the current Regulation does not specify any legal effect for certificates, probably because (1) certificates are instrumental to electronic signatures and seals (which receive specific legal effects); (2) a general legal effect of confirmation of identity, in any context, could affect sovereignty of Member States with respect to national ID and (3) it would possibly require to enhance the security requirements with respect to qualified certificates and, of course, qualified electronic signature (or seal) creation devices.

This does not mean, though, that qualified certificates have any legal effect. It is clear that a trust service provider failing to comply with its obligations under the eIDAS Regulation (including, among many others, proofing the natural or legal person's identity) is liable for damage caused intentionally or negligently to any natural or legal person (Article 13 (1) of the eIDAS Regulation). This applies to qualified and non-qualified trust service providers. Thus, any party receiving an electronic signed or seal transaction may rely on the identity of that person, which is clearly an indirect legal effect of a certificate. This is perfectly applicable to DLT-based transactions, when authenticated by using digital signatures.

We could set a parallelism between SSI eIDAS qualified certificates (that confirm the name of a natural or legal person) and Verifiable Attestations, which

would confirm the identity attributes contained therein. Differently from SSI eIDAS qualified certificates or notified Verifiable Attestations, these other Verifiable Attestations would not benefit, nor directly nor indirectly, of any legal effect, it may be convenient to define a specific legal effect.

This legal effect could be to presume the authenticity of the identity attributes contained in a qualified Verifiable Attestation, under the strict liability model for qualified trust services. This presumption would reverse the burden of the proof in case of a conflict, protecting relying parties that trusted in *bona fide* the identity attributes, but it would still be possible to challenge it in a judicial or administrative procedure.

As happens with other non-qualified trust services, it would be convenient to create a specific admissibility and non-discrimination rule with respect to non-qualified Verifiable Attestations.

The adoption of this scenario would increase the market size for EU qualified trust service providers, helping them compete in a global scale with other SSI network's trust models, requiring issuers to be authorised by the network's stewardships, preventing the risk to shifting dependency from trust anchor stores to decentralised networks trusted issuers registries.

On the other hand, this possibility could also facilitate natural and legal persons to share their Verifiable Attestation issued by qualified trust service providers (probably in collaboration with third parties) with public sector bodies. An example would be to share a bank account information contained in a Verifiable Attestation with a public sector body, in a voluntary basis.

In case this qualified Verifiable Attestation has also been notified (see scenario 10.1), then this credential would benefit from the legal benefit of that process.

Recommendation/s:

[Recommendation 28] Propose modifying Chapter III of the eIDAS Regulation with the necessary Articles to define and regulate a new trust service, qualified and non-qualified, with respect to Verifiable Attestations.

[Recommendation 29] Propose defining the legal effect of qualified Verifiable Attestations of presuming the authenticity of the identity attributes contained therein.

[Recommendation 30] Create a specific admissibility and non-discrimination rule with respect to non-qualified Verifiable Attestations.

10.3. Regulate the activity of Identity Hubs as a trust service, in support of SSI-based Once Only Principle

Description: This scenario focus on the adoption of identity hubs, repositories of identity data shared by a subject, directly or when consent has been explicitly given; in that sense, they support the privacy-by-design approach of the verifiable credentials and presentations, thus supporting an SSI-based The Once

Only Principle (TOOP) in new scenarios (e.g., when interchanging public sector issued data with private sector third parties, and the other way around).

Discussion:

Identity hubs are an open source project developed by the Decentralized Identity Foundation (DIF), which aims to provide a high availability personal data storage solution for users.

The identity hub would replace the Data Storage component in the user application. Credentials that a user received would be send based on a previous authentication process to the identity hub utilizing the interaction manager of the user application. At later points, services can refer to the user's hub as a high availability source for up to date credentials.

Note that the specifications of Identity Hubs by DIF also provide the possibility to configure DID base access control rules, allowing other entities to directly access user data from the user's hub. Instead of sending verifiable presentations to a relying party the user application would need to set a permission on the connected identity hub to permit access of the relying party to the data on the hub. Afterwards the relying party is allowed to query and receive this data on the identity hub[56].

Thus, Identity Hubs store verifiable credentials and presentations, DID documents, manage permissions, generate information with legal relevance (e.g., access logs), all of it on behalf of the subject. As the data stored in the Identity Hub is, in principle, only accessed by the subject or by third parties under the subject's sole control, adopting this component helps reconciling the use of DLT systems with GDPR compliance, but under the responsibility of the service provider, acting as a data controller.

It would be convenient to regulate this activity as a trust service, with the aim to set up a strict legal framework with the final protect subjects, especially because of (1) the high dependency of the user with respect to the provider, and (2) as each user should be able to select the identity hub he or she wants, it may be offered by an entity who does not provide any other identity or trust service. Of course, it does not prevent an entity to offer this service in combination with other SSI-based services, such as signing or sealing verifiable credentials or presentation (see scenarios 8.2 and 10.4), or issuing SSI eIDAS qualified certificates.

This approach also follows the legal logic of some trust services currently regulated in the eIDAS Regulation as ancillary services, in support of electronic

[56] The previous paragraphs have been copied from 4.4. Technical specification ESSIF - Identity Hub, available at https://ec.europa.eu/cefdigital/wiki/display/EBP/4.4.+Technical+specification+ESSIF+-+Identity+Hub.

signatures and seals, such as the signature or seal validation service or the signature or seal preservation service.

As in those cases, it does not seed necessary to establish a legal effect with respect to Identity Hubs, but as explained before, there are some cases where it may be relevant to ensure the continuous storage of some information, to comply with legal requirements applicable to specific transactions based on verifiable presentations.

