Framework for Trust with Electronic Identities And Trust Services (eIDAS) compliance, European Blockchain Services Infrastructure (EBSI) compliance and Qualified Trust Service Providers (QTSP)

Erwin Nieuwlaar
Delft University of Technology

August 2022

Abstract

A European Digital Identity is being developed by the European Commission. eIDAS is the legal framework and source of trust for the upcoming European Digital Identity. In this thesis an open standard with open source reference implementation at eIDAS high level is developed. Collaboration among EU Member States is vital to avoid fragmentation in this field. The Open Source collaborative method at will avoid delays and costly learning by each and every individual EU Member State. Delft University of Technology is helping the Netherlands with hosting the EBSI technical infrastructure. Delft also was among the first to develop an open source mobile-first wallet which is EBSI-compatible. Note that the commercial closed implementation of the EU reference wallet is expected to be delivered only in 2023. We argue that pre-competitive open standard development and reference implementation in a open model will provide superior quality, deliver results faster, and at lowered cost. Critical infrastructure for identity, money, and data is only compatible with the open innovation process, open standard setting processes, and simply has no commercial business case. Focus of our open standard and open source reference implementation is eIDAS high compliance, GDRP compliance, EBSI wallet compliance, and integrating multiple legal Dutch data bases such as the Company Register from the Netherlands Chamber of Commerce, the Vehicle Registry of the Netherlands Vehicle Authority, and the Netherlands Personal Records Database.

Contents

1 Introduction

Citizens must be able to comprehend their digital world, select how they want to interact with it, and act autonomously. At the moment, this is not obvious in the digital realm. Although technology is getting simpler to use, it is becoming more difficult to comprehend precisely how it operates and how data, whether personal or not, is used. This may be enhanced by, among other measures, reducing data collecting. In order to reduce the current data economy, the European Union, and accordingly, the Dutch government is striving to develop an alternative [1]. The Data Act [2] the Data Governance Act [3] the European Commission is pushing a data economy in which users are controlling their data. Reducing the dependence on organisations which do not adhere to European principles. With the European Data Act, the European Union is developing standards for fair access to and use of non-personal data, including the right to access data and the ability to readily transfer data to other parties. The new Data Act addresses genuine rights to access and use data. A new, more privacy-friendly method of processing data, in which people are given actual options, does not spontaneously appear. European citizens will obtain a digital identity that is widely useable so that they may securely identify themselves in the digital world and have more control over their own data - similar to using a passport in the physical world [4]. These means of identification enable us to establish our identity. By using digital identification, we can streamline interactions and save time. Digital identity tools are presently available from a variety of private and public suppliers, for instance enabling consumers to utilize online banking or various public services. There are several levels of security and reliability offered by digital IDs, the most universal European standard (and solely used in this paper) is the Level of Assurance provided in the eIDAS regulation [5]. At the moment, large platforms allow their users to login to a variety of online services, like shopping and reading the news, but these logins do not provide consumers complete choice over the information they submit to identify themselves with online services. These means of identification provided by Big Tech control most of the market share [6] and induce privacy issues [7]. Although the European Commission has not set a strict release date for the new European digital identity, the first toolbox to experiment with implementation should be released by 30 October 2022 [8]. The most innovative aspect of the new regulation with regard to the new European digital passport is that everyone will be entitled to a European Digital Identity Wallet that is recognized by all Member States. However, there will not be any obligation either. The European Digital Identity Wallet will be designed as a Self-Sovereign Identity Wallet where users choose to disclose their personal information with online services, enabling people to digitally identify themselves, as well as store and manage identity data and official documents in an electronic format. These may include a driver's license, a prescription, or educational certification. With the wallet, users will be able to access internet services, transfer digital documents, or simply confirm a certain personal trait, such as age, without disclosing their identity or other personal information. While the European Digital Identity will be required to be recognized by public services and some commercial services, its security characteristics entice all private service providers to recognize it for services that demand rigorous authentication, opening up new economic prospects which could lead to a 3 to 13% increase of GDP by 2030 if integrated successfully [9]. Three of such potential economic prospects is the integration of the Company Register from the Netherlands Chamber of Commerce, the Vehicle Registry of the Netherlands Vehicle Authority, and the Netherlands Personal Records Database. These institutions will be Qualified Trust Service Providers, and will serve as an anchor for legal certainty for Dutch persons and businesses. In this work, we will provide alignment of notions within Self-Sovereign Identity, eIDAS, and EBSI, provide a framework for eIDAS and EBSI integration in a Self-Sovereign Identity environment such as the coming European Digital Identity Wallet, and implement a use case in collaboration with the Netherlands Chamber of Commerce, Netherlands Vehicle Authority and the Personal Records Database.

2 Problem Description

In utopia an user would have full control, independence and access over all their data where their rights are protected, sharing of data is done minimally and with consent. Nonetheless, the system should be transparent, interoperable, portable and persistent [10]. This vision with regard to identity is often seen as the preeminent Self-Sovereign Identity (not all opinions are aligned on this matter [11, 12]), where people or organizations have exclusive ownership of their digital and analog identities, as well as control over the sharing and use of their personal data. Aforementioned, the European Commission envisions a similar perception with the upcoming European Digital Identity wallet [13]. However, the steps that should be taken from the current means of identification and authentication to a fully operational Self-Sovereign Identity, such as the European Digital Identity, have a steep slope. Below is a list of the current challenges in the field of Self-Sovereign Identity and the application thereof [14].

1. Protocols, practices, and rules pertaining to data management, data interchange, and user experience should be created and executed with care. The system should be secure, private, user-centric, and compliant to regulations.

2. In the Self-Sovereign Identity paradigm, the users are responsible for key-management and the accompanying risks. Numerous examples exist in which users have lost their cryptographic keys, resulting in the loss of important data [15] or irretrievable capital [16]. Resolving the core management needs of the Self-Sovereign Identity architecture is a prerequisite for the widespread adoption of Self Sovereign Identity. Where dependence on decentralized key custodians is one solution to Self-Sovereign Identity key management [17].

3. Another challenge is that the should give its consent which is; unambiguous, explicit, well-formed,

and freely granted. This procedure is difficult to implement and validate using existing identification models. In addition, requiring users to accept to several privacy rules and data sharing practices has resulted in a phenomenon known as *consent fatigue* [18], in which the user is inundated with privacy alerts. Hence, in Self-Soverign Identity the management of consent management, its presentation, and the enforcement thereof should be considered.

4. Many Self-Sovereign Identity solutions use distributed ledger technology. Certain distributed ledgers are public, enabling any entity to access or write to the ledger, whilst others are permissioned and only let a limited number of allowed entities to read or write new data into the ledger. The permissionless and public paradigm, are susceptible to assaults prevalent in open distributed ledger systems [19]. On the other hand, the permissioned method runs the danger of developing a centralized and censored architecture comparable to an oligopoly among the few permitted entities if it is not properly constructed [20, 21].

5. It is essential to recognize and communicate the necessary level of decentralization required to meet the preceding mentioned Self-Sovereign Identity vision. Certain identity management processes, such as identity claim issuance, identity search, and safe data storage, may rely on centralization and trusted intermediates to varying degrees. Some implementations of Self-Sovereign Identity give considerable power in the hands of a small number of trusted entities that must adhere to a shared contractually binding trust structure, possibly making these entities the network's weakest link. An example is of a governance system using machine-readable showing several problems in the past [21]. Efforts to find the optimal balance between centralization and decentralization should be considered.

6. The underlying Self-Sovereign Identity network may be safe, resilient, and decentralized. Nevertheless, the means for establishing trust among the entities and the trust in data, including the verified credentials transmitted, must be meticulously constructed. Data validation may call for a trusted party external to the blockchain network.

7. As a new identification model, Self-Sovereign Identity necessitates a number of system architectural improvements. Important to the success of Self-Sovereign Identity are dependent on the appropriate technology stacks, deployment methods, user experience considerations and operating procedures. Proper design measures must be made to prevent the fate of several other valuable breakthroughs, *e.g.* Pretty Good Privacy [22], which, although being a helpful technology, has not attained the desired level of widespread adoption [23].

8. Self-Sovereign Identity is a relatively new venture with a growing ecosystem, but with limited knowledge on the revenue model [24], and there are user-acceptance concerns [25]. The adoption of new technology by users relies on service providers' support, and vice versa, which might result in the chicken-and-egg dilemma in the Self-Sovereign Identity economic model.

Altogether, there is enough work to be done to lead Self-Sovereign Identity to a successful implementation. In this work the scope will be narrowed to an European Self-Sovereign Identity use case including interoperability of the European Blockchain Services Infrastructure (EBSI) which is a permissioned peer-to-peer network of nodes that operate a blockchain-based services architecture.

