34 Avenue Marie Therese, 2132 Luxembourg Tel.+352691333311 luxembourg.office@ewitness.lu ewitness.lu

What is needed in eIDAS for making standards for European Digital Identity Wallets (EDIWs) and for Qualified Trust Services (QTSs)[1].

The Dir 1999/93/EC and the Reg. 2014/910/UE had a distinctive approach for allowing the making of European standards for (qualified) electronic signatures and (qualified) electronic trust services. Following the same approach, with the revision of eIDAS, the **following** (not only technical) **definitions and security targets are needed**, if we want to continue the successful production of eIDAS related standards:

I. A proper **functional** and **security definition for all qualified trust services** and in particular for **attestations of attributes** and their **validation,**
II. A proper **functional** and **security definition** for **electronic identity**,
III. A **clear distinction between validation (art. 3(41), 32 and 33), authentication (art. 3(5)), and identification (art. 3(2))** in the context of eIDAS,
IV. The **functional** and **security definition of "sole control"**, of the EDIW (the Directive and the Regulation have always provided such definition for the SSCD/QSCD),
V. A proper **functional** and **security definition** for **electronic ledger.**

ABSTRACT

Regulating highly technical areas such as electronic identification and trust services requires a careful interaction between law and technology. The law should be technology neutral but written in a way that enables existing technology to fulfil the legal requirements while preferably not blocking development of new technology.

The Dir 1999/93/EC (**the Directive**) and the Reg. 2014/910/UE (**the Regulation**) **provided clear** legal **definitions** for a series of fundamental features of the electronic signature and of the trust services. These are:

1) Since 1999 a **functional and security definition of advanced electronic signature**;
2) Since 1999 a thereupon based **functional and security definition of qualified electronic signature**;
3) Since 1999 a **functional and security definition of secure signature validation**;
4) Since 1999 a **functional and security definition of the entity issuing qualified certificates**;
5) Since 2014 a **functional and security definition for all the (qualified) trust services introduced by the Regulation**.

The availability at European level of legally mandated functionalities and security objectives, was the **condition necessary and sufficient for producing all the standards needed** for implementing the Regulation in a technologically neutral, transparent, secure manner, eliminating the barriers to the single market, that national legislation and national security requirements had posed since the entry into force of the 93/1999EC Directive.

With the entry into force of the Regulation, the number of European qualified trust services (QTS) increased[2], without extending the requirements for the secure validation (Annex IV of the Directive) to all QTSs (see articles 32 and 33 of the Regulation, that refer only to signatures and seals).

Furthermore, the current revision of the Regulation (eIDAS2) discussed in Parliament and Council, doesn't define the functionalities and the security requirements of the new QTSs: attestations of attributes, ledgers, electronic archiving. The European standardisation effort can hardly produce secure, transparent, and technologically neutral standards, if the law doesn't set the needed functional and security requirements for QTSs.

Without European standards, national/proprietary solutions will prevail, harming technical interoperability and breaking up the single market for trust services, that has been built successfully by the Regulation, until now.

Article 1 of the Regulation (Subject matter) clearly states that IT security cannot be achieved at the detriment of the single market: the aim of the regulation is "*ensuring the proper functioning of the internal market while aiming at an adequate level of security of electronic identification means and trust services*" (see also recitals 4, 5, 6, and 32). Putting security above interoperability and the single market, is incompatible with the goals stated by article 1 of the eIDAS Regulation and thus, tantamount to fully abrogate the eIDAS Regulation.

[1] Speaker's notes by Riccardo Genghini, ETSI ESI Chairperson, for introducing the panel discussion **moderated by Slawomir Gorniak** (ENISA Senior Cybersecurity Expert) with the title "**eIDAS2: Certification and Standardisation in EU Digital Identities**", during the ENISA Trust Services Forum and CA Day 2022 (Berlin 27 and 28 October 2022).

[2] See the definitions of "Trust service" in article 3(16) and the definition of "Validation" in article 3(41) in the second consolidated draft of the revised Regulation.

HOW LEGAL RULES AND TECHNICAL NORMS HAVE INTERACTED IN THE DIRECTIVE AND IN THE REGULATION.