For instance, from the perspective of private sector entities, it is interesting to note Article 40 (1) of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amended by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 mandates, according to which, "Member States shall require obliged entities to retain the following documents and information in accordance with national law […] (a) in the case of customer due diligence, a copy of the documents and information which are necessary to comply with the customer due diligence requirements laid down in Chapter II, including, where available, information obtained through electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities". Additionally, the list of factors and types of evidence of potentially higher risk referred to in Article 18 (3) includes "(1) (c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic identification means, relevant trust services as defined in Regulation (EU) No 910/2014 or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities, for a period of five years after the end of the business relationship with their customer or after the date of an occasional transaction".

In case a relying party subject to this regulation decides to accept verifiable presentations for the customer due diligence process, under Article 13 (1) (a) of Directive (EU) 2015/849, as amended by Directive (EU) 2018/843, probably it will download and store the verifiable presentations, but another possibility could be to rely on the Identity Hub, if it stores the information in a trustworthy manner. While this is a decision to be taken by each relying party, according to their risk analysis, it is clear that this decision may consider whether a legal effect is granted to the identity information preserved in an Identity Hub.

Following the experience of Member States as Belgium[57], the legal effect pf a qualified Identity Hub could consist in presuming compliance with any legal

[57] Belgian law has regulates a national-level trust service for electronic archives, which consists of the preservation of electronic data or the digitization of documents on paper, and which is offered by a trusted

obligation to preserve identity data, and that it has not been altered, in spite of changes made in its electronic medium or format, during all the time this information is to the preserved.

Regarding access by third parties to the content of and Identity Hub, for instance to re-identify a verifiable credential issuer (as when using the eIDAS Bridge, see section 8.2 of this report), there are several legal challenges to address in the future:

- Definition of a specific authorisation model to allow subjects to define and manage access by third parties to her DID document (if stored in the Identity Hub) and verifiable presentations.

- Analyse the special treatment for third parties' access to subject's data without consent and even against her will, obviously when this is according to GDPR and national legislation.

- Design of the Identity Hub policies and practices to leverage The Once Only Principle, thus allowing the subject to use this service to give access to identity data, both to and for public sector bodies, but also private entities.

If this service would also provide, in the future, verifiable presentation generation services, especially implementing techniques such as zero-knowledge proofs, it will be really needed to regulate aspects such as algorithms, use of validated or certified software, sound operational practices or liability in front of third parties per potential damages.

Regarding zero-knowledge proofs, they constitute assertions that may legally substitute the corresponding documents that evidence the personal attributes (i.e. instead of showing the boarding pass, with all personal data, one shows a partial, derived identity that proves the fact that the person has a personal and valid boarding pass), thus increasing privacy effectively, while reducing compliance costs to data controllers, by only if there is legal certainty that the will be accepted as substitutive evidence in legal proceedings.

This objective could be achieved, as proposed by (Alamillo Domingo, Valero Torrijos, Fortune, & Martin, 2017), by establishing a legal effect; i.e.

service provider within the meaning of Article 3, section 19, of the eIDAS Regulation or that is operated on its own account by a public sector body or by a natural or legal person. This service may be subject to qualification, in which case it receives the legal effect of presuming compliance with any legal obligation to preserve a document if it has been incorporated into this service, and that it has not been altered, without prejudice to changes made in its electronic medium or format. Cf. *Loi mettant en œuvre et complétant le règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII " Droit de l'économie électronique " du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique; 21 juliet 2016*.

establishing some sort of equivalence principle such as "where the law requires the documental accreditation of a personal attribute, it will be possible to use a [service name] evidence".

More research is needed in the future to address these topics.

Recommendation/s:

[Recommendation 31] Propose modifying Chapter III of the eIDAS Regulation with the necessary Articles to define and regulate a new trust service, qualified and non-qualified, with respect to Identity Hubs.

[Recommendation 32] Propose defining the legal effect of identity data stored for long-term preservation in qualified Identity Hubs, of presuming compliance with any legal obligation to preserve that identity data, and that it has not been altered, in spite of changes made in its electronic medium or format, during all the time this information is to the preserved.

[Recommendation 33] Define a specific authorisation model to allow subjects to define and manage access by third parties to her DID document (if stored in the Identity Hub) and verifiable presentations. Analyse the special treatment for third parties' access to subject's data without consent and even against her will, obviously when this is according to GDPR and national legislation.

[Recommendation 34] If Identity Hubs would also provide, in the future, verifiable presentation generation services, especially implementing techniques such as zero-knowledge proofs, research which regulation is needed with respect to aspects such as algorithms, use of validated or certified software, sound operational practices or liability in front of third parties per potential damages.

10.4. Regulate delegated key management as an independent trust service, in support of remote wallets

Description: Due to its very design, DIDs require key management activities. Other blockchain transaction also require digital signatures.

eIDAS advanced electronic signature (for natural persons) require that the signatory has exclusive control of the signature creation data. In a similar way, advanced electronic seal requires that the legal person has control of the seal creation data.

When used to endorse a transaction, the DID key could be considered signature or seal creation data. In many cases wallet providers are already offering server-side wallet services with few or no guarantees at all, in the best case supported by social recovery mechanisms.

Discussion:

As introduced in section 7.2 of this report, an interesting legal discussion regarding DID control keys used to sign or seal DID documents, verifiable credentials or verifiable presentations is the possibility of using cloud-based wallets offering key management services, where these keys are managed by third parties, including its generation and ulterior management. While is seems not to be the most developed possibility in the current market, that bets clearly for client-side wallets[58], there are some experiences[59].