The next Chapter contains relevant literature and the background necessary to fully comprehend this paper. In Chapter 4, a framework will be devoted to address to the aforementioned issues of Self-Sovereign Identity. Chapter 5.1 will provide a State-of-the-Art of the eIDAS regulation with regard to the technical implementation of identification and authorization on the highest level of assurance. Furthermore, this Chapter will give an overview and expectation of the coming revised eIDAS regulation, *i.e.* eIDAS2. Furthermore, Chapter 6 will entail the details of the infrastructure necessary to develop a trustworthy Self-Sovereign Identity implementation, consisting of TrustChain, IPv8 and EBSI. Thereafter, Chapter 7 elaborates on the anchors of trust needed to make the Self-Sovereign Identity ecosystem trustworthy. Specifically, these anchors are the Netherlands Chamber of Commerce's Business Register (KVK Handelsregister), Netherlands Vehicle Authory Vehicle Register (RDW kentekenregister) and the Dutch Personal Records Database (BRP). Consecutively, as mentioned as the first challenge in Self-Sovereign Identity, protocols and practices are needed. Accordingly, in Chapter 8 an EBSI implementation at the Dutch Chamber of Commerce and Netherlands Vehicle Authory is realized and discussed. Providing a template for integrating Qualified Trust Service Providers in the EBSI. Lastly, in Chapter 9 a conclusion is drawn and future work is discussed.

3 Background

4 Design

To successfully solve the issues addressed in the problem description, a model for trust is proposed. The pillars of this design will be discussed further in the coming Chapters. The overhauling goal of Self-Sovereign Identity and all of its applications is to establish online trust. "Trust" means "reliance on the integrity, strength, ability, and surety of a person or thing" [26]. The basis of trust is identification [27]. Having an identity makes it possible to build and map the history, or previous encounters, to that identity [28]. While visual recognition or identification may be used to verify an individual's identity in the physical world, authentication and tokens are used to verify an individual's identity online [29]. In the European Union, there exist a legal framework to establish a legally bounded identification online. Such methods of identification are so far always bound to entities that guarantee the legitimacy of the identification. Examples are the Dutch DigiD and eHerkenning, Italian SPID, and the Swedish BankID. A full list of European Commission approved electronic identifications can be found in [30]. The legal framework for identification is named Electronic Identities And Trust Services also known as eIDAS. As each application requires a different level of trust, the eIDAS framework distinguishing in three different levels of trust namely, 'low', 'substantial' and 'high'. The eIDAS framework includes legal binding in ascending degrees, as the level 'low' and 'substantial' are a subset of the level 'high', the focus of this work will be on the highest level of assurance. Moreover, the implementation provided in 8 would require the highest level of assurance as well. Further elaboration on the legal backbone of trust, eIDAS, is treated in Chapter 5.1. Furthermore, to establish a network of trust, an anchor of legally binding information is needed. Such sources of information is defined in the eIDAS regulation as well and are named Qualified Trust Service Providers. Qualified Trust Service Providers are capable of providing Qualified Electronic Signatures and are considered as the most trustworthy [31]. A complete list of the current Qualified Trust Service Providers can be found in [32]. In our use case. the Netherlands Chamber of Commerce and the Netherlands Vehicle Authority could be Qualified Trust Service Providers providing the legally binding information on the network. Lastly, the identification of a person and the information sources from Qualified Trust Service Providers should communicate and operate on a trustworthy infrastructure. Hence, the last pillar of trust, the infrastructure of the network. In the use case, this will relay on IPv8, TrustChain, and the EBSI. Combining all of these elements brings forth the model of trust shown in Figure 1.

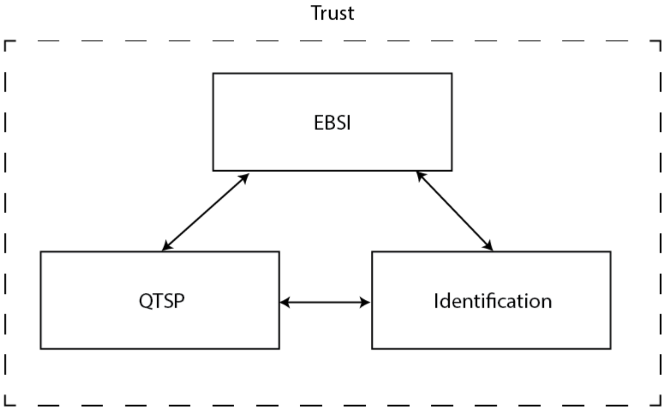


Figure 1: Model of trust

The proposed design aims to solve or provide a considerate answer to the problems addressed in the problem description. The following is a list of how this design will provide solutions or answers to the addressed challenges.

1. This study will contain a guide to eIDAS legislation and an open source solution compliant to EBSI standards to support wallet standardization and data management. While advocate the paradigms of Privacy by Design and Security by Design, as well as be as eIDAS level 'high' compliant as much as possible.
2. Key management will be handled by the TU Delft SSI wallet and guidance in the form of literacy will be provided in the chapter on infrastructure.
3. The design includes minimal necessity of consent to refrain from consent fatigue and will be as made clear as possible.
4. The distributed ledger technology will be permissioned by reason of EBSI being structured in such matter.
5. The accountability of the Self-Sovereign Identity implementation will be distributed over the stakeholders in the system (specifiekere uitleg nodig).
6. The trusted data in our work is assumed to be correct, as the data provided by Netherlands Vehicle Authority and Netherlands Chamber of Commerce is legally binding. Therefore, the data of the Netherlands Chamber of Commerce is 'correct' even if it is incorrect in the Netherlands Chamber of Commerce's database.
7. The expectation is that as soon as the Self-Sovereign Identity wallet made available by the European Commission, the digital identity will be adopted.
8. Accordingly, the imposition of the European Commission will solve the chicken-and-egg dilemma, as the investment to create the infrastructure for European citizens is done by the European Commission. From this, the commercialization can be developed.

5 Identification

'Online identification' is the term used to describe any data which is exposed online and connected to a particular person. Even though they are often associated with personal accounts, such as banking profiles, online identities may include any form of identifiable personal information. The concept of online identities has become increasingly important as a result of the noticeable expansion of the number of online services over the last few years. In the past, an individual could simply submit personal information for a service like an email account, without any additional hurdles. On the contrary, nowadays online identification is crucial to the delivery of services that are for example age-restricted, *i.a.* gambling websites or secure management of data for the financial and medical sectors (bron). In order to establish trust in an online environment online identification is required (bron). In this thesis the scope is narrowed down to the establishment of online trust through the eIDAS regulatory framework. At the moment, governmental organizations of EEA countries (this includes all European Union Member States and Iceland, Liechtenstein, and Norway) typically identify people through their physical passport. For instance, if you hold a Croatian passport, the Netherlands will accept the passport as identification at the border or for other official purposes. For electronic identification however, like DigiD as used in the Netherlands, this is not always the case. Using an electronic identification issued by one country will not automatically be acknowledged by other countries for identification purposes. This discrepancy will be altered as a result of the eIDAS Regulation [33]. Organizations in the public sector that operate within EEA countries are now obliged, according to the eIDAS Regulation, to allow users of national electronic identification systems from other EEA countries, to use their online services. Accordingly, a national electronic identity system may be used in other EEA countries after it has received recognition in the country of the individual's nationality. Currently, the EEA nations adhere to the first version of the eIDAS Regulation.

In Section 5.1, a practical textual and graphic overview of the eIDAS Regulations with respect to levels of assurance is provided. In the subsequent Section (verwijzing fixen) a comparison and overview of the upcoming revision of the eIDAS Regulation (also known as eIDAS 2.0) is presented. The present chapter focuses on providing guidance to becoming a 'high' level of assurance Qualified Trust Service Provider. The chapter also discusses the proposed amendments of the current eIDAS Regulation, which intend to facilitate the wide adoption of online identification means.

5.1 eIDAS

As of 17 September 2014, the Electronic Identities And Trust Services (eIDAS) Regulation entered into force for all European Union (EU) Member States [34],[1] and it has been in effect since the first of July 2016 [34], [35]. The eIDAS Regulation articulates agreements with regard to using the same reliability levels, concepts, and mutual digital infrastructure of electronic identification (eID), *i.a.* in order to ensure the adequate functioning of the internal market [36]. As such, the eIDAS regulatory framework *e.g.* enables secure cross-border transactions for natural and legal persons [36]. One of the merits for the EU's citizens is the possibility of using their national eID within all the Member States of the EU, without the need to establish several different eIDs. In the eIDAS Regulation, the distinct levels of assurance of eIDs are described, whereby the different levels of classification of eIDs are defined, and the systems that can be used to authenticate users are determined. Among other things, three levels of assurance are introduced, namely 'low', 'substantial', and 'high', whereby their respective criteria are set out in Article 8 of the eIDAS Regulation [37]. According to recital 15 of the eIDAS Regulation [37], the assurance level of an eID should be equal to or higher than that of the online service in question, in order for there to exist an obligation to recognize an eID. *I.e.*, there is no obligation to authenticate a user which uses a 'low' level classified eID, when the authority itself requires a 'substantial' or 'high' level of assurance. In the eIDAS Regulation [37], as well as the Commission Implementing Regulation of 8 September 2015 [5] (Level of Assurance Regulation), the levels of assurance are elaborated upon with regard to the regulatory implementation, technical specifications, and theoretical concepts. In order to enhance proper applicability and (future) compliance, the present thesis provides a technically-oriented analysis on achieving the eIDAS different levels of assurance as well as an open source reference implementation. In Article 8 of the eIDAS Regulation, the level of assurance requirements are defined. Although, as indicated before, this thesis will focus on eIDAS compliance with a 'high' level of assurance, the 'low' and 'substantial' levels of assurance will be touched upon as well, as they are essentially a subset thereof.

