An eIDAS 'high' Open Standard and Open Source Implementation

Erwin Nieuwlaar
Delft University of Technology
May 2022

1 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. We are developing an open standard with open source reference implementation at eIDAS high level. We believe collaboration at EU-scale is vital to avoid fragmentation. The Open Source collaborative method at EU-scale will avoid delays and costly learning by each and every individual EU member state. Delft University of Technology is helping The Netherlands with the EBSI technical infrastructure hosting. Delft was also 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. First focus of our open standard and open source reference implementation is eIDAS high compliance, GDRP compliance, EBSI wallet compliance, and ISO/IEC 18013-5:2021 (Mobile driving licence, mDL).

2 Introduction

As of 17 September 2014, the Electronic Identities And Trust Services (eIDAS) Regulation came into force for all European Union (EU) Member States [1],[1] and it has been in effect since the first of July 2016 [1], [2]. The eIDAS Regulation articulates agreements with regard to using the same reliability levels, concepts, and mutual digital infrastructure of electronic identification (eID), in order to ensure the adequate functioning of the internal market [3]. As such, the eIDAS regulatory framework *i.a.* enables secure cross-border transactions for natural and legal persons [3]. 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 separate 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 [4]. According to recital 15 of the eIDAS Regulation [4], the assurance level of an eID should be equal or higher to that of the online service in question, in order for there to exist an obligation to recognise. *I.e.*, there is no obligation to authenticate a user which uses a 'low' level classified eID, when the authority requires a 'substantial' or 'high' level of assurance. In the eIDAS Regulation [4], as well as the Commission Implementing Regulation of 8 September 2015 [5] (Level of Assurance Regulation), the levels of assurance are elaborated upon in light of the regulatory implementation, technical specifications, and theoretical concepts. In order to enhance proper applicability and (future) compliance, the present paper provides a technically-oriented analysis on achieving the eIDAS different levels of assurance as well as an open source reference implementation. The paper will predominantly focus on the eIDAS compliance and specifically on the 'high' level of assurance. Nevertheless, as the 'low' and 'substantial' levels of assurance partially overlap therewith, these levels of assurance will be touched upon as well. Delft University has running application which is EBSI wallet compliant and GDRP compliant. Therefore, the main focus of this work is on complying to the eIDAS 'high' level of assurance and provide a standard and implementation thereof.

3 eIDAS Levels of Assurance

As indicated prior, the eIDAS Regulation construes three different levels of assurance, namely 'low', 'substantial' and 'high'. In order to comply any of these levels of assurance, a number of minimum requirements needs 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)

[1] See Article 52 of the eIDAS Regulation.

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 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 [6]. 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.

3.1 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].

3.1.1 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 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).

3.1.2 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

[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 [1].

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

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 [7]. 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 [8].

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.

3.1.3 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.

3.1.4 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 1 a summarized overview of the enrolment level of assurance requirements is provided.

3.2 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.

3.2.1 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.

3.2.2 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.

3.2.3 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.

3.2.4 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.

3.3 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.

3.4 Management and Organisation

3.4.1 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.

3.4.2 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.

3.4.3 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.

3.4.4 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.

3.4.5 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.

3.4.6 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.

3.4.7 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.

4 Use Case

In this Section we will describe potential use cases for implementing the first steps of an eIDAS high compliant application.

4.1 Token

Implementing FIDO2 is not an use case on itself but a tool to

4.2 Biometric

A possible use case to implement eIDAS regulation is the implementation of biometrics. Many types of biometrics exist, the ones most interesting with regard to eIDAS regulation are finger recognition and facial recognition as this biometric data is stored on EU passports. However, the Irish passports do not store fingerprint data on their passports [9]. As an eIDAS 'high' level solution should be interoperable, the only biometric use case option is facial recognition. Use case, facial recognition passport photo verifier standard.

4.3 DAO

Decentralized Marktplaats? Decentralized cryptoexchange, vanaf 18 mei 2020 zijn cryptoexchanges gebonden aan Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) en de Sanctiewet 1977 (onder integriteitstoezicht van DNB).

4.4 Notary Signature

The eIDAS regulation provides three levels of electronic signatures, where each electronic signature has different legal consequences and a level of confidence [7]. The three types of electronic signatures are the electronic signature (further on called the simple electronic signature), the advanced electronic signature, and the qualified electronic signature [10]. The electronic signatures can only be used by a natural person, legal persons can use a comparable electronic seal [8][4]. The concept electronic signature contains various elements, a combination of these

[7] "Level of confidence" should not be confused with the "level of assurance".

[8] The electronic seal is described in Section 5 of the eIDAS regulation

elements with some additional requirements results in one of the levels of electronic signature identified by the eIDAS regulation. To renounce from misinterpretation, an electronic signature is a collective name for all signatures made on a electronic device. Therefore, an electronic signature can consist *i.a.* of one or multiple combinations of a digital signature, biometric identification, scanned signature, signature based on symmetric encryption or pin-code. Accordingly, the digital signatures are a subset of electronic signatures and are based on asymmetric encryption [11]. Another key difference between an electronic signature is that an electronic signature is used to verify a document whereas a digital signature secures a document.