(Wang & De Filippi, 2020, p. 17) have noted that "a true self-sovereign identity system would require a certain level of infrastructure, primarily high penetration of affordable smartphones that can securely store private keys and reliable connectivity"; these authors have also identified that "another problem with localized key storage –beyond hardware affordability– is the larger issue of key recovery, since, in a self-managed environment, losing one's phone necessarily entails losing one's private key", concluding that "perhaps the most important obstacle to achieving full self-sovereignty is the problem of key recovery, combined with the price of hardware".

While this analysis is closely associated with the use of SSI systems by very economical vulnerable citizens, it is nonetheless important to highlight that the key recovery problem presents a general nature. Thus, for the same authors, "in light of these issues, there is a consensus that the best practice at the moment is a custody or guardianship model, whereby program administrators […] can manage keys on behalf of constituents, but constituents always have the ability to opt-out of guardianship should they choose to self-manage".

As seen when discussing about the eIDAS Bridge (scenario 8.2), for certain operations it is convenient to update a DID document with an additional key, used for signing or sealing verifiable credentials. To this end, the eIDAS Regulation has authorised qualified Trust Service Providers to generate and manage signature or seal creation data on behalf of the signatory or the seal creator. Additionally, these providers are authorised to provide key backup and recovery services.

From a technical perspective, sole control requirements in these third party scenarios have been defined in CEN EN 419 241-1 and ETSI TS 119 431-1 (in the case of qualified electronic signatures, CEN EN 419 241-2 may be very relevant in the future, if included in the eIDAS QSCD Decision, to be applied *mutatis mutandis* to qualified electronic seals), but it could be considered against the SSI principles, as nothing prevents the qualified TSP to delete the private key, even if it was an incorrect action from a contractual perspective, or even an illegal behaviour in case any national Law rules on this matter.

[58] See, for instance, Evernym, uPort, etc.

[59] See, for example, Spaceman.ID.

An issue is that the eIDAS Regulation is not so clear when referring to the possibility of organisations that are not qualified TSPs to generate and manage advanced signature or seal creation data, as it only explicitly relates to qualified electronic signatures and qualified electronic seals.

It is quite obvious that the current eIDAS approach is clearly against the DPKI philosophical bases, both from the perspective of SSI and DKMS, but it is also true that in some cases there may be convenient to have cloud-based wallets, at least to avoid social exclusion.

In this sense, the notions of remote advanced and qualified electronic signatures and seals provide key properties, such as a legal construction for sole control, with a high level of confidence, which may perfectly be applied to this scenario, probably by adapting the technological approach (i.e. by modifying the current legislation).

For instance, to adhere to DPKI approach, key generation management should be done in a distributed manner, for instance by applying multi-signature operations to prevent the server wallet provider from taking control of the key, erasing it or other sensitive operations.

With proper technical measures, SSI and DKMS may be maintained in cloud-based wallet services with a similar level of security, if not a better one, to the self-management based in a device with a secure element; but with the benefit of the application of a sound, strict, supervisory system.

As seen in section 6.1, key generation and management it not considered a trust service in the current eIDAS. Thus, it can only be provided by a (qualified) trust service provider. Although it may be any trust service provider, this service is provided by a qualified TSP issuing qualified certificates, because of the close connexion between the process of generating a key pair and the process of issuing its corresponding public key certificate.

This inherent connexion is not so needed when moving into DPKI, where different issuers could be issuing different credentials to subjects. Maintaining this model could be more interesting in the case of scenario 9.2, but even in this case we are still facing a potential market competition issue; because of the strict liability regime contained in the eIDAS Regulation, it has been generally understood that the TSP issuing qualified certificates is responsible of the security of the keys. This approach may make sense in a hierarchical PKI, because of the trust management model (you trust a digital signature because you trust the early binding of a public key to certain identity attributes by a certification authority; and you trust a certification authority because an upper certification authority has done the same kind of binding, until you arrive to a trust anchor, i.e. those contained in eIDAS Trusted Lists); but is does not fit well in a DPKI world.

Instead, in this new world, users need trustworthy decentralised key management services, fully decoupled from any verifiable credential provider,

to maintain self-sovereignty. Thus, it would be needed to regulate key management as an independent trust service.

An additional benefit of this approach is the it would allow asserting, in the DID document, information about the security and quality level of the DID control key, and also implement key rotation and key derivation services, in support of more privacy respecting techniques, such as pairwise-pseudonymous DIDs (Reed, Law, Hardman, & Lodder, 2018).

From a different perspective, Cloud wallet services are also offered in support of other Blockchain transactions[60], such as in the case of Bitcoin virtual currency transactions, as seen in Figure 15.

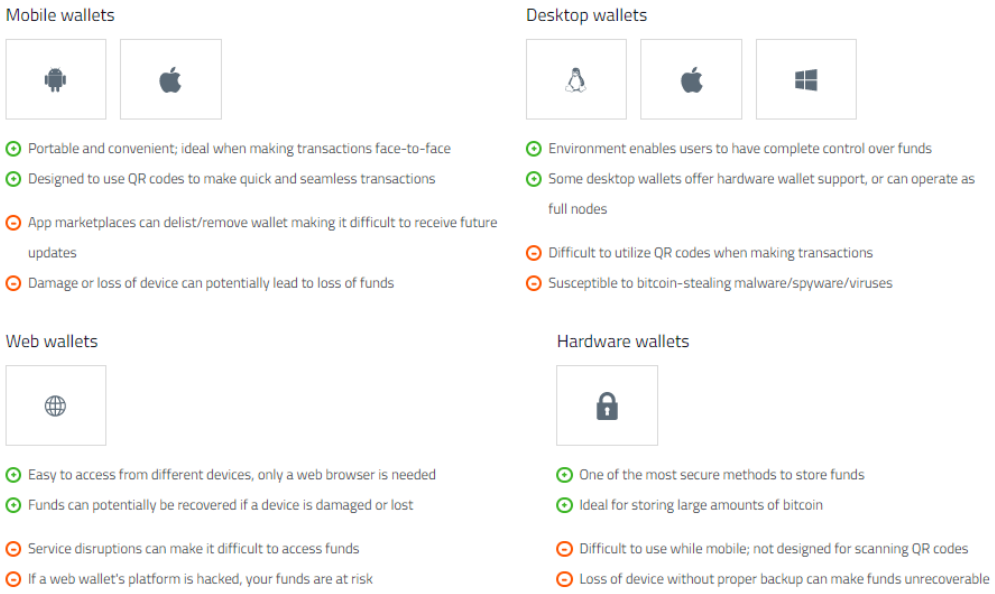

Figure 17. Choose your Bitcoin Wallet.