Levels of Assurance

As indicated prior, the eIDAS Regulation construes three different levels of assurance, namely 'low', 'substantial' and 'high'. In order to comply with any of these levels of assurance, a number of minimum requirements need to be met. These basic criteria can be divided into four different groups of requirements, as indicated in Article 1(2) of the Level of Assurance Regulation [5]: (1) enrolment, (2) eID management, (3) authentication, and (4) management & organisation. Each of these groups contains particular subgroups of requirements. Firstly, the enrolment group contains the subgroups (i) application and registration; identity proofing and verification (ii) for natural persons, and (iii) for legal persons; and (iv) binding between the electronic identification and the natural or legal

[1] See Article 52 of the eIDAS Regulation.

Table 1: eIDAS requirement groups and subgroups for assurance levels of eIDs

Enrolment	**eID management**	**Authentication**	**Management and organisation**
• Application and registration • Identity proofing and verification for a natural person • Identity proofing and verification for a legal person • Binding the eID	• eID characteristics and design • Issuance, delivery and activation • Suspension, revocation and reactivation • Renewal and replacement	• Authentication mechanism	• Information security management • General provisions • Published notices and user information • Record keeping • Facilities and staff • Compliance and audit • Technical controls

person.[2] Secondly, the eID management group contains the requirement subgroups of (i) eID characteristics and design; (ii) issuance, delivery and activation; (iii) suspension, revocation and reactivation; and (iv) renewal and replacement.[3] Furthermore, the group of criteria that focuses on authentication, solely consists of one subgroup, namely authentication mechanism requirements.[4] Lastly, the management and organisation group covers several subgroups, namely one which contains (i) general provisions; one on (ii) published notices and user information; (iii) information security management; (iv) record keeping; (v) facilities and staff; (vi) technical controls; and one regarding (vii) compliance and audit.[5] As such, there are many different requirement groups and criteria subgroups to take into account. In order to create a clearer overview, all of these groups and their corresponding subgroups are visualised in Table 1.

The three different levels of assurance that are described in the eIDAS Regulation, can be used in order to provide a service, such as an the issuance of an eID. The service provider can decide with which level of assurance it wishes to provide the service. Naturally, it then needs to meet the corresponding requirements for the chosen level of assurance. *E.g.*, if a service provider wishes to fulfill the 'substantial' level of assurance, it should meet all the general requirements and the criteria following from the different subgroups, whereby the fulfilment thereof at least meets the qualifications of the 'substantial' or 'high' level of assurance [38]. If the level of assurance would classify as 'low' on any of the given points, this would not suffice for that particular service provider. In the following subsections, the eIDAS Regulation and the Level of Assurance Regulation are described briefly in relation to the different levels of assurance, with the aim to provide a concise summary.

5.1.1 Enrolment

The enrolment for an eID concerns the procedure through which legal and natural persons can apply for the issuance of an eID, that usually demands proper proof for the verification of their identity.[6] In the subsequent subsections the various processes and requirements for obtaining an eID are described, whereby the different levels of assurance will be discussed as well. The subsections will follow the structure wherein the requirement subgroups are introduced in paragraph 2.1 of the Annex to the Level of Assurance Regulation [5].

Application and registration

The eIDAS Regulation criteria with regard to the application and registration process, consists of three elements. First of all, it is necessary that the service provider ensures that the applicant is aware of the terms and conditions that apply when using the eID. Secondly, it should be ensured too that the applicant is aware of any security precautions that are recommended in relation to the eID. Lastly, the service provider should collect relevant identity data from the applicant, in order to enable the proofing and verification of the applicant's identity. Although these three elements apply to all three assurance levels whereby no distinction is made between them, it is

[2] Paragraph 2.1 of Annex to Level of Assurance Regulation [5].
[3] Paragraph 2.2 of Annex to Level of Assurance Regulation [5].
[4] Paragraph 2.3 of Annex to Level of Assurance Regulation [5].
[5] Paragraph 2.4 of Annex to Level of Assurance Regulation [5].
[6] Article 8(3)(b) eIDAS Regulation [34].

important to note that the specific data that is demanded from the applicant, differs per eID assurance level. An overview of the disparities in that regard, is provided in Table X (to be created).

Natural person identity proofing and verification

The Level of Assurance Regulation [5] discusses the proofing and verification process for natural persons and legal persons in distinct paragraphs. With regard to the proofing and verification of natural persons, the Regulation elaborates upon the specific requirements for the three different levels of assurance separately. For a 'low' level of assurance, three criteria are introduced. The first requirement is, that it can be assumed that the natural person has evidence of their identity that is recognised by the Member State in which territory the application is made, *i.e.* a Member State passport. The second requirement is that the evidence of the identity is presumably real and that it seems valid. The third requirement for a 'low' level of assurance, is that there is an authoritative entity that is aware of the fact that the provided identity exists, and that it can be assumed that the natural person corresponds to the presented identity.

If a service provider however wishes to enhance the level of assurance, and therefore wishes to apply a 'substantial' level of assurance, these three requirements are equally applicable. Nevertheless, an additional requirement should be met. The Regulation provides four alternative sets of requirements of which (at least) one set should be completely fulfilled. The first set of requirements consists of three subcriteria, namely (a) that it has been verified that the natural person possesses evidence of the indicated identity; and (b) that the evidence has been examined in light of its validity, or that an authoritative source has confirmed that such evidence exists and belongs to a real natural person; and lastly, (c) adequate measures have been taken in order to diminish the chances that an individual falsely claimed the presented identity. The Regulation specifically points at *i.a.* instances of theft or expiration of evidence. The second alternative set of requirements that would fulfill the 'substantial' level of assurance, if combined with the criteria of the 'low' level of assurance, consists of two cumulative subrequirements. The first subcriterion is the presentation of an identity document during the enrolment process within the Member State that issued the document, whereby the identity document appears to relate to the individual who has provided it. The second subcriterion is almost identical to the third subrequirement of the former set of criteria, and relates to the taking of measures in order to lower the risk that identity is falsely claimed, for example due to taking into account the possibility of theft, expiration or revocation. The third and fourth set of requirements, only contain one subrequirement each. They both relate to instances where the identity of the natural person has already been verified with at least a 'substantial' level of assurance, *e.g.* for a different purpose. In such cases, it is not necessary to repeat the identity proofing and verification. The equivalent level of assurance should then be confirmed by a conformity assessment body [39]. The conformity assessment body determines if the substantial level of assurance reliability criteria have been met. The list of accredited conformity assessment bodies concerning eIDAS identity proofing and verification can be found in [40].

Finally, in order to obtain a 'high' level of assurance for identity proofing and verification, one of the following two criteria needs to be met. The first option is that one complies fully with the 'substantial' level requirements and in addition to that, one meets one of the following three combinations of criteria, namely: (a) the natural person possesses a photo or biometric identification evidence, which is recognized by the Member State where the application for the eID is made. The presented evidence is verified by an authoritative source with regard to validity, and the individual has been identified through verification of at least one physical characteristic, when comparing the person to the provided evidence; the second option is that (b) the person has previously been verified for another purpose by a public or private entity, whereby an equivalent level of assurance was applied. This process does not have to be repeated, if the service provider takes sufficient measures to ensure that the previous check is still valid; (c) The last subcriterion is quite similar to the former, however if focuses upon instances where a notified eID was issued. Alternatively, applicants can comply with the 'high' level of assurance if the same procedures are followed for the application for the eID, as for the application for *i.a.* biometric identification evidence within a Member State. Interestingly, this could mean that the applicant needs to physically appear before the service providing entity. Moreover, the Level of Assurance Regulation essentially indicates that if the aforementioned criterion is met, it is not necessary to comply with any of the other discussed requirements, nor with any of the corresponding lower levels of assurance.

Legal person identity proofing and verification

Legal persons such as corporations or governmental bodies, can apply too for an eID. For the proofing and verification of the identity of a particular legal person at a 'low' level of assurance, three cumulative requirements have to be adhered to. Firstly, the evidence that is provided in order to claim the identity of the legal person, should be recognised by the Member State where the application for the eID is being made. Secondly, the evidence must seem valid, and it should be possible to assume that the evidence is genuine, or that it exists according to an authoritative source. Thirdly, to the authoritative source, the legal person should not appear to be in a state in which it would not be possible to act as that legal person, *e.g.* in instances where the legal person has been revoked.