The Dir 1999/93/EC (the Directive) and the Reg. 2014/910/UE (the Regulation) provided clear (not only technical) definitions for a series of fundamental features of the electronic signature and of the trust services. These are:

1) Since 1999 a functional and security definition of advanced electronic signature[3];
2) Since 1999 a thereupon based functional and security definition of qualified electronic signature[4];
3) Since 1999 a functional and security definition of secure signature validation[5];
4) Since 1999 a functional and security definition of the entity issuing qualified certificates[6];

Directive EC/1999/93	Trust Service	Functional definition and Security requirements	SECURITY REQUIREMENTS FOR		
			Device	Certificate	TSP
	QES	A2(2) A5 ETSI TS 102 176 ETSI TS 102 734 ETSI TS 102 904 ETSI TS 102 176 ETSI TS 101 733 ETSI ES 201 733 ETSI TR 102 047 ETSI TR 102 038 ETSI TS 102 778	A2(5) Annex III CWA 14169 ETSI TS 102 176	Annex I ETSI TS 119 412 ETSI TS 102 280 ETSI TS 101 862	A2(10) Annex II ETSI TS 102 042 ETSI TR 102 437 ETSI TS 102 231
	QES Validation	A2(7) A2(8) Annex IV ETSI TR 101 564 ETSI TS 102 853	n.a.	n.a.	n.a.

5) Since 2014 a functional and security definition for all the (qualified) trust services, introduced by the Regulation[7] (see the picture on the next page).

Following these definitions and requirements set by the law, it was possible to provide **technical standards** that where **technologically neutral**, in the sense that all technical solutions that fulfilled the given definitions and objectives, were considered, and admitted in the standardization process.

So, every advanced signature that fulfilled the requirements of article 3(11) and 26 of the Regulation[8] was fit for becoming a qualified electronic signature, if attached to a qualified certificate and using an

---

[3] Article 2(2) of the Directive and articles 3(11) and 26 of the Regulation.

[4] Article 5 of the Directive and articles 3(12), 29, 30, 31, Annex I and Annex II of the Regulation.

[5] Article 3 (6) and Annex IV of the 93/1999 Directive and Articles 32 and 33 of the eIDAS Regulation.

[6] Article 2(10) and Annex II of the Directive and Articles 19 to 24.

[7] The eIDAS Regulation provides the security and functional requirements for the (qualified) electronic trust services as follows:

1) Qualified Electronic Signatures (QESig): articles 26, 28 and Annexes I and II
2) Qualified Electronic Seals (QESeal): article 36
3) Qualified Trust Service Providers (QTSP): articles 19, 20, 21, 22, 23 and 24
4) Qualified Electronic **Signature Validation** (ServiceQESig Validation): articles 32 and 33
5) Qualified Electronic **Seal Validation** Service (QESeal Validation): article 40
6) Qualified Long Term Preservation of QE Signatures and Seals (QLTP of QES): articles 34 and 40
7) Qualified Electronic Time Stamps (QETS): article 42
8) Qualified Electronic Delivery Service (QERDS): article 44
9) Qualified Website Authentication Certificate (QWAC): article A3(12) A3(16) A45.

[8] ***Article 26*** *(Requirements for advanced electronic signatures)*
An advanced electronic signature shall meet the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

SSCD/QSCD. Every signature creation device that has been certified to be conformant to EN 419 211, is admitted as a qualified signature creation device (QSCD) in all Europe. And every qualified signature certificate that fulfils the requirements of Annex I of the Regulation, is accepted in all 27 member states of the Union.

Even if in article 3(15) of the Regulation, the validation is considered part of each trust service, the requirements of articles 32 and 33 refer only to qualified signatures and seals: therefore the (current version of) **the Regulation, lacks functional and security requirements on validation services**[9], **for Qualified Time Stamps, for QWACs and for Qualified Long Term Preservation of QES: this poses security and interoperability risks**[10].