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU has established rules to custodian wallet providers, defined as "an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies", in connexion with the fact that "the anonymity of virtual currencies allows their potential misuse for criminal purposes" (Recital (9)); thus, under the same recital, "to combat the risks related to the anonymity, national Financial Intelligence Units (FIUs) should be able to obtain

[60] For a detailed analysis of these services, see (Allen & Appelcline, 2019), chapter 4.

information allowing them to associate virtual currency addresses to the identity of the owner of virtual currency".

To this end, custodian wallet providers are considered as obliged entities and, according to the new text of Article 47 (1) of Directive (EU) 2015/849, "Member States shall ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered […]".

Whether custodian wallet providers can be considered as providers generating and managing signature or seal creation data (keys) depend on the operations supported by those keys and its legal interpretation. Moreover, it could happen that a transfer operation is considered as a signature produced on behalf of, but his will depend on a number of factors, including the technical implementation.

In this case, it could be a legal conflict between the two different legal instruments. From another point of view, though, aligning both legislations could represent an opportunity to have a neutral regulatory framework for legal acts performed electronically by natural and legal persons.

More research is needed in the future to address these topics.

Recommendation/s:

[Recommendation 35] Propose modifying Chapter III of the eIDAS Regulation with the necessary Articles to define and regulate a new trust service, qualified and non-qualified, with respect to Decentralised Key Management.

[Recommendation 36] Study the alignment between the decentralised key management trust service and the new custodian wallet provider legislation.

10.5. Regulate a specific type of DLT node as a trust service

Description: Finally, we may envision the possibility of extending the eIDAS Regulation to a specific trust service consisting on the operation of a specific type of node, for a specifically designed DLT, tailored for the generation of electronic evidences.

Discussion:

As explained in section 2 of this report, DLT is based in distributed computing formed by a network of nodes executing a common software. According to ISO/FDIS 22739. Blockchain and distributed ledger technologies – Terminology[61], a DLT node is a device or process that participates in a

[61] This standard is still under development.

distributed ledger network and stores a complete or partial replica of the distributed ledger.

ISO/CD 23257.3. Blockchain and distributed ledger technologies – Reference architecture [62], identifies the different actors intervening in a DLT system, as shown in Figure 18.

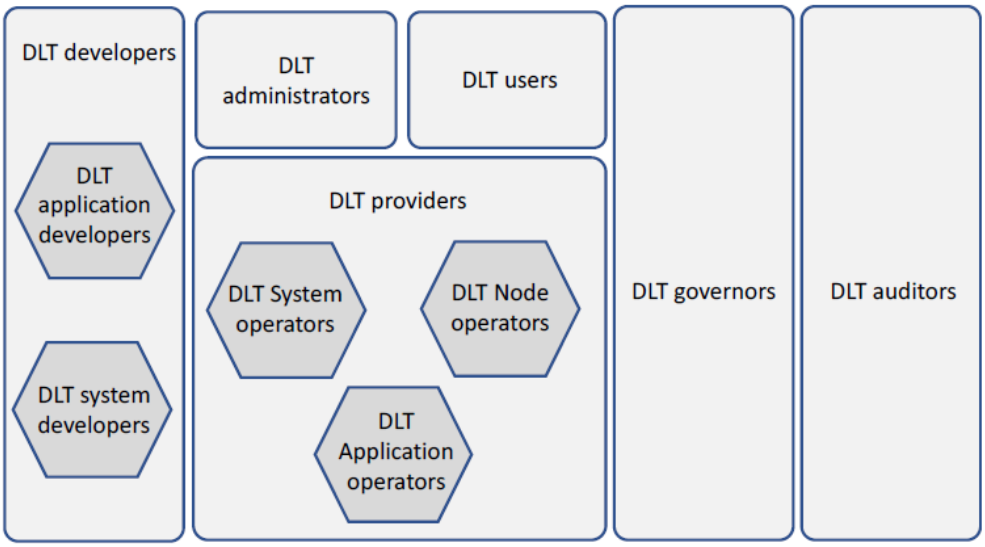

Figure 18. DLT System roles and sub-roles (ISO/CD 23257.3)

Specifically, DLT providers own and operate one or more nodes within DLT systems and DLT networks. They agree to create/instantiate nodes, join networks, pay for, and handle legal agreements for joining the network.

In a systemic view (Figure 19), it is easy to see that, even if these systems are said to be “trustless”, in the sense of not needed a third party, they are still provided by someone, in many cases as an economic activity. The fact that they need to necessarily cooperate in the execution of the consensus algorithm (to name an example), does not mean they should not have legal obligations nor bear liability in case of damaging third parties, at least with respect to their functions, and regardless of other DLT systems roles, significantly the DLT governor.

Currently, this service must be considered as an information society service, subject to the general provisions contained in Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), as implemented in national legislation, and thus, any service provider in a DLT system will need to comply with the corresponding legal requirements[63], as applicable. And in

[62] This standard is also under development.