If alternatively the service provider wishes to comply with the 'substantial' level of assurance, one of the following three requirements need to be met, in addition to all the criteria that follow from the 'low' level of assurance. The first requirement entails a set of three subrequirements which indicate that (a) the claimed identity for the legal person is demonstrated by evidence which is recognised by the Member State where the eID is being requested, and that certain data, such as the name of the legal person, is included; further, that (b) the evidence is checked for authenticity and that its existence according to an authoritative source is verified; and lastly, that (c) precautions are taken in order to minimize the risk of false applications, for example due to lost or stolen evidence. Alternatively, if the proofing and verification has yet occurred in a previous procedure, it is not necessary to repeat this process, provided that the previous level of assurance corresponds to 'substantial' or 'high', and that it is confirmed by a conformity assessment body. The last alternative criterion is similar to the former, however it focuses on valid notified eIDs.

Finally, for a 'high' level of assurance, it is necessary that all the requirements of the 'substantial' level of assurance are met, in conjunction with (at least) one of the following additional requirements. The first option is that the identity being claimed is being demonstrated by evidence that is verified with regard to its validity by an authoritative source. The second option is that the proofing and verification procedure has previously taken place for other purposes, whereby the level of assurance was 'high', as has been confirmed by a conformity assessment. Moreover, it should be demonstrated that the outcome of such previous verification procedure is still valid. Lastly, there is a third option which again is quite similar to the former one, although with a focus on valid notified eIDs.

Binding between natural and legal persons and the eID

The eIDAS Regulation identifies conditions for the binding of an eID of a natural person to the eID of a legal person. The Level of Assurance Regulation specifically indicates that it should be possible to suspend and revoke a binding. Furthermore, it is established that a natural person that is bound to a legal person should be able to delegate the binding of that legal person to another natural person, for which nationally recognized procedures must be followed. The Level of Assurance Regulation further stipulates how the binding process should take place with regard to the different levels of assurance. To adhere to the ‘low’ level of assurance, three cumulative requirements should be met for the binding. Namely firstly, when a natural person is acting on behalf of a legal person, it must be verified that the identity proofing of the natural person has taken place at the assurance level ‘low’ or higher. Moreover, the application and registration which led to the binding, must have followed nationally recognised procedures of the Member State where the binding was established. Lastly, the natural person must not be known by an authoritative source as having a status that would prevent the individual from acting on behalf of the legal person, *e.g.* a natural person being forbidden to act on behalf of the legal person due to the natural person being under criminal investigation.

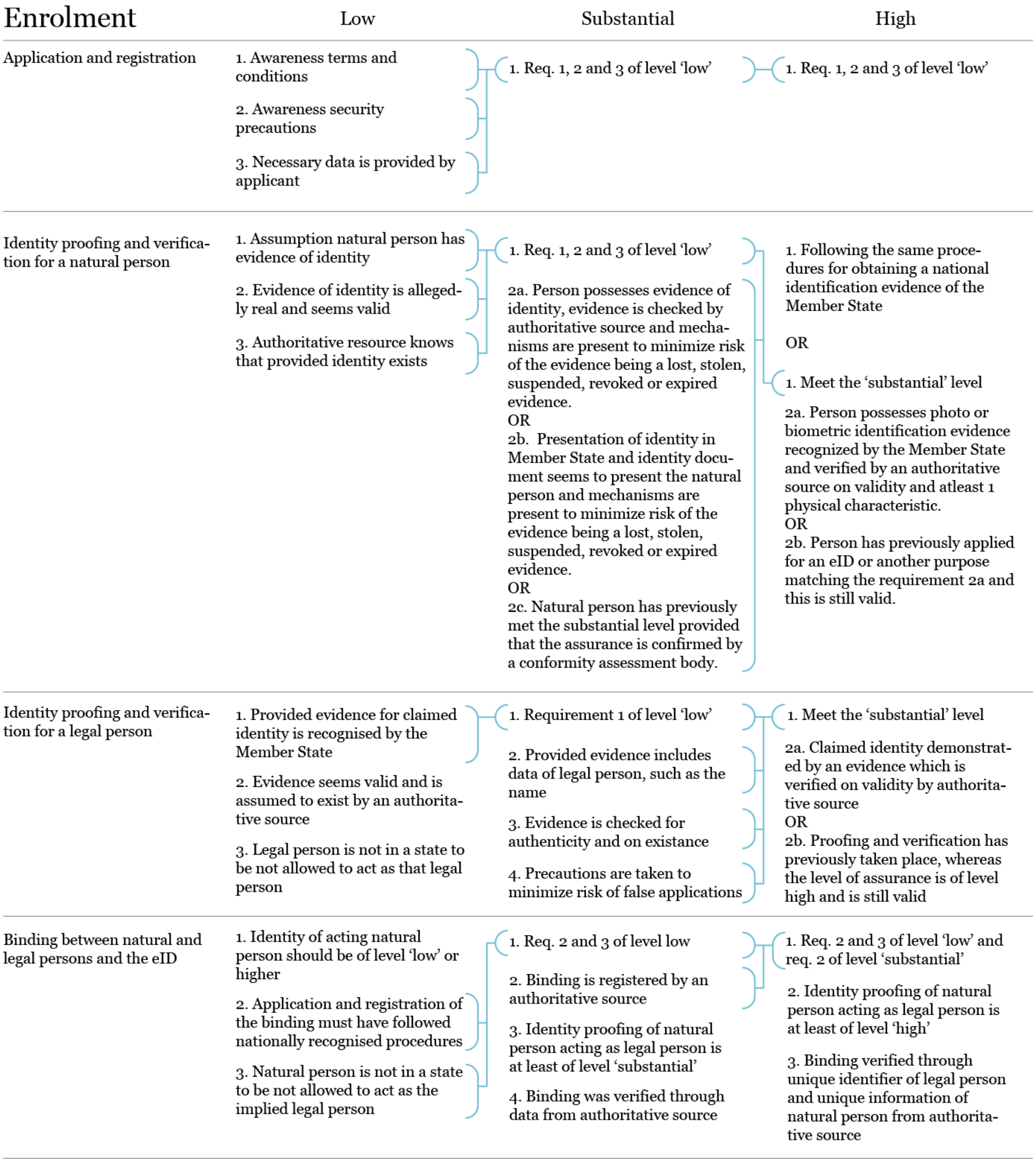
The latter requirement is also essential in order to obtain a ‘substantial’ level of assurance for binding, and the same is true for acquiring the ‘high’ level of assurance. Additionally, for both the ‘substantial’ and ‘high’ level, the second criterion of the ‘low’ level of assurance similarly applies, namely demanding that nationally recognized procedures are followed in the establishment of the binding. Nonetheless, an additional element thereby requires that the binding is registered in an authoritative source. Moreover, two other requirements need to be met. The first additional requirement is that the identity proofing of the natural person who acts on behalf of the legal person, took place on the levels ‘substantial’ or ‘high’. The second requirement demands that the binding was verified through data from an authoritative source.

Lastly, to conform with a ‘high’ level of assurance, apart from the previously discussed requirements (see the paragraph concerning the ‘substantial’ level of assurance, indicating that the nationally recognized procedures should be followed, as well as registration of the binding at an authoritative source, and that the natural person should not have a status that prevents them from acting on behalf of the legal person), two additional criteria should be met. Firstly, the proofing of identity must have been verified on a ‘high’ level of assurance. Finally, the binding should be verified through a unique identifier that relates to the legal person, as well as unique information from an authoritative source that relates to the natural person.

In Figure 2 a summarized overview of the enrolment level of assurance requirements is provided.

5.1.2 eID Management

The management of eIDs needs to meet specific standards, which naturally differ per assurance level. These elements will be discussed in the following paragraph, whereby the structure of paragraph 2.2 of the Level of Assurance Regulation [5] is followed.