4.4.1 Simple Electronic Signature

The 'simple' electronic signature is *"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"*[9]. The 'simple' electronic signature is the most used, a few examples of a 'simple' electronic signature are, a scanned hand drawn signature, a name at the bottom of a mail, and a digitally drawn signature. This type of electronic signature has no legal binding in the eIDAS regulation except for that it cannot be denied legal effect and admissibility as evidence solely because of the signature being in an electronic form or not complying to the requirements of a qualified electronic signature. In other words, the 'simple' electronic signature cannot be easily rejected as legal evidence. In this case the legal binding of the 'simple' electronic signature depends on the circumstances of signing, such as, the likelihood that the signature belongs to the intended signatory, the awareness of the signatory with regard to the signed document, the timestamp, and proof that the signature provided belongs to the signed document [12]. The Dutch law[10] is a bit more specific on the binding. Concretely, the Dutch law sees the 'simple' electronic signature equal to a hand drawn signature with the additional requirement that the method used for signing must be sufficiently reliable and considers the circumstances of signing (same as the aforementioned circumstances).

4.4.2 Advanced Electronic Signature

An advanced electronic signature is an electronic signature which fulfills four requirements, namely: (a) the signature is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) the signature is created such that the signatory retains control, and lastly; (d) the signature is linked to the document such that if any subsequent change of the data can be detected. The legal binding is equal to the 'simple' electronic signature.

4.4.3 Qualified Electronic Signature

Zelfde als natte handtekening. Zelfde als Advanced, maar dan met: created by a qualified signature creation device (QSCD) (TU Delft potentiele QSCD?); and is based on a qualified certificate for electronic signatures (volgens mij uitgegeven door QTSP (qualified trust service provider), deze: `https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/NL` (Met esig label zijn van belang) , wellicht TU Delft ook TTP maken? PKI stopt. eIDAS is/wordt de standaard. Decentralized qualified electronic signature use case states: A prerequisite, that the diploma can be issued or verified, is that the HEI must at least own a QDC (Qualified Digital Certificate) issued by a QTSP from the EU. Meaning that everyone who wants to create a qualified electronic signature should have a certificate verified by a QTSP.

5 eIDAS 'high' compliance

The previous Chapter outlined the eIDAS regulations with regard to the assurance levels. The regulations provided by the European Commission are of legal nature. The legal notions should be converted into actual requirements to be able to be implemented. Accordingly, eIDAS implementations across the European Union will be discussed in this Chapter as well as, a discussion on how Delft University of Technology's TrustChain[11] could comply to these requirements. Furthermore, a design will be provided on how the implementation will look like.

5.1 Technical Requirements

TODO: Identify the technical requirements interesting for TrustChain

5.2 eIDAS Implementations

TODO: Discuss how other eIDAS 'high' implementations integrated these technical requirements.

5.3 Implementation Design

5.3.1 Existing Solutions

TODO: Research current existing solutions within TrustChain (EBSI wallet compliance and GDRP).

5.3.2 Design Open Standard

TODO: Provide design of an open standard

5.3.3 Design Implementation

TODO: Provide design of implementation regarding the open standard. Implement inside TU Delft's TrustChain.

[9] Article 3(10) eIDAS regulation

[10] Article 3:15a BW

[11] https://github.com/Tribler/trustchain-superapp

6 Implementation

TODO: Create open standard and open source implementation which is of eIDAS assurance level 'high', GDRP compliant, EBSI wallet compliant and ISO/IEC 18013-5:2021 compliant.

7 Evaluation

TODO: Evaluate if provided standard provides more quality, provides results faster, cost effective, is scalable and secure.

References

[1] 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.

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

[3] 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.

[4] 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.

[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] 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

[7] 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.

[8] ——, "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.

[9] J. P. Aus *et al.*, "Decision-making under pressure: The negotiation of the biometric passports regulation in the council," ARENA Oslo, Tech. Rep., 2006.

[10] S. van der Hof, "Regulering van elektronische handtekeningen," *DD Dielissen-Breukers ea (red.), JUVAT-dag*, pp. 35–44, 2001.

[11] J.-F. Blanchette, "The digital signature dilemma," in *Annales des télécommunications*, vol. 61, no. 7. Springer, 2006, pp. 908–923.

[12] F. Standaardisatie, "Betrouwbaarheidsniveaus voor digitale dienstverlening," 2016. [Online]. Available: https://www.forumstandaardisatie.nl/sites/bfs/files/atoms/files/Betrouwbaarheidsniveaus_voor_digitale_dienstverlening_v4.PDF

	Low	Substantial	High
Enrolment 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 legel 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 1: Enrolment assurance level requirements