[63] For a general listing of these requirements, see (Alamillo Domingo, Valero Torrijos, Fortune, & Martin, 2017).

case, any entity acting in a DLT system that produce any damaged to a third party is subject to non-contractual liabilities.

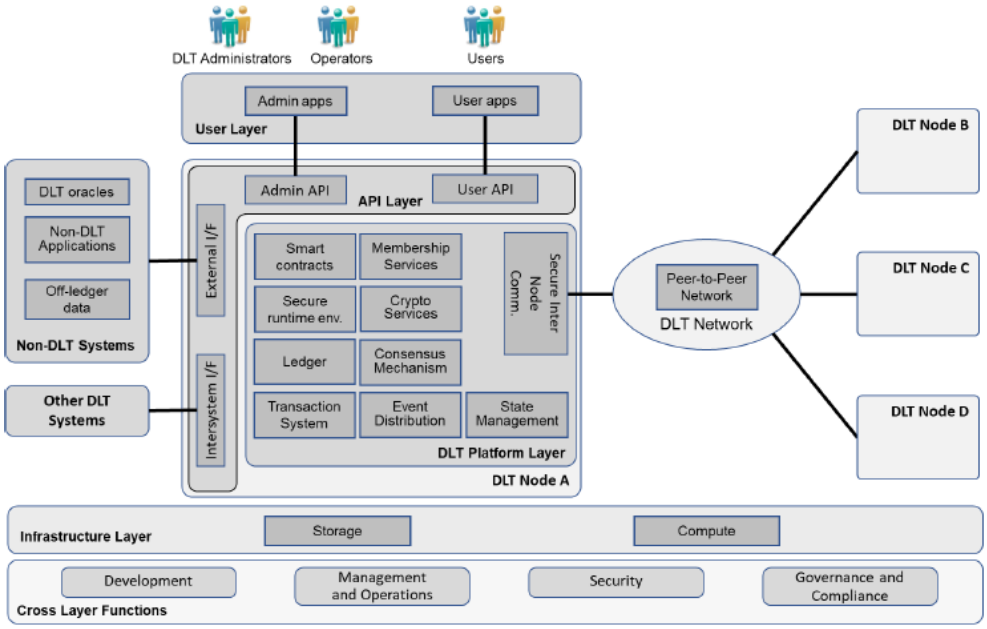

Figure 19. System view of functional components of a DLT system (ISO/CD 23257.3)

The logic of any trust service in the eIDAS regulation, especially those that are subject to qualification, is to determine a set of rules to ensure its trustworthiness, in view of defining a specific legal effect for it, or to ensure legal certainty and consumer protection.

This legal logic is perfectly applicable to the provision of services in a DLT, with some adjustments. For instance, qualification should be granted for each DLT node forming the network, with a minimum number of them, according to the DLT governance framework set up (for instance, before launching the genesis block).

The advantage of this approach is that it would allow setting up a series of legal requirements aimed to deploy distributed networks that balance the public/legitimate interest in the legal certainty of electronic evidences, with the rights and expectations of all parties.

Thus, as DLT networks provide many of the core services for applications, this legal framework could foster the availability of baseline services on top of which other services would be reliably deployed (namely, identity and signature/seal services, timestamping services or electronic registered delivery services).

Regulation would cover aspects such as governance and consensus models, time synchronization, crypto security, software certification, then need to get an administrative authorisation to make a fork, etc., but also legal limits to anonymity and some privacy rights, such as right to modification or right to erasure, attending to the final purpose of these specific DLT networks, which is to provide trust to transactions.

More research is needed in the future to address these topics.

Recommendation/s:

[Recommendation 37] Propose modifying Chapter III of the eIDAS Regulation with the necessary Articles to define and regulate a new trust service, qualified and non-qualified, with respect to DLT systems addressed to consumers.

[Recommendation 38] Consider imposing balanced limitations of privacy rights when using qualified DLT systems trust service, attending to the public interest in electronic evidence, supporting legal certainty.

References

Abraham, A., Hörandner, F., Omolola, O., & Ramacher, S. (2019). Privacy-Preserving eID Derivation for Self-Sovereign Identity Systems. In L. X. Zhou J. (Ed.), *Information and Communications Security. ICICS 2019. Lecture Notes in Computer Science. 11999*, pp. 307-323. Cham: Springer.

Abraham, A., Theuermann, K., & Kirchengast, E. (2018). Qualified eID Derivation Into a Distributed Ledger Based IdM System. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 1406-1412). New York, NY: IEEE. doi:10.1109/TrustCom/BigDataSE.2018.00195

Alamillo Domingo, I. (2010b). La identidad electrónica en la red. En A. Rallo Lombarte, & R. Martínez Martínez (Edits.), *Derecho y Redes Sociales* (Primera ed., págs. 37-54). Cizur Menor, Navarra, España: Aranzadi.

Alamillo Domingo, I. (2016). Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autenticación de los ciudadanos. In E. Gamero Casado, S. Fernández Ramos, & J. Valero Torrijos (Eds.), *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público* (Primera ed., pp. 675-768). Valencia, España: Tirant lo Blanch.

Alamillo Domingo, I. (2019a). *Identificación, firma y otras pruebas electrónicas. La regulación jurídico-administrativa de la acreditación de las transacciones electrónicas.* Cizur Menor, Navarra: Aranzadi.

Alamillo Domingo, I. (2019b). *El uso de los sistemas de identidad auto-soberana en el sector público español y en la Unión Europea.* Retrieved from Blockchain Intelligence Institute: https://blockchainintelligence.es/2019/03/10/articulo-el-uso-de-los-sistemas-de-identidad-auto-soberana-en-el-sector-publico-espanol-y-en-la-union-europea-por-ignacio-alamillo

Alamillo Domingo, I., & Curry, P. (2019). *Report on Study – Trust Anchors for Decentralised Identity Management (TADIM). ISO/TC 307/JWG 04, doc. N91*. Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG Blockchain and distributed ledger technologies and IT Security techniques .