Enrolment	Low	Substantial	High
Application and registration	1. Awareness terms and conditions 2. Awareness security precautions 3. Necessary data is provided by applicant	1. Req. 1, 2 and 3 of level ‘low’	1. Req. 1, 2 and 3 of level ‘low’
Identity proofing and verification for a natural person	1. Assumption natural person has evidence of identity 2. Evidence of identity is allegedly real and seems valid 3. Authoritative resource knows that provided identity exists	1. Req. 1, 2 and 3 of level ‘low’ 2a. Person possesses evidence of identity, evidence is checked by authoritative source and mechanisms are present to minimize risk of the evidence being a lost, stolen, suspended, revoked or expired evidence. OR 2b. Presentation of identity in Member State and identity document seems to present the natural person and mechanisms are present to minimize risk of the evidence being a lost, stolen, suspended, revoked or expired evidence. OR 2c. Natural person has previously met the substantial level provided that the assurance is confirmed by a conformity assessment body.	1. Following the same procedures for obtaining a national identification evidence of the Member State OR 1. Meet the ‘substantial’ level 2a. Person possesses photo or biometric identification evidence recognized by the Member State and verified by an authoritative source on validity and atleast 1 physical characteristic. OR 2b. Person has previously applied for an eID or another purpose matching the requirement 2a and this is still valid.
Identity proofing and verification for a legal person	1. Provided evidence for claimed identity is recognised by the Member State 2. Evidence seems valid and is assumed to exist by an authoritative source 3. Legal person is not in a state to be not allowed to act as that legal person	1. Requirement 1 of level ‘low’ 2. Provided evidence includes data of legal person, such as the name 3. Evidence is checked for authenticity and on existance 4. Precautions are taken to minimize risk of false applications	1. Meet the ‘substantial’ level 2a. Claimed identity demonstrated by an evidence which is verified on validity by authoritative source OR 2b. Proofing and verification has previously taken place, whereas the level of assurance is of level high and is still valid
Binding between natural and legal persons and the eID	1. Identity of acting natural person should be of level ‘low’ or higher 2. Application and registration of the binding must have followed nationally recognised procedures 3. Natural person is not in a state to be not allowed to act as the implied legal person	1. Req. 2 and 3 of level low 2. Binding is registered by an authoritative source 3. Identity proofing of natural person acting as legal person is at least of level ‘substantial’ 4. Binding was verified through data from authoritative source	1. Req. 2 and 3 of level ‘low’ and req. 2 of level ‘substantial’ 2. Identity proofing of natural person acting as legal person is at least of level ‘high’ 3. Binding verified through unique identifier of legal person and unique information of natural person from authoritative source

Figure 2: Enrolment assurance level requirements

Characteristics and Design

For a ‘low’ level of assurance, the eID needs to ensure the usage of at least a single factor authentication and is designed such that it can be assumed that the person owning the eID is in control. The substantial assurance level is met if the eID uses a minimum of two factor authentication and is designed such that it is supposed that the person owning the eID is in control. The high level of assurance requires the requirements of the substantial level along with two additional requirements. Namely, the eID provides protection against copying, faking and other attacks. Furthermore, the eID should be designed such that it can be reliably protected in the case that other unauthorized persons use it.

Issuance, Delivery and Activation

For a low level of assurance, the issuance mechanism of the eID is made such that it can be assumed that the intended person was reached. The substantial level requires the issuance mechanism of the eID to be such that it can be assumed that the eID is only in the possession of the person to whom the eID belongs. With regard to the high level of assurance, the issuance of an eID requires an activation process in which it is verified that the eID is delivered to the person to whom the eID belongs.

Suspension, Revocation and Reactivation

Concerning the suspension, revocation and reactivation of the eID, the level of assurance requirements are equal for all levels. The first requirement entails, the possibility to suspend or revoke the eID timely and effectively. Secondly, there exists mechanisms to prevent unauthorized suspensions, revocations and reactivations. Lastly, the eID can only be reactivated if the assurance requirements are met which were in effect prior to the suspension or revocation.

Renewal and Replacement

In the use case of a renewal or replacement of an eID, the low and substantial level of assurance require taking into account a change of a person's identification data. Furthermore, it requires the same assurance requirements as the initial process of identity proofing and verification. Alternatively, a valid evidence of an eID of the same or higher level of assurance is provided. With respect to the high level of assurance, in the case an eID is used for the renewal or replacement of the eID, the identity data has to be verified at an authoritative source.

In Figure 3 a graphical overview of the eID management assurance level requirements is provided.

5.1.3 Authentication

With regard to the low level of assurance, the first requirement is that prior to releasing person identification data, the eID and its validity is verified. The second requirement involves, in case the authentication mechanism entails the storage of a person's identity, the data has to be protected against loss, compromising and offline analysis. The third requirement oughts the authentication mechanism to provide security measurements for making it unlikable against multiple methods of bypassing the authentication process *viz.* guessing, eavesdropping, replay and communication manipulation. Concerning the substantial level of assurance, all low level requirements should be met along with two more requirements. Specifically, prior to releasing person identification data, the eID and its validity is verified by using of dynamic authentication. Dynamic authentication is a method to provide a proof of an eID where the provided proof is different each time, hence dynamic. Additionally, the substantial level requires measurements in order to make it highly unlikely to bypass the authentication process. To reach the high level of assurance, the authentication mechanism has to consider attackers bypassing the authentication method with a high attack potential.

Figure 4 provides a graphical summary of the authentication assurance level criteria.

5.1.4 Management and Organisation

General Provisions

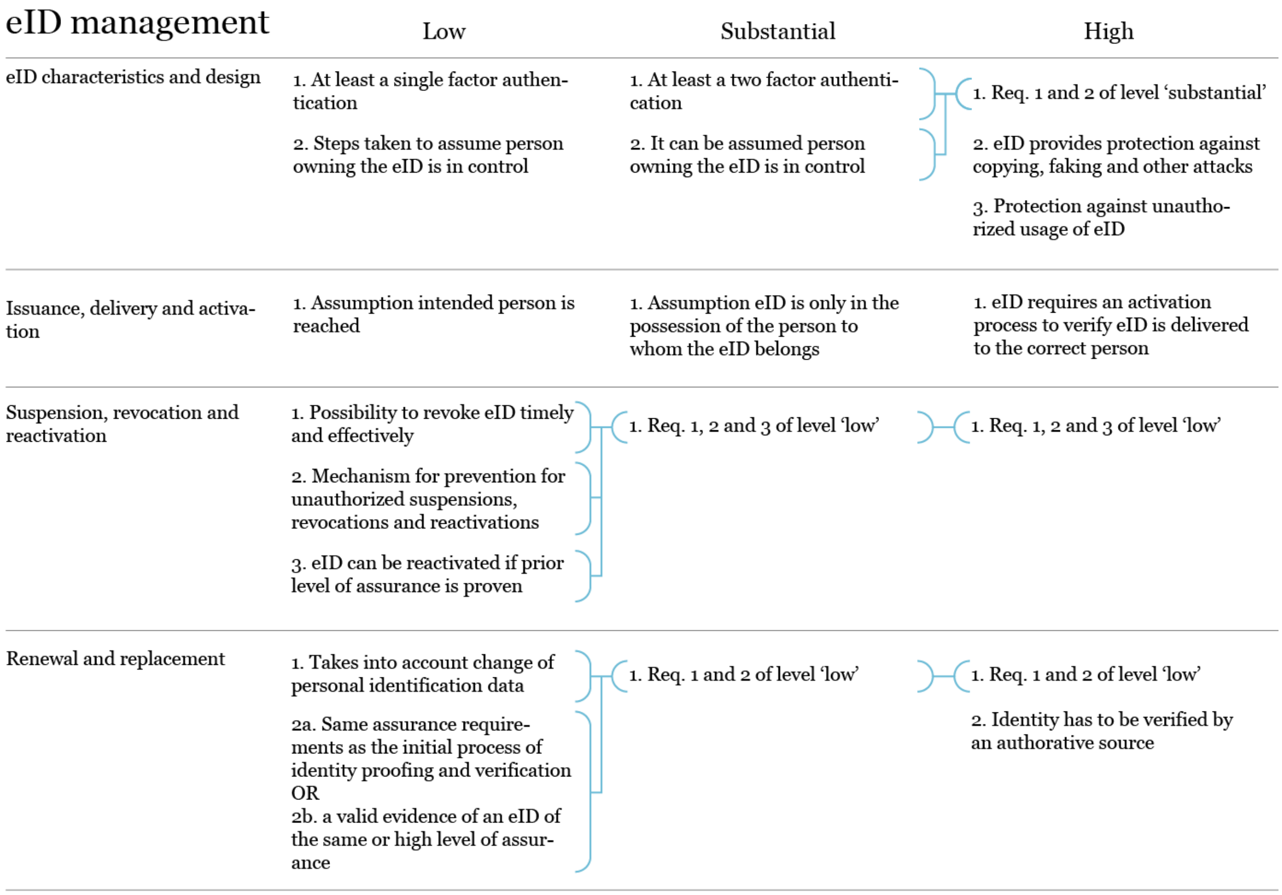
The requirements concerning general provisions are identical for all levels of assurance. There are five general provisions to comply to fulfill all assurance levels. First off, service providers covered by this regulation, should be governmental institutions or legal persons which are recognised by the Member State. Secondly, the providers of a service have to comply to all their legal obligations *i.a.* the kinds of information the service may request, the procedure of the request, the information the service is allowed to store and for how long. Thirdly, the service provider can proof to have sufficient financial resources for operation and possible liability damage. Fourthly, the service provide is responsible for all their outsourced business. Fifthly, eID services should have a plan of termination. Which includes a provisions for a shutdown or continuation by another service provider, how the user is notified, how the administration is protected, stored or deleted.

