Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)

Jos Dumortier

Abstract:

On 23 July 2014 the European Parliament and the Council adopted a Regulation "on electronic identification and trust services for electronic transactions in the internal market" (the "eIDAS Regulation"). The Regulation deals with two distinct topics. In the first place it introduces a system of cross-border mutual recognition of electronic identification schemes used in Member States for the access to online public services. If this mechanism succeeds, it will be possible for a citizen from one Member State to use his/her eID for accessing an online public service in another Member State. In the second place the eIDAS Regulation creates a common legal framework for trust services. This part of the Regulation contains a series of common provisions related to electronic signatures, electronic seals, electronic time stamps, electronic registered mail and web authentication. It is uncertain whether or not the eIDAS Regulation will have a tangible effect on online transactions in Europe.

Keywords: electronic identity**,** trust services, electronic signatures, electronic seals, electronic time stamps, web authentication

1. Introduction

The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) was adopted by the European Parliament and the Council on 23 July 2014.[1] It was published in the Official Journal of the European Union on 28 August 2014 and entered into force starting from 17 September 2014. For most of the provision however, a transition period has been established before they have to be effectively applied.[2]

In establishing, back in 2010, its strategy for the coming decade - the so-called Digital Agenda - the European Commission explicitly referenced the existing barriers to Europe's digital development and proposed legislation on e-signatures (Key Action 3) and the mutual recognition of e-identification and authentication (Key Action 16).[3] Against this background, on 4 June 2012, the Commission presented a

[1] 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*, OJ* L 257, 28.8.2014, p. 73–114

[2] Crucial dates are 1 July 2016 (effective application of the provisions on trust services, end of the application of national provisions transposing the 1999/93 eSignature Directive) and 18 September 2018 (mandatory recognition of eID schemes notified by Member States)

[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 26 August 2010, A Digital Agenda for Europe, *COM(2010) 245 final/2*.

proposal for a regulation on electronic identification and trust services for electronic transactions in the internal market.[4]

A first question raised by the initiative of the European Commission is that of the choice for a *regulation* as the legislative instrument for these matters. While the proposal made a number of references toward its goal of providing for a better accessibility of cross-border online services by removing existing barriers, it did not directly address the need for a regulation as the specific type of legislative instrument. The choice for a regulation can be more clearly deducted from the policy impact assessment conducted as part of the preliminary works.[5] Here, it is argued that the use of two instruments – e.g. two directives or a directive and a regulation – could lead to these instruments having divergent goals, thus limiting the uptake of the services addressed here. As a result, the Commission proposed the use of one single instrument. Subsequently, the report argues against amending the existing directive, holding that "*the freedom given to MS when transposing a Directive (in terms of interpretation and of implementation of the systems) contributed to the current problems of mutual recognition of services and products and of cross-border interoperability*".[6] It is argued that a regulation can provide stronger harmonization and would "*present an immediate solution to current problems and develop a long-term-use instrument*".[7]

While it is true that a regulation, unlike a directive, does not require a transposition into the national legislation of the Member States, regulations also need to find their place in the legislative order of the Member States. Each time a regulation references a matter covered by the national legislation of the Member States, there will still be 28 different combinations of regulation and national legislation, just like a directive can lead to 28 different transpositions. For instance, as will be explained later, rhz Regulation holds that a "*qualified electronic signature shall have the equivalent legal effect of a handwritten signature*".[8] It is clear that this provision doesn't result in an identical legal effect for qualified electronic signatures all over the EU, simply due to the fact that it doesn't affect the different legal status of handwritten signatures in the 28 Member States.

From a substantive point of view, the eIDAS Regulation consists of two more or less autonomous sections. The first section deals with government-recognized electronic identification systems and establishes a legal framework that will allow all EU Member States to mutually recognize each other's identification systems. This section targets the public sector and requires Member States to permit citizens from other Member States to use their own electronic IDs for accessing online public services. Private sector companies are not directly impacted by this portion of the Regulation, although services developed for the public sector will likely also be extended to them.

---

[4] Commission proposal for a regulation of the European Parliament and of the Council of 4 June 2012 on electronic identification and trust services for electronic transactions in the internal market, *COM(2012) 238 final.* See also the "IAS" feasibility study carried out on behalf of the Commission, available at https://ec.europa.eu/digital-single-market/en/news/feasibility-study-electronic-identification-authentication-and-signature-policy-ias-0 (last checked on 1 April 2016)

[5] Commission staff working document of 7 June 2012 impact assessment accompanying the document proposal for a regulation of the European Parliament and of the Council on electronic identification and tryst services for electronic transactions in the internal market, *SWD(2012) 135 final*, p. 40-41. https://www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vj0945gt4mzt#p1 (last checked 1 April 2016)

[6] *Ibid.*, p. 40.

[7] *Ibid.*, p. 41.

[8] Article 25.2 eIDAS Regulation.