Alamillo Domingo, I., Valero Torrijos, J., Fortune, D., & Martin, D. (2017). *ARIES H2020 D2.3 - Legal requirements and analysis of ID legislation and law enforcement aspects.* Retrieved from https://www.aries-project.eu/content/legal-requirements-and-analysis-id-legislation-and-law-enforcement-aspects-0

Allen, C. (2016, 04 27). *The path to self-sovereign identities.* Retrieved from Coindesk: https://www.coindesk.com/path-self-sovereign-identity/

Allen, C., & Appelcline, S. (2019). *#SmartCustody. The use of advanced cryptographic tools to improve the care, maintenance, control, and protection of digital assets.* Blockchain Commons, LLC. Retrieved from https://www.smartcustody.com

Alonso Ureba, A., & Alcover Garau, G. (2000). La firma electrónica. In *Derecho de Internet. Contratación electrónica y firma digital* (pp. 175-206). Cizur Menor, Navarra, España: Aranzadi.

Anguiano Jiménez, J. (2015, 10 09). *Sobre la emisión de declaraciones de voluntad mediante el uso de firmas digitalizadas.* Retrieved from El Derecho.com: http://www.elderecho.com/tribuna/www-elderecho-com/emision-declaraciones-voluntad-firmas-digitalizadas_11_870430001.html

Arslanian, H., & Fischer, F. (2019). A High-Level Taxonomy of Crypto-assets. In *The Future of Finance* (pp. 139-156). Cham: Palgrave Macmillan.

Atzeni, A., & Lioy, A. (2011). *STORK. D2.4 – Mapping of the national authentication levels of the new Member States to the STORK QAA levels.* STORK-eID Consortium. Retrieved from https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1876

Baldwin, A., Shiu, S., & Cassasa Mont, M. (2002). Trust Services: A framework for service-based solutions. *Proceedings of the 26 th Annual International Computer Software and Applications Conference (COMPSAC'02)* (pp. 507-513). IEEE.

Batubara, F., Ubacht, J., & Jansenn, M. (2018). Challenges of blockchain technology adoption for e-government: a systematic literature review. *dg.o '18: 19th Annual International Conference on Digital Government Researc* (pp. 1-9). Delft The Netherlands: ACM. doi:10.1145/3209281.3209317

Baum, C., Frederiksen, T., Hesse, J., Lehmann, A., & Yanai, A. (2019). *PESTO: Proactively Secure Distributed Single Sign-On, or How to Trust a Hacked Server.* Retrieved from https://ia.cr/2019/1470

Bernal Bernabé, J., Canovas, J. L., Hernández-Ramos, J. L., Torres Moreno, R., & Skarmeta, A. (2019). Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE Access, 7*, 164908-164940. doi:10.1109/ACCESS.2019.2950872

Bierekoven, C., Bazin, P., & Kozlowski, T. (2004). Electronic signatures in German, French and Polish law perspective. *Digital evidence and electronic signature law review, 1*, 7-13. doi:http://dx.doi.org/10.14296/deeslr.v1i0.1719

Boer, A. (2009). *Legal theory, sources of law and the semantic web.* Amsterdam: IOS Press. doi:10.3233/978-1-60750-003-2-i

Borges, G. (2012, 09 05). The Draft Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, COM (2012) 238. *Presentation at the Workshop on Electronic Identification and Trust Services*. Brussels.

Bouma, T. (2018, 12 08). *Less Identity*. Retrieved from Medium.com: https://medium.com/@trbouma/less-identity-65f65d87f56b

Brugger, J., Fraefel, M., Meerbergen, P., Van der Donckt, C., Riedl, R., & Sánchez, J. (2014). *STORK 2.0. D.7.2 Service Design and Pricing - Consolidated Report & Open Questions.* STORK 2.0 Consortium. Retrieved from https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=39:d72-service-design-and-pricing-consolidated-report-a-open-questions&Itemid=177

Cameron, K. (2005, May). *The Laws of Identity*. Retrieved from Microsoft: https://msdn.microsoft.com/en-us/library/ms996456.aspx

Cameron, K. (2006). *The identity metasystem.* Retrieved from Kim Cameron's Identity Weblog. Digital Identity, Privacy, and the Internet's Missing Identity Layer: https://www.identityblog.com/?p=355

Caprioli, É. (2014). *Signature électronique et dématérialisation. Droit et pratiques.* Paris, France: LexisNexis.

Chou, E. Y. (2015). What's in a name? The toll e-signatures take on individual honesty. *Journal of Experimental Social Psychology*(61), 84-95.

Couto Calviño, R. (2007). Reflexiones acerca de la firma electrónica y el nuevo mercado de servicios de certificación. *Revista de Contratación Electrónica*(83), 3-37.

De Miguel Asensio, P. A. (2015). *Derecho privado de Internet* (Quinta ed.). Cizur Menor, Navarra, España: Aranzadi.

Dumortier, J. (2004). Legal Status of Qualified Electronic Signatures in Europe. In P. Sachar, N. Polhmann, & H. Reimer (Ed.), *ISSE 2004 — Securing Electronic Business Processes. Highlights of the Information Security Solutions Europe 2004 Conference* (pp. 281-289). Wiesbaden: Vieweg+Teubner Verlag.