Published Notices and User Information

Regarding the published notices and user information, three requirements have to be satisfied to meet all levels of assurance. The first requirement, there is a public available description of the applicable terms, conditions, fees, usage limitations and privacy. Furthermore, in case of a change of the aforementioned information, there should be a procedure to notify users timely. Lastly, it should be possible to request information about the service which are answered appropriately.

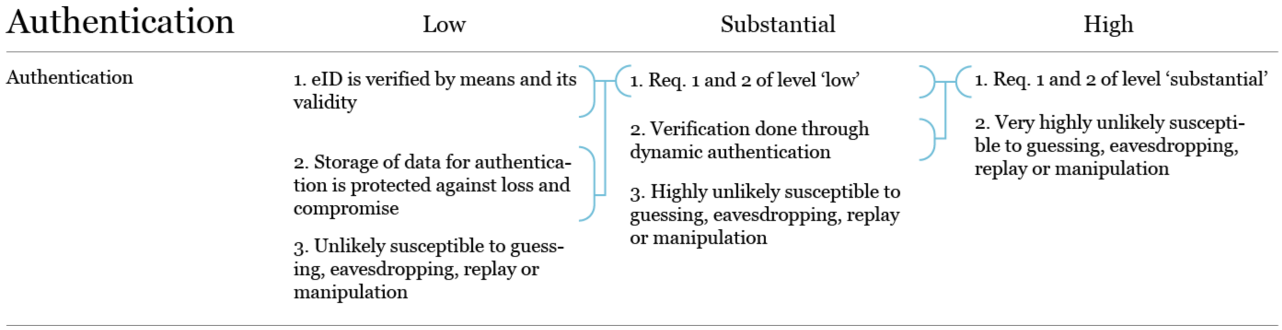
Information Security Management

To reach the low level of assurance, an information security system that takes care of the management of information security risks and the management thereof. To fulfil the substantial level, the information security system has to adhere to proven standards regarding information security risks and management. The high level of assurance corresponding to information security management is the same as the substantial level.



eID management	Low	Substantial	High
eID characteristics and design	1. At least a single factor authentication 2. Steps taken to assume person owning the eID is in control	1. At least a two factor authentication 2. It can be assumed person owning the eID is in control	1. Req. 1 and 2 of level 'substantial' 2. eID provides protection against copying, faking and other attacks 3. Protection against unauthorized usage of eID
Issuance, delivery and activation	1. Assumption intended person is reached	1. Assumption eID is only in the possession of the person to whom the eID belongs	1. eID requires an activation process to verify eID is delivered to the correct person
Suspension, revocation and reactivation	1. Possibility to revoke eID timely and effectively 2. Mechanism for prevention for unauthorized suspensions, revocations and reactivations 3. eID can be reactivated if prior level of assurance is proven	1. Req. 1, 2 and 3 of level 'low'	1. Req. 1, 2 and 3 of level 'low'
Renewal and replacement	1. Takes into account change of personal identification data 2a. Same assurance requirements as the initial process of identity proofing and verification OR 2b. a valid evidence of an eID of the same or high level of assurance	1. Req. 1 and 2 of level 'low'	1. Req. 1 and 2 of level 'low' 2. Identity has to be verified by an authorative source

Figure 3: eID Management assurance level requirements



Authentication	Low	Substantial	High
Authentication	1. eID is verified by means and its validity 2. Storage of data for authentication is protected against loss and compromise 3. Unlikely susceptible to guessing, eavesdropping, replay or manipulation	1. Req. 1 and 2 of level 'low' 2. Verification done through dynamic authentication 3. Highly unlikely susceptible to guessing, eavesdropping, replay or manipulation	1. Req. 1 and 2 of level 'substantial' 2. Very highly unlikely susceptible to guessing, eavesdropping, replay or manipulation

Figure 4: Authentication assurance level requirements

Record Keeping

For record keeping, relevant information has to be stored and maintained as long as the Member State law requires to store the record keeping for auditing. After the duration of storing the record keeping data, the data can be destroyed securely. This requirement is the same for all levels of assurance.

Facilities and Staff

To comply with all levels of assurance, four requirements are to be fulfilled for those covered by this regulation. Firstly, the staff, including outsourced, are qualified to fulfil their tasks. Secondly, there is enough personnel to fulfil all necessary tasks. Thirdly, the facilities of the service provider are protected against environmental influences and unauthorized access. Lastly, the access to data is restricted to strictly the authorized personnel.

Technical Controls

To meet the low level of assurance in technical controls, five requirements should be met. Namely, there exists protection and controls to manage risks opposed to the confidentiality, integrity and availability of the information processed. Additionally, the communication channels between eID holder and service provider are protected against eavesdropping, manipulation and replay attacks. As well as, encrypted information is decrypted only when access is strictly necessary and decrypted information is never stored. The ability should exist to respond in case of an incident or a security breach. Lastly, all media have to be stored, transported and disposed in a safe and secure way. To comply with the substantial and high level of assurance, the data used for eID and authentication have to be protected from tampering.

Compliance and Audit

For the compliance and audit of the eIDAS low level of assurance, periodical internal audits have to be performed to ensure that the regulations are followed. To adhere to the substantial level of assurance, periodical independent internal or external audits have to be conducted. For the compliance of the high level of assurance, the periodic independent audits can only be performed by an external party. Additionally, in case the service is managed by a governmental body, the auditing is done according through the national law.

A graphical summary of the criteria for the management and organisation of the service provider is shown in Figure 5.

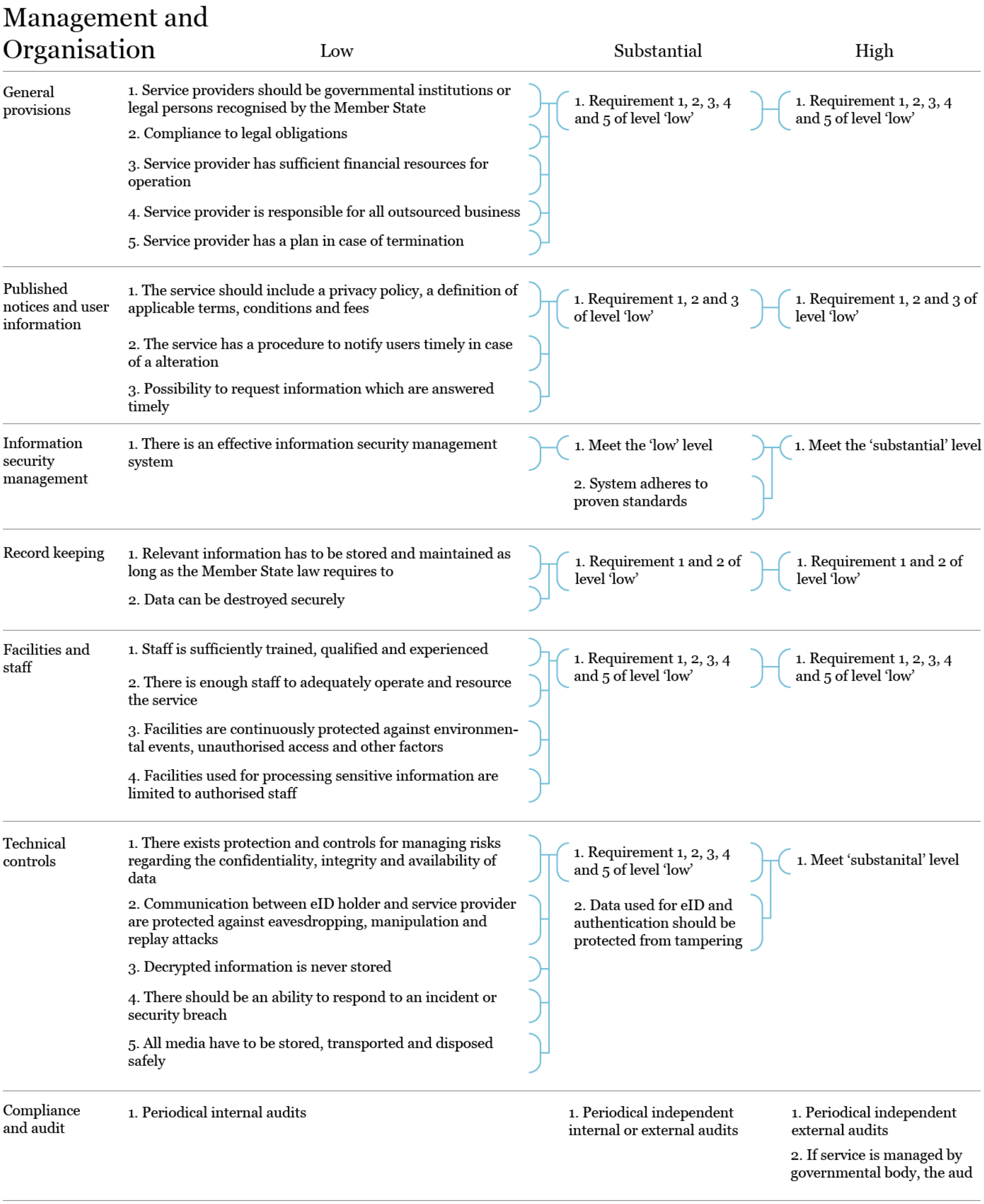
5.2 eIDAS 2.0

The European Union is currently in the process of amending the eIDAS legislation [41]. There are no changes proposed to Article 8, which concerns the levels of assurance and the respective requirements. Accordingly, the previous section will remain up-to-date and relevant in that regard. Nevertheless, there are amendments proposed through which the European Commission opts for an 80% adoption of digital identification for its citizens by the year 2030 [42]. This target, among other reasons, led to the proposal [41] of changing the original eIDAS Regulation [37], do note that this Section covers the proposal of the amendment which is still subject to change.