The second section of the eIDAS Regulation deals with trust services. The term "trust services" refers to services related to electronic signatures, electronic seals, time stamps, electronic delivery services and website authentication. In practice the Regulation mainly addresses PKI-based services. Inspired by the 1999/93 Electronic Signature Directive, it creates a category of "qualified" trust services supervised by national public authorities in the Member States.[9]

2. Electronic identification

2.1. Mutual recognition

The goal of the first part of the eIDAS Regulation is to provide for a harmonized recognition and acceptance of (notified) electronic identification schemes across the EU Member States.[10] Recital (9) of the Regulation states that, in most cases today, EU citizens cannot use their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes in their country are not recognised in other Member States. Mutually recognised electronic identification means facilitate cross-border provision of services in the internal market and are a first step in enabling citizens and businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities.

Article 6 of the Regulation establishes how the mutual recognition framework will actually work. It determines that wherever an electronic identification using an electronic identification means and authentication is required – by legislation or administrative practice – to access an online service provided by a public sector body online, the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that service online, provided that three conditions are met:

a) the electronic identification means is issued under an electronic identification scheme that is included in a list published by the Commission;

b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State;

c) the relevant public sector body uses the assurance level substantial or high in relation to accessing that service online.

In a first step the Commission will consequently publish a list of electronic identification schemes. These schemes will be notified to the Commission by Member States. For example: Belgium could decide to notify the Belgian electronic identity card scheme rolled-out in that country and if all conditions are met, the European Commission would then include that scheme on its list.

Member States can start notifying identification schemes once the list held by the Commission is operational. When notifying a scheme, the Member State will specify under which assurance level that scheme should be categorized. Each identification scheme will be categorized in one of three assurance levels. Assurance levels essentially correspond to the degree of security provided by the identification

[9] See Recital (3): "*Directive 1999/93/EC of the European Parliament and of the Council dealt with electronic signatures without delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions. This Regulation enhances and expands the acquis of that Directive.*"

[10] Article 1(a) of the Regulation.

scheme. As will be explained in further detail later, the Regulation distinguishes three assurance levels: "low", "substantial" and "high". Defining such levels is necessary because the list of notified electronic identification schemes will presumably contain all kinds of security levels: from simple user-password solutions to highly secured e-ID cards. Online public services requiring strong authentication in one Member State, will evidently not be accessible by using simple password schemes issued in another Member State.

The third condition mentioned in Article 6 of the Regulation determines the scope of the mutual recognition regime. Identification means required in other Member States and issued under an identification scheme included in the list held by the European Commission, will only have to be recognized for accessing online public services requiring an assurance level "substantial" or "high". Moreover, as stated in Recital (15), the obligation to recognise electronic identification means relates only to those means the assurance level of which corresponds to the level equal to or higher than the level required for the online service in question. For example, if access to a particular online public service in Member State A requires identification means corresponding to assurance level "high", that Member State will not be forced to recognize identification means of other Member States that have been categorized as "substantial". In addition, the obligation only applies when the public sector body in question uses the assurance level 'substantial' or 'high' in relation to accessing that service online. Member States remain free however to recognise electronic identification means having lower identity assurance levels.

The solution adopted by the Regulation is inspired by the STORK large-scale pilot project.[11] This EU-funded project was aimed at making the cross border operation of online public services easier for citizens by having EU Member States mutually recognize each other's electronic identity scheme (eID). One of the preferred solutions developed in the context of STORK consists in the use of national gateways (so-called "Pan-European Proxy Services" or "PEPS").

2.2. Terminology

As mentioned before, Article 6 of the Regulation establishes the principle that wherever an electronic identification using an electronic identification means and authentication is required – by legislation or administrative practice – to access an online service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State shall, if all conditions are met, be recognised in the first Member State for the purposes of cross-border authentication for that service online.

What does the Regulation mean by concepts such as "person identification data", "electronic identification", "electronic identification means" or "authentication"?

"Person identification data" means "*a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established*". Examples of person identification data are unique identification numbers. Person identification data should however not necessarily *uniquely* identify natural or legal persons. Persons can, for example, be identified by a name, a place and date of birth a mobile telephone number, an e-mail address or by a combination of data. Online service providers will often identify their users via a user name and a password. All these can be considered as "person identification data". As will be explained later, mutual recognition of identification schemes is not possible without a minimal agreement on the person identification data which will be used to identify a natural or

[11] Secure idenTity acrOss boRders linked, *www.eid-stork.eu* .

a legal person. Therefore, one of the Implementing Regulations[12] establishes "minimum sets" of person identification data uniquely representing a natural or legal person.

"Electronic identification means" refers to a material and/or immaterial unit containing person identification data and which is used for authentication for an online service. Examples are user name/password combinations, electronic identity cards, etc. These are the means which are used by natural or legal persons as a proof of their identity.

The process to *uniquely* identify a natural or legal person by making use of person identification data in *electronic* form is called "electronic identification". Electronic identification can, for example, be carried out by checking a user name and a password or by verifying a digital certificate.

"Authentication" means an electronic process that enables the electronic identification of