Dumortier, J. (2016, July 1). *Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation).* Retrieved from SSRN: https://ssrn.com/abstract=2855484

Dumortier, J., & Vandezande, N. (2012a, September 26). *Critical Observations on the Proposed Regulation for Electronic Identification and Trust Services for Electronic Transactions in the Internal Market. ICRI Research Paper 9.* Retrieved from SSRN: https://ssrn.com/abstract=2152583

Dumortier, J., & Vandezande, N. (2012b, October). Trust in the proposed EU regulation on trust services? *Computer Law & Security Review, 28*(5), 568-576. doi:10.1016/j.clsr.2012.07.010

Eertink, H., Hulsebosch, B., & Lenzini, G. (2008). *STORK. D2.1 - Framework Mapping of Technical/Organisational Issues to a Quality Scheme.* STORK-eID Consortium. Retrieved from https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=579

eIDAS Cooperation Network. (2018). *Guidance for the application of the levels of assurance which support the eIDAS Regulation.* Retrieved from https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Guidance+documents

European Commission. (2005). *Signposts toward eGovernment 2010.* Luxembourg: Office for Official Publications of the European Communities.

European Commission. Directorate-General for Informatics. (2003). *Electronic interchange of data between administrations (IDA). The Horizontal Actions and Measures (HAM) 2003 Work Programme.* Obtenido de http://ec.europa.eu/idabc/en/document/2548/3.html

European Commission. Directorate-General for Informatics. (2004). *Electronic interchange of data between administrations (IDA). The Horizantal Actions and Measures (HAM) Work program 2004.* Obtenido de http://ec.europa.eu/idabc/en/document/2548/3.html

European Commission. Information Society and Media Directorate-General. eGovernment Unit. (2006). *A Roadmap for a pan-European eIDM Framework by 2010, v1.0.*

Fraenkel, B. (1992). *La signature. Genèse d'un signe.* Paris, France: Gallimard.

Fraenkel, B. (2008). La signature: du signe à l'acte. *Sociétés & Représentations*(25), 15-23.

Gobert, D. (2015, Février). *Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie.* Retrieved from http://www.droit-technologie.org

Graux, H. (2011). Rethinking the e-Signatures Directive: On laws, trust services and the digital single market. *Digital Evidence and Electronic Signature Law Review*(8), 9-24.

Graux, H., & Majava, J. (2007). *eID Interoperability for PEGS. Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms.* European Communities. Retrieved from http://ec.europa.eu/idabc/en/document/6484/5938/

Grüner, A., Mühle, A., Gayvoronskaya, T., & Meinel, C. (2018). A Quantifiable Trust Model for Blockchain-Based Identity Management. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 1475-1482). Halifax, NS, Canada: IEEE.

Haddouti, S. E., & Ech-Cherif El Kettani, D. M. (2019). Analysis of Identity Management Systems Using Blockchain Technology. *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)* (pp. 1-7). Rabat, Morocco: IEEE. doi:10.1109/COMMNET.2019.8742375

Halpin, H. (2011). Sense and Reference on the Web. *Minds & Machines*(21), 153–178. doi:10.1007/s11023-011-9230-6

Hulsebosch, B., Lenzini, G., & Eertink, H. (2009). *STORK. D2.3 - Quality authenticator scheme.* STORK-eID Consortium. Retrieved from https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577

Illescas Ortíz, R. (2001). *Derecho de la contratación electrónica.* Madrid, España: Civitas Ediciones.

Jøsang, A., Fabre, J., Hay, B., Dalziel, J., & Pope, S. (2005). Trust Requirements in Identity Management. In P. Montague, & R. Safavi-Naini (Ed.), *Australasian Information Security Workshop 2005 (AISW 2005). Conferences in Research and Practice in Information Technology. 44*, pp. 99-108. Newcastle, Australia: Australian Computer Society.

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems, 43*(2), 618-644.

Kennedy, E., & Millard, C. (2016). Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU Member States. *Computer Law & Security Review*(32), 91-110.

Kuperberg, M. (2019). Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective. *IEEE Transactions on Engineering Management*, 1-20. doi:10.1109/TEM.2019.2926471

Lim, S. Y., Fotsing, P. T., Almasri, A., Musa, O., Kiah, M. L., Ang, T. F., & Ismail, R. (2018). Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey. *International Journal on Advanced Science Engineering Information Technology, 8*(4-2), 1735-1745.

Madrid Parra, A. (2001). Aspectos jurídicos de la identificación en el comercio electrónico. In R. Illescas Ortiz, & I. Ramos Herranz (Eds.), *Derecho del comercio electrónico* (Primera ed., pp. 185-250). Las Rozas, Madrid, España: La Ley-Actualidad.

Marlinspike, M. (15 de 02 de 2012). *What is 'Sovereign Source Authority'?* Obtenido de The Moxie Tongue: https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html

Marlinspike, M. (2016, 02 09). *Self-Sovereign Identity*. Retrieved from The Moxy Tongue: https://www.moxytongue.com/2016/02/self-sovereign-identity.html

Martin, A. K., van Brakel, R. E., & Bernhard, D. J. (2009). Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society*(6(3)), 213-232.

Martínez Nadal, A. (2009). *Comentarios a la Ley 59/2003 de firma electrónica* (Segunda ed.). Cizur Menor: Civitas Thompson Reuters.

Mason, S. (2017). *Electronic Signatures in Law* (Fouth ed.). London, United Kingdom: University of London. doi:10.14296/117.9781911507017

Merchán Murillo, A. (2016). *Firma electrónica: Funciones y problemática (Especial referencia al Reglamento [UE] nº 910/2014, relativo a la identificación electrónica por la que se deroga la Directiva 1999/93/CE de firma electrónica)* (Primera ed.). Cizur Menor, Navarra, España: Aranzadi.

Moles Plaza, R. J. (2004). *Derecho y control en Internet. La regulabilidad de Internet.* Barcelona: Ariel.