The 2014 eIDAS Regulation did not satisfy the vision of the European Commission as the structure imposed by it did not enable the market demand to be satiated. Meanwhile, private sector efforts did successfully address this issue as they managed to respond to the market demand. Accordingly, the private sector developed authentication services which are currently frequently used to access online services. The downside of this is that these organizations are not bound by the eIDAS Regulation and as such, they do not provide the same level of legal certainty, data protection, and privacy because they are self-asserted and not linked to reliable and secure governmental eIDs [43]. The Commission's Expert group on regulatory barriers to financial innovation [44] and the Expert group on electronic identification and know-your-customer [45] both acknowledged that national governmental bodies within the EU have varying standards with regard to their compliance of technical solutions for digital identity verification. Furthermore, the European Commission's review of the eIDAS framework also showed that the present regulatory framework is insufficient to meet changing market desires [46]. Therefore, the Commission anticipates that the security and control provided by the enhanced eIDAS framework will provide all EU citizens with the ability to determine precisely who has access to their eID. Additionally, a high degree of security will be needed for the infrastructure for the collection, storage, and disclosure of digital identity data, as well as for all elements related to digital identity provisioning, such as the creation of a European digital identity wallet. Subsequently, the goals of the eIDAS amendment are to provide EU citizens with full control over their personal data and ensure their security when using digital identity solutions and ensure equal conditions for the provision of qualified trust services in the EU, as well as their acceptance. Furthermore, provide access to trusted and secure digital identity solutions that can be used across borders, meeting user expectations and market demand and ensure that public and private services can rely on trusted and secure digital identity solutions across borders.

The amendment would solve the eIDAS issues identified by the evaluations by making the framework more efficient through expanding its advantages to the commercial sector and opening it for mobile usage. Within a year after the Regulation is enforced, it envisions that each Member State will provide a European digital identity wallet [7]. Any European digital identity wallet must either be issued by a Member State, operate under its authority, or exist independently while being acknowledged by that state. Therefore, Member States will create digital wallets that enables citizens to connect their national digital identities in order to identify themselves to services, for example for a bank account. With regard to the issuance of wallets, public or private organizations may issue such wallets as long as they are recognized by a Member State. Interestingly, the amendment does not

[7] Article 6a of the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 [41].



Management and Organisation	Low	Substantial	High
General provisions	1. Service providers should be governmental institutions or legal persons recognised by the Member State 2. Compliance to legal obligations 3. Service provider has sufficient financial resources for operation 4. Service provider is responsible for all outsourced business 5. Service provider has a plan in case of termination	1. Requirement 1, 2, 3, 4 and 5 of level 'low'	1. Requirement 1, 2, 3, 4 and 5 of level 'low'
Published notices and user information	1. The service should include a privacy policy, a definition of applicable terms, conditions and fees 2. The service has a procedure to notify users timely in case of a alteration 3. Possibility to request information which are answered timely	1. Requirement 1, 2 and 3 of level 'low'	1. Requirement 1, 2 and 3 of level 'low'
Information security management	1. There is an effective information security management system	1. Meet the 'low' level 2. System adheres to proven standards	1. Meet the 'substantial' level
Record keeping	1. Relevant information has to be stored and maintained as long as the Member State law requires to 2. Data can be destroyed securely	1. Requirement 1 and 2 of level 'low'	1. Requirement 1 and 2 of level 'low'
Facilities and staff	1. Staff is sufficiently trained, qualified and experienced 2. There is enough staff to adequately operate and resource the service 3. Facilities are continuously protected against environmental events, unauthorised access and other factors 4. Facilities used for processing sensitive information are limited to authorised staff	1. Requirement 1, 2, 3, 4 and 5 of level 'low'	1. Requirement 1, 2, 3, 4 and 5 of level 'low'
Technical controls	1. There exists protection and controls for managing risks regarding the confidentiality, integrity and availability of data 2. Communication between eID holder and service provider are protected against eavesdropping, manipulation and replay attacks 3. Decrypted information is never stored 4. There should be an ability to respond to an incident or security breach 5. All media have to be stored, transported and disposed safely	1. Requirement 1, 2, 3, 4 and 5 of level 'low' 2. Data used for eID and authentication should be protected from tampering	1. Meet 'substanital' level
Compliance and audit	1. Periodical internal audits	1. Periodical independent internal or external audits	1. Periodical independent external audits 2. If service is managed by governmental body, the aud

Figure 5: Management and organisation assurance level requirements

mention any specific technology, leaving the door open for innovation. The official identification information supplied by Member States will be included in the proposed European digital identity wallet as electronic attestations of attributes. The proposed Regulation's article 6a mandates that Member States adhere to the European cybersecurity certification structure created by the Cybersecurity Act, including a mandatory conformity assessment. The proposal also establishes strict requirements for data protection and privacy for the issuer of the European digital identity wallet and for QTSP's attestations of attributes, including GDPR compliance. Furthermore, article 6a states that the user should have complete control over the wallet. Additionally, the amendment also includes a revision that forces web browser manufacturers to make it easier to utilize certified certificates for website authentication. This is done to guarantee users to be able to tell who is in charge of a certain website. To ensure enactment, accredited public or private sector organizations chosen by Member States will certify that European digital identity wallets comply to these standards. The Commission will lay out a procedure to promote a shared approach enabling Member States and other stakeholders to work toward the creation of a toolbox [47]. By outlining the technological architecture, common standards, best practices, and guidelines for the European digital identity framework, this toolkit will hasten the work in order to fulfill the 12 month time frame for a European digital identity wallet to be approved in each Member State. By these measurements the European Commission banks on achieving the aforementioned goals.

6 Infrastructure

6.1 TrustChain

6.2 IPv8

6.3 EBSI compliance

7 Qualified Trust Service Providers

7.1 Legally binded trust

7.2 KVK Handelsregister

7.3 RDW Vehicle Register

7.4 Basisregistratie Personen

8 Implementation

9 Conclusion

9.1 Future Work

- Implement decentralized identification with eIDAS level high assurance.

References

[1] A. van Huffelen, M. Adriaansens, and D. Yeşilgöz-Zegerius, "Kamerbrief hoofdlijnen beleid voor digitalisering." [Online]. Available: https://www.rijksoverheid.nl/documenten/kamerstukken/2022/03/08/kamerbrief-hoofdlijnen-beleid-voor-digitalisering

[2] Feb 2022. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

[3] Nov 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

[4] U. Leyen, "State of the union address by president von der leyen at the european parliament plenary," Sep 2020. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

[5] The European Commission, "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," 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1502&from=ES.

[6] V. Mokshagundam, "Top social login tools compared," Jan 2017. [Online]. Available: https://medium.com/@Vamshi_Mokshagundam/top-social-login-tools-compared-b350eae26118

[7] O. Tene and J. Polonetsky, "Big data for all: Privacy and user control in the age of analytics," Apr 2013. [Online]. Available: https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1/

[8] eIDAS Expert Group, "The toolbox process," 2021. [Online]. Available: https://webgate.ec.europa.eu/regdel/web/meetings/2409/documents/6690

[9] D. Mahajan, O. Sperling, and O. White, "Digital id: The opportunities and the risks — mckinsey & company." [Online]. Available: https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/digital-id-the-opportunities-and-the-risks

[10] C. Allen, "The path to self-sovereign identity," Apr 2016. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

[11] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," 2010.