EU Reg. 2014/910	Trust Service	Functional definition and Security requirements	SECURITY REQUIREMENTS FOR		
			Device	Certificate	TSP
	QESig (also remote)	A26 A28 Annex ETSI EN 319 102 ETSI EN 319 142 ETSI TS 101 733 ETSI TS 101 903 ETSI TS 102 778 ETSI TS 119 432	A29 to 31 EN 419 211	A28 ETSI EN 319 411 ETSI EN 319 412	A19 to 24 ETSI EN 319 401 ETSI EN 319 403
	QESeal (also remote)	A36 ETSI TS 119 172	A39	A38 ETSI EN 319 411 ETSI EN 319 412	A19 to 24 ETSI EN 319 401 ETSI EN 319 403
	QESig Validation	A32 A33 ETSI EN 319 102 ETSI TS 119 441 ETSI TS 119 172	n.a.	n.a.	A19 to 24 ETSI EN 319 401 ETSI EN 319 403
	QESeal Validation	A 40 ETSI TS 119 172	n.a.	n.a.	A19 to 24 ETSI EN 319 401 ETSI EN 319 403
	QES QLTPreservation	A34 A40 ETSI TS 101 533 ETSI TS 119 511 ETSI TS 119 512	n.a.	n.a.	A19 to 24 ETSI EN 319 401 ETSI EN 319 403
	QETimeStamps	A42 ETSI EN 319 421	A42 ETSI EN 319 421	n.a. ETSI EN 319 422	A19 to 24 ETSI TS 102 023 ETSI EN 319 401 ETSI EN 319 403
	QERDS	A44 ETSI SR 019 050 ETSI TR 102 605 ETSI EN 319 522 ETSI EN 319 532 ETSI TS 119 524	A44 ETSI SR 019 050 ETSI TR 102 605 ETSI EN 319 522 ETSI EN 319 532 ETSI TS 119 524	n.a.	A19 to 24 ETSI EN 319 531
	QWACs	A3(12) A3(16) A45 ETSI TS 119 495	n.a.	Annex IV ETSI EN 319 412 ETSI TS 119 495	A19 to 24 ETSI EN 319 401 ETSI EN 319 403 ETSI TS 119 495

Article 27.

[9] QERD inherently includes the verification of integrity and origin of the registered email, the same isn't true for Qualified Time Stamps, QWACs and Qualified Long Term Preservation of QES, all of them clearly need a trustworthy validation service.

[10] In the Directive such security requirements were recommended for qualified signatures in Annex IV and named "***secure signature validation***". The Regulation mentions validation services only for qualified electronic signatures (article 36) and qualified electronic seals (article 40).

eIDAS2 ISN'T FOLLOWING THE SAME LEGISLATIVE APPROACH AS THE DIRECTIVE AND THE REGULATION: THIS SIGNIFICANTLY CHANGES THE ROLE OF STANDARDS

The amendments to the Regulation proposed by the Commission (so called eIDAS2) **lack sufficient functional and security requirements** on the Qualified Electronic Attestations of Attributes (articles 45a to 45f), on the Qualified Electronic Archiving Services (article 45g of eIDAS2) and on the Qualified Electronic Ledgers (articles 45h and 45i). In the following picture all eIDAS2 qualified trust services that miss proper functional and security definitions are highlighted in red.

eIDAS2	Trust Service	Functional definition	SECURITY REQUIREMENTS FOR		
			Device	Certificate	TSP
	QEAoA (attestation of attributes)	A45a to A45f	n.a.	Annex V	A19 to 24 ETSI EN 319 401 ETSI EN 319 403
	QEAS (electronic archiving)	A45i	?	QEAoA?	A19 to 24 ETSI EN 319 401 ETSI EN 319 403
	QEL	A45 i	n.a.	QEAoA?	A19 to 24?
	QEAoA Validation	missing (A32 A33 ?)	Qualified Validation Tool?	QEAoA?	A19 to 24 ?
	QEL Validation	missing (A32 A33 ?)	Qualified Validation Tool?	QEAoA?	A19 to 24 ?

The lack of proper functional and security requirements in eIDAS2 will have significant consequences, for standardization, interoperability and single market.

Let's make a few examples.

First of all, if functional and security requirements aren't enshrined in the law, their uptake is most unlikely. In fact, **role and attribute certificates** (the Dir. 93/1999/EC forebearer of electronic attestations of attributes), had been **standardized by ETSI ESI already in 2002**[11]: but there was/is no legal requirement on them, neither in the Directive, nor in in the Regulation. Therefore, nobody bothered to use them.

The same happened for several standards developed for "**signature policies**". They weren't foreseen in the Regulation, so they have remained unused.

Moreover, **ETSI ESI published already in 2007 European standards for registered emails**[12]. But the effort to use European standards for registered emails gained traction only after article 44 of the Regulation entered into force, mandating its essential functionalities and security requirements, and mandating mutual recognition. Without these legislative definitions/provisions, no registered email provider embarked (in the ten years between 2007 and 2016) in the effort to implement the European standard for REM.

If the Regulation will not provide clear and sufficient functional and security requirements on the new (qualified) trust services, the same will happen again: they will remain unused. **Good standards aren't sufficient for the general uptake by the market.**

If the law doesn't define functional and security requirements, it becomes impossible to write secure, technologic neutral standards: for an instance, the proposed article 45g of eIDAS2 doesn't clarify if the **qualified electronic archiving service** shall make use of (qualified) signatures, seals, or time stamps[13]. So, in theory, (qualified) electronic archiving could be provided by a non-rewritable hardware module: but in this case, should it be evaluated for security? And (if yes) according to what criteria? This kind of decisions cannot be left to standards and/or best practices. If the legislator has deemed necessary to create a new and different (qualified) trust service for (qualified) electronic

[11] ETSI TR 102 044 2002: Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates.

[12] Its acronym was REM: ETSI TR 102 605 and ETSI TS 102 640.

[13] As it obviously a qualified signature long term preservation service must

archiving (article 45g)[14], it must also define in what way it is different from (qualified) long term preservation of QES (article 34): the difference and the consequent different functional and security requirements of the two QTSs must be defined by the law. If qualified electronic archiving can also be a hardware module (without signatures, seals, timestamps), it seems reasonable that it should be security-evaluated. Reasonable, but not legally necessary: the legislation needs to clarify this aspect. Standard organisations don't have the (legal and political) legitimization to make such decisions. If they foresee a security evaluation that isn't required by the law, it will always be just a recommendation, even if mandatory in the standard. All this considered, the lack of a proper functional and security definition of qualified electronic archiving services, will fragment into several different (and possibly incompatible) standards, and even (national) proprietary solutions, that will make very difficult the portability of data that are archived in a qualified service[15].

But the most striking miss, is that **eIDAS2 doesn't provide security and functional requirements on the electronic attestation of attributes** in the same way it does it for qualified certificates for signatures (article 28) and seals (article 36). According to article 3(14) and 3(15) a **qualified certificate for electronic signatures is** "***an electronic attestation*** *which links electronic signature validation data to a natural person (...) issued by a qualified trust service provider and meets the requirements laid down in Annex I*"[16]. Article 3 doesn't provide any such definition for qualified attestations of attributes. The **qualified electronic attestation of attributes** should have been better defined by the law as "***an electronic attestation of attributes*** *which is issued by a qualified trust service provider issuing qualified electronic attestations of attributes, is validated by means of the issuer's signature validation data, and meets the requirements laid down in Annex V*". The imprecise/incomplete definition provided by articles 3 and 45g of eIDAS2 requires a great deal of legal interpretation, before a proper standardization process of attestations of attributes may be carried out. The same, mutatis mutandis, is true for qualified electronic archiving and ledgers.

THE IMPORTANCE OF SECURE VALIDATION SERVICES SEEMED FORGOTTEN (UNTIL THE SEEMINGLY UNSOLVABLE PROBLEM OF THE WALLET'S RELYING PARTIES)

The problem that EDIW relying parties pose isn't new. Since 1999 there was awareness that the validation of qualified signatures and qualified certificates is important for the overall trustworthiness of qualified signatures. **The Regulation**, while increasing the number of qualified trust services, **hasn't provided definitions and requirements for the (qualified) validation of all other qualified trust services[17].** There is the evident need in the Regulation of secure validation requirements also for Qualified Time Stamps, for QWACs and for Qualified Long Term Preservation of QES. The eIDAS2 proposal doesn't address this important issue. eIDAS2 adds to the list of the **other qualified trust services that are missing secure validation criteria**, the Qualified Attestation of Attributes (articles 45a – 45f), the Qualified Electronic Archiving (article 45g) and the Qualified Electronic Ledgers (articles 45h and 45i).

Secure (transparent, non-discriminatory) validation criteria are important for the security of all qualified trust services. Only QERD, as defined by article 44 of the Regulation, has incorporated both validation of the signatures and (implicitly) of time stamps of the registered emails.

The importance of secure (transparent, non-discriminatory) validation criteria is particularly evident in the debate about QWACs: qualified website authentication certificates don't have enshrined in the law secure validation criteria. Therefore, it is impossible (not convenient) for

---

[14] As a different trust service with respect to the qualified signature long term preservation foreseen by article 34 of the Regulation.

[15] On top of that, the national competent authorities, according to article 7 of the NIS2 Directive proposal, established in the 27 member states of the Union, may impose on qualified long term preservation of signatures and qualified electronic archiving, varying additional security requirements, and even different certification obligations, that will make portability and interoperability all but impossible.

[16] Article 3(29) and 3(38) provide identical definitions for qualified electronic seal certificates and qualified website authentication certificates. But article 32 and 33 only refer to signatures and seals.

[17] The Regulation provides secure validation criteria only for qualified signatures (in articles 32 and 33) and for qualified seals (in article 40)..

web-browsers to implement API's towards such a trust service, because it isn't foreseen by the law[18]. It is urgent and highly recommended to extend the functional and security requirements of articles 32 and 33 to the validation of (attestations issued by) all other (qualified) trust services. It should also be clarified that the attestation of the outcome of the validation procedure should be signed and have an open standardised format. For ensuring interoperability, the format of the validation attestation should be compliant to European Standards, that the Commission may reference in the Official Journal of the Union. Article 32(3) of eIDAS2 should be accordingly amended.

eIDAS IS MISSING A CLEAR FUNCTIONAL DISTICTION BETWEEN IDENTIFICATION AND AUTHENTICATION.

Signature, *Certificate* and ***Identification*** are the most used terms in the Regulation (respectively 17, 140 and 117 times). The next most used term is "***Authentication***" (89 times in the Regulation and 57 times in the eIDAS2 proposal)[19]: it is defined in article 3(5) of the Regulation in a way, that seems to include identification.

Therefore, identification and authentication are sometimes used in the Regulation confusingly as synonyms.

IDENTITY, IDENTIFICATION: PASSIVE AND ACTIVE

A person's '**digital identity**' can be defined as the collection of all digital information that can be linked to the person[20]. These days, most of the information about a person is recorded in digital form and can be accessed independently of physical location. A digital identity defined this way consists of arbitrary types of information elements ("***attributes"***), including the person's national identity linked to citizenship, residency, and rights and obligations associated with a national identity.

Identification from a legal and functional point of view, in the context of the eIDAS Regulation, has different moments/functions:

1) **Passive Identification.** The bestowing by the state upon citizens of their official administrative identity, fixing some person identity attributes, that are represented on one or more identification tools (currently ID, Passport, Driving license, etc. and, with eIDAS2, the European Digital Identity Wallet), through which a certain degree of unique and persistent identification is achieved. **This function is not explicitly defined (in its functional and security requirements) in the Regulation (or in eIDAS2):** it is presupposed, but not defined, by Chapter II (whose title is "ELECTRONIC IDENTIFICATION"), and by article 6a(4)(e), 6a(5)(c), 7(d), 7(e) and 8. Functionally passive identification is the **generation of the digital administrative identity of a citizen and its uploading on a digital identification means (i.e. EDIW)**. In most states it is steered/executed by a public sector body. According to Union law[21] this is an **exclusive competence of the member states of the Union**.
2) **Active Identification**. The **utilization by the citizens of their person identification data**, when interacting with platforms, websites, apps and other on-line services, defined as "***identification***" by article 3(1) of the Regulation (even if, in most cases, functionally it will be an authentication). Currently, if the user hasn't a national digital identification means, all identities are claimed and the therewith generated user profiles are managed exclusively by the relying parties (normally for-profit companies, large platforms, gatekeepers, etc.). With eIDAS2 European citizens will be able to take advantage of a certified identity, without a loss of privacy, by means of the European Digital Identity Wallet (EDIW), but only if the law will properly define its functional and security requirements.

---

[18] **One of the possible compromise solutions discussed in the CAB Forum and in ETSI ESI, is precisely to define a policy for presenting the QWACs to European validation services. The fact that such a service isn't among the qualified trust services, makes such compromise solution more difficult to realise.**

[19] Relying party is used in the eIDAS2 proposal (only) 33 times and Wallet 75 times.

[20] As we can see in the "identity" provided to users by large platforms and gatekeepers (FAANGS and similar).

[21] Pursuant to Directive 2004/38/EC, Member States are to issue and renew identity cards or passports to their nationals in accordance with national laws. Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement.

According to Union law (GDPR), citizens (when interacting with any legal entity) have the right not to disclose their full person identity data, and the disclosure of such person identification attributes cannot be mandated, unless there is a legal obligation (like in the case of legislation against money laundering, i.e. KYC). Also in this case, if the law will properly define the functional and security requirements of EDIWs, there will be more security in the citizen's online interactions with public administrations and private entities, without a compression of their fundamental rights, in particular their right to privacy.

AUTHENTICATION: IN eIDAS, IT IS THE VALIDATION PROCESS OF SOME SIGNED ATTRIBUTES THAT IS FORWARDED TO AN EDIW OR A RELYING PARTY,

Active identification is an authentication process, carried out by presenting a sufficient number of person identification data, to reveal the identity of a single person or legal entity. Authentication is the same technical process, carried out without presenting person identification data, or presenting just a limited set of them, so that they don't reveal the identity of a a single person or legal entity.

But it is hard to find such a clear distinction of the two in the Regulation. The article 3(5) legal definition of authentication covers identification of persons and authenticity and integrity of data communicated. It does not cover authentication of trust service providers, which is clearly needed for validation of attestations made by such providers. There is a need to define in eIDAS2 what exactly authentication means in the context of eIDAS, considering that authentication is necessary with each and every (qualified) trust service: one authenticates towards a SSCD (token or remote service); QERD providers need to mutually authenticate; validation of a time stamp means authentication of the issuer; and the same is the case for issuers of attestations of attributes and providers of validation, preservation, or archive services; EDIW are not only tools for identification, but also for authentication (authentication is mentioned more than 30 times in Chapter II of eIDAS2); and so on.

It helps to read the ISO 27000 functional description of authentication[22]: it becomes clear that "authentication" is the same technical procedure of "validation", with the additional feature that it automatically presents the outcome of the validation to a relying party that has a set of rules for determining the access rights of the claimant.

There are the **three main steps of any authentication process**[23]:

1) The **presentation of some information** (attributes, credentials, identification data, authentication data and other formalised tokens). It is, in principle, the **same** technical function as **in validation**.
2) The **validation of the data presented against a set of rules**. It is, in principle, the **same** technical function as **in validation**.
3) The forwarding of the outcome of the validation of the presented information to a relying party, that uses the outcome of the authentication for defining the **access rules to a given set of functionalities/data within its domain**.

Therefore, we can conclude that **for the purposes of the Regulation, the validation of electronic identification means, electronic timestamps, of QERD, of Long Term Preservation of QESs, of website authentication certificates, of electronic attestation of attributes, and of other signed attestations, is an essential part of the more specific "authentication" service**.

A proper definition of "***Authentication***" in the context of eIDAS may be the following (article 3(5)):

---

[22] "*Authentication: provision of assurance that a claimed characteristic of an entity is correct*".

[23] See ETSI TS 119 461 V1.1.1 (2021-07) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf
ETSI TR 119 460 V1.1.1 (2021-02) Electronic Signatures and Infrastructures (ESI); Survey of technologies and regulatory requirements for identity proofing for trust service subjects
https://www.etsi.org/deliver/etsi_tr/119400_119499/119460/01.01.01_60/tr_119460v010101p.pdf
For a short presentation of both ETSI deliverables read:
file:///Users/rgenghini/Downloads/ETSI%20standards%20for%20trust%20services%20and%20digital%20signatures%20-%206%20identity%20proofing%20SL%20v3%20(2).pdf

5) 'authentication' means an electronic process where signed attributes or certificates are validated

(a) according to articles 3(41), 32, 33 and

(b) against a set of formalised requirements defined by the applicable legislation or by a relying party.

The **essential technical authentication components** are:

1) A **formalised set of attributes/tokens** needed for being recognized and authenticated by the system: they may be tokens, attributes, certificates (such as QWACs), credentials, personal data, and so on;
2) A **formalised set of technical rules** against which the attributes are validated;
3) When authentication (validation) is performed by a trust service provider, a **protocol/format** for presenting the outcome of the validation of the attestations to a relying party.

All this considered, articles 32 and 33 should be entitled respectively "***Requirements for the validation of qualified electronic signatures and other attestations of qualified trust services***" and "***Qualified validation service for qualified electronic signatures and other attestations of qualified trust services***". In both should be added a paragraph stating: "*Mutatis mutandis, the same requirements apply to the validation of attestations issued by other qualified trust service providers*".

Several articles of eIDAS2 mention authentication as a process carried out by means of an EDIW or by means of authentication/identification data: in Chapter I, articles 1(c), 3(2) definition of identification, 3(5) definition of authentication, (3(16) definition of trust services, 3(38), 3(39), 3(42) definition of European Digital Identity Wallet, 3(44) definition of electronic attestation of attributes, 3(50) definition of strong user authentication. In Chapter II (about EDIW) we have articles 6a(3)(a), 6a(4)(c), 6a(4)(d), 6b(2), 6b(3), 7, 8(3)(c), 9(1)(b)(ii), 9(1)(f), 9(1)(g), 10(1), 10(2), 11(3), 11a(1), 12b(1), 12b(2),12b(3), 12b(4), 12c(1), 12c(2). In Chapter III (trust services) we have articles 45(1), 45(2), 45(3), 45b, 49, and Annex IV.

Considering the central relevance of authentication services for EDIWs and for qualified trust services, such as QERD, QWACs, Qualified Electronic Attestation of Attributes, Qualified Electronic Archiving, Qualified Long Term Preservation of Signatures/Seals, Qualified Electronic Ledgers, it seems necessary to provide legislative functional and security requirements for authentication in an Annex to eIDAS2[24]. Such functional and security requirements may be defined as follows:

Advanced authentication means shall ensure, by appropriate technical and procedural means, that at least:

a. the confidentiality of the authentication data is reasonably assured.

b. authentication by use of the electronic authentication data can practically occur only once; NOTE: As for electronic signatures implies a cryptographic operation on a challenge resulting in a unique value.

c. the electronic authentication data used for authentication cannot, with reasonable assurance, be derived using currently available technology.

d. the authentication data used for authentication can be reliably protected by the legitimate person against use by others.

e. the therein stored data can be created, modified and deleted only with the explicit consent of its owner

f. the advanced electronic authentication tool be uninstalled only by its owner

g. accept all formats of Advanced electronic attestation of attributes

h. provide only to its legitimate users a seamless history of all identification/authentication processes carried out with the Advanced Electronic authentication/identification Tool.

As it is for validation, authentication is an essential part of most (if not all) qualified trust services. So, as in article 33 for qualified validation services, **in eIDAS2 there should be a definition of the functional and security requirements on authentication for qualified trust services**. It may be the following: *Qualified electronic authentication means, are advanced authentication means that are issued by a Qualified Trust Service Provider*.

[24] For the same reasons it is necessary to have a functional and security requirements on validation.

THE IMPORTANCE OF SOLE CONTROL OF THE EDIW

The precise definition of "**sole control**" of the advanced and qualified signatures, was essential for their successful adoption worldwide. The same is true for the electronic identity: but not only for reasons related to the needs of cybersecurity; it is evident that flaws in the functionalities of the eID may impact directly the fundamental rights enshrined in the TEU and in the other treaties of the Union.

eIDs are extremely more complex than signatures and certificates. Still, there is another analogy between eIDs and advanced/qualified electronic signatures: they can be under the sole control of the citizens both remotely or locally and, also, through a hybrid solution, e.g. where a RFID token activates the identification/authentication tool.

For the standardisation process, it is needed that the legislation provides a complete and clear definition of "sole control" of the EDIW.

We may safely assume that "sole control" of a wallet is based on the requirements for authentication in/for a qualified trust service, with additional requirements, because the EDIW is not only an authentication means, but also an identification means.

But, still, without a security target defined by the law, technologic neutrality and interoperability will remain fiendishly elusive for EDIWs, as the experience with the national identification schemes (lacking common functional and security requirements) has proved.