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*(30), 80-86. doi:10.1016/j.cosrev.2018.10.002

Muñoz Soro, J. F. (2003). *Decisión jurídica y sistemas de información* (Primera ed.). Madrid, España: Fundación Beneficentia et Peritia Iuris. Colegio de Registradores de la Propiedad y Mercantiles de España.

Nguyen, K. (2018). Certification of eIDAS trust services and new global transparency trends. *Datenschutz und Datensicherheit*(7), 424-428.

Ølnes, J. (2001). A Taxonomy for Trusted Services. In B. Schmid, K. Stanoevska Slabeva, & V. Tschammer (Eds.), *Towards the E-Society: E-Commerce, E-Business, and E-Government* (Vol. 74, pp. 31-44). Kluwer Academic Publishers.

Pelletan, J. (2017). *Sociétés sécuritaires ou sociétés de confiance.* Paris, France: L'Harmattan.

Polanksi, P. (2015). Towards the single digital market for e-identification and trust services. *Computer law & security review*(31), 773-781.

Posch, R. (2017). Digital sovereignty and IT-security for a prosperous society. *Informatics in the Future. Proceedings of the 11th European Computer Science Summit (ECSS 2015), Vienna, October 2015* (pp. 77-86). Cham: Springer.

Reed, D., & Sabadello, M. (2019). Decentralized identifiers. In D. Reed, & A. Preukschat (Eds.), *Self-Sovereign Identity. Decentralized Digital Identity and Verifiable Credentials.* Manning Publications.

Reed, D., & Slepak, G. (2015). DPKI's Answer To The Web's Trust Problems. *Decentralized Public Key Infrastructure. A White Paper from Rebooting the Web of Trust.*

Reed, D., Law, J., Hardman, D., & Lodder, M. (2018, 04 02). *DKMS (Decentralized Key Management System) Design and Architecture V3*. Retrieved from GitHub: https://github.com/hyperledger/indy-sdk/blob/677a0439487a1b7ce64c2e62671ed3e0079cc11f/doc/design/005-dkms/DKMS%20Design%20and%20Architecture%20V3.md

Rico Carrillo, M. (2015). El Reglamento europeo sobre identificación y servicios de confianza electrónicos. *Revista General de Derecho Europeo*(35), 1-24.

Rodríguez Ayuso, J. F. (2018). *Impacto de la nueva regulación europea sobre identificación electrónica y servicios de confianza en el ámbito de la contratación privada dotada de firma electrónica.* Alma Mater Studiorum - Università di Bologna, Bologna.

Roβnagel, H. (2006). On diffusion and confusion - Why electronic signatures have failed. In S. Fischer-Hübner, S. Furnell, & C. Lambrinoudakis (Eds.), *Trust and Privacy in Digital Business. 3rd International Conference on Trust and Privacy in Digital Business, TrustBus 2006* (Vol. LNCS 4083, pp. 71-80). Springer.

Rundle, M., Blakley, B., Broberg, J., Nadalin, A., Olds, D., Ruddy, M., . . . Trevithick, P. (2007). At a crossroads: "personhood" and digital identity in the information society. STI Working Paper 2007/07. Organisation for Economic Co-operation and Development. Obtenido de http://www.oecd.org/sti/working-papers

Somorovsky, J., & Mladenov, V. (2017). *FutureTrust D2.2. Overview of eID Services.*

Sorge, C. (2014). The legal classification of identity-based signatures. *Computer Law & Security Review*(30), 126-136.

Spark legal network, Tech4i2 & Datarella. (2020). *Study on Blockchains. Legal, governance and interoperability aspects (SMART 2018/0038).* European Commission. Luxembourg: Publications Office of the European Union. doi:10.2759/4240

Srivastava, A. (2011, November). Resistance to change: Six reasons why businesses don't use e-signatures. *Electronic Commerce Research, 11*(4), 357-382. doi:10.1007/s10660-011-9082-4

Stokkink, Q., & Pouwelse, J. (2018). Deployment of a Blockchain-Based Self-Sovereign Identity. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 1336-1342). Halifax, NS, Canada: IEEE. doi:10.1109/Cybermatics_2018.2018.00230

Sullivan, C., & Burger, E. (2019). Blockchain, Digital Identity, E-government. In H. Treiblmaier, & R. Beck (Eds.), *Business Transformation through Blockchain* (Vol. II, pp. 233-258). Cham: Palgrave Macmillan.

Swan, M. (2016). Blockchain Temporality: Smart Contract Time Specifiability with Blocktime. En J. Alferes, L. Bertossi, G. Governatori, P. Fodor, & D. Roman (Ed.), *Rule Technologies. Research, Tools, and Applications. RuleML 2016. Lecture Notes in Computer Science, vol 9718* (págs. 184-196). Cham: Springer. doi:10.1007/978-3-319-42019-6_12

Timón, C., Valero Torrijos, J., Alamillo Domingo, I., Torres Moreno, R., Bernal Bernabé, J., Rodríguez, J., . . . Frederiksen, T. (2020). *D3.2 Security and Privacy-aware OLYMPUS Framework Impact Assessment.* Retrieved from https://olympus-project.eu/wp-content/uploads/2020/02/Olympus_pu_d3_2_v1_0.pdf

Trotter, G. (2014). Autonomy as Self-Sovereignty. *HEC Forum*(26), 237–255.

Wang, F., & De Filippi, P. (2020). Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. *Frontiers in Blockchain, 2*(28), 1-22. doi:10.3389/fbloc.2019.00028

Wolf, C., & Zeibig, N. (2015). *Evidence in Civil Law – Germany*. Maribor, Slovenia: Institute for Local Self-Government and Public Procurement Maribor.

SSI eIDAS Legal Report

How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market