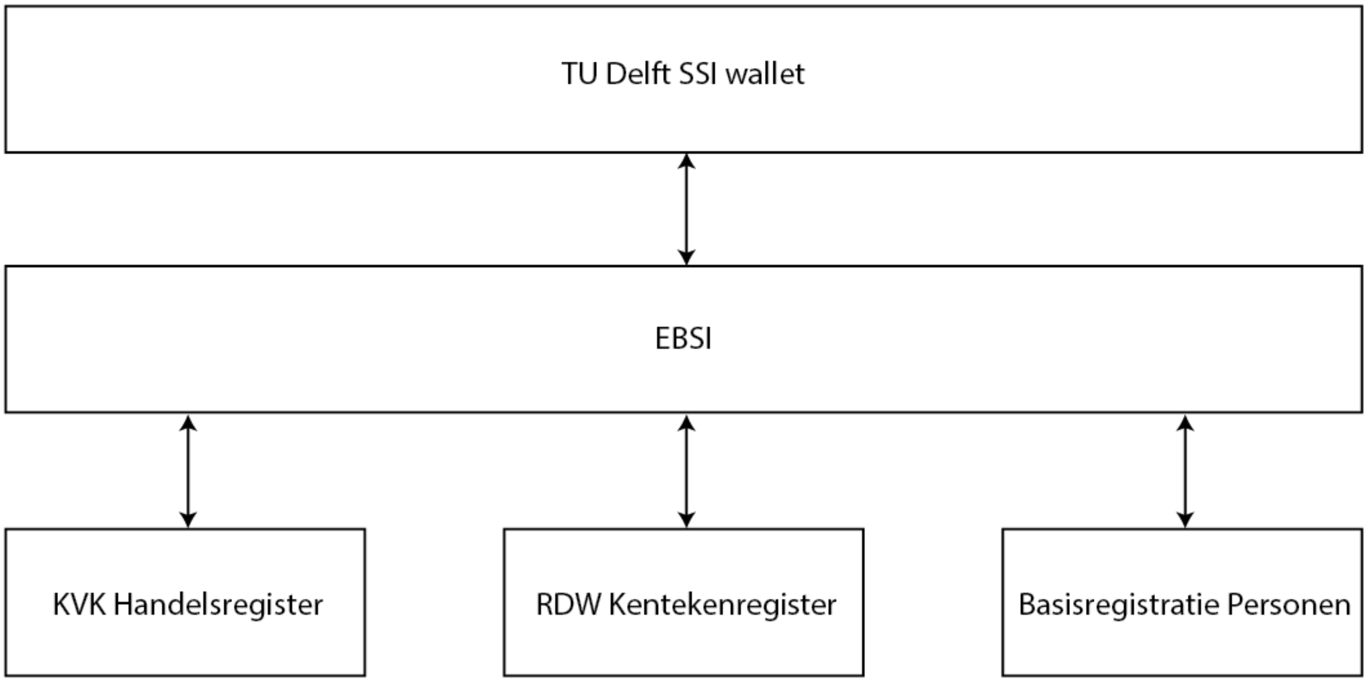


Figure 6: Overview implementation TU Delft, EBSI, RDW, BRP, and KVK

[12] T. Speelman, “Self-sovereign identity: Proving power over legal entities,” Jul 2020. [Online]. Available: https://repository.tudelft.nl/islandora/object/uuid%3Aaab1f3ff-da54-47f7-8998-847cb78322c8

[13] Jun 2021. [Online]. Available: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_nl

[14] R. Soltani, U. T. Nguyen, and A. An, “A survey of self-sovereign identity ecosystem,” *Security and Communication Networks*, vol. 2021, pp. 1–26, jul 2021. [Online]. Available: https://doi.org/10.1155%2F2021%2F8873429

[15] H. Montgomery, “Japanese man lost a usb drive with entire city’s personal data after a night out,” Jun 2022. [Online]. Available: https://www.vice.com/en/article/wxn88x/japanese-man-lost-usb-drive-entire-city

[16] M. Brown, “Top 5 biggest lost bitcoin fortunes,” 2022. [Online]. Available: https://www.cryptovantage.com/news/the-top-5-biggest-lost-bitcoin-fortunes-that-we-know-about/

[17] R. Soltani, U. T. Nguyen, and A. An, “Decentralized and privacy-preserving key management model,” in *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, 2020, pp. 1–7.

[18] K. Vidhani, V. Banahatti, and S. Lodha, “Challenges in enabling privacy self management,” *CSI Transactions on ICT*, 10 2021.

[19] T. Neudecker and H. Hartenstein, “Network layer aspects of permissionless blockchains,” *IEEE Communications Surveys & Tutorials*, vol. PP, pp. 1–1, 09 2018.

[20] Dec 2018. [Online]. Available: https://coinstelegram.com/crypto-alphabet/benefits-and-drawbacks-of-permissioned-blockchains/

[21] M. Sørensen, M. Milkov, and A. K. Angelov, “Decentralized identity management system for self-sovereign identity,” Jun 2018. [Online]. Available: https://projekter.aau.dk/projekter/en/studentthesis/decentralized-identity-management-system-for-selfsovereign-ide .html

[22] S. Garfinkel, D. Russell, and T. Phung, *PGP: Pretty Good Privacy*, ser. Encryption for everyone. O’Reilly Media, Incorporated, 1995. [Online]. Available: https://books.google.nl/books?id=cSe_0OnZqjAC

[23] S. Garfinkel, *Pretty Good Privacy (PGP)*. GBR: John Wiley and Sons Ltd., 2003, p. 1421–1422.

[24] S. Hori, “Self-sovereign identity: future of personal data ownership? — world

economic forum," Aug 2021. [Online]. Available: https://www.weforum.org/agenda/2021/08/self-sovereign-identity-future-personal-data-ownership/

[25] A. Slater, "On self-sovereign identity: What's the business value of ssi? — hackernoon," Nov 2019. [Online]. Available: https://hackernoon.com/self-sovereign-identity-what-is-the-business-value-uq6l36wh

[26] [Online]. Available: https://www.dictionary.com/browse/trust

[27] Z. Aljazzaf, M. Perry, and M. Capretz, "Online trust: Definition and principles," pp. 163 – 168, 10 2010.

[28] M. Daignault, M. Author, S. Marche, and C. Watters, "Enabling trust online," pp. 3 – 12, 02 2002.

[29] M. Lughu, "The attitude of trust showed by king david in holy bible in the book of psalm "the literary work through poetry for character education"," *Journal of English Language and Literature Teaching*, vol. 4, 07 2019.

[30] Sep 2019. [Online]. Available: https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

[31] V. Allen, "What is a trust service provider?" Jan 2021. [Online]. Available: https://blog.ascertia.com/what-is-a-trust-service-provider

[32] [Online]. Available: https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home

[33] [Online]. Available: https://www.government.nl/topics/online-access-to-public-services-european-economic-area-eidas/everything-you-need-to-know-about-eidas

[34] The European Parliament and the Council of the European Union, "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," https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG.

[35] European Union Aviation Safety Agency, "Faq n.19112," https://www.easa.europa.eu/faq/19112.

[36] The European Parliament and the Council of the European Union, "Article 1 of 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," https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG.

[37] The European Parliament and the Council of the European Union , "Regulation (eu) no 910/2014 of the european parliament and of the council," 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG.

[38] N. Tsakalakis, S. Stalla-Bourdillon, and K. O'Hara, "Identity assurance in the uk: technical implementation and legal implications under eidas," *The Journal of Web Science*, vol. 3, no. 3, pp. 32–46, 2017. [Online]. Available: http://dx.doi.org/10.1561/106.00000010

[39] The European Parliament and the Council of the European Union , "Regulation (ec) no 765/2008 of the european parliament and of the council of 9 july 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing regulation (eec) no 339/93," 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008R0765.

[40] ——, "Compiled list of conformity assessment bodies as defined in point 13 of article 2 of regulation (ec) no 765/2008 and accredited as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides against the requirements of eidas regulation (eu) 910/2014," 2019, https://cesk.gov.al/regjistri/regjistri/list_of_eidas_accredited_cabs.pdf.

[41] "Proposal for a regulation of the european parliament and of the council amending regulation (eu) no 910/2014 as regards establishing a framework for a european digital identity," June 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281

[42] "Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions 2030 digital compass: the european way for the digital decade," March 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

[43] J. Sahabu, "Signing away your personalized data: Service for data models," 2020. [Online]. Available: https://blogs.ischool.berkeley.edu/w231/2020/06/01/signing-away-your-personalized-data-service-for-data-models/

[44] "Final report of the expert group on regulatory obstacles to financial innovation: 30 recommendations on regulation, innovation and finance," Dec 2019. [Online]. Available: https://finance.ec.europa.eu/publications/

final-report-expert-group-regulatory-obstacles-financial-innovation-30-recommendations-regulation_en

[45] "Reports of the expert group on eid and kyc processes," Mar 2020. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/reports-expert-group-eid-and-kyc-processes

[46] "Report from the commission to the european parliament and the council - on the evaluation of regulation (eu) no 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eidas)," June 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0290

[47] "Commission recommendation (eu) 2021/946 of 3 june 2021 on a common union toolbox for a coordinated approach towards a european digital identity framework," June 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021H0946&qid=1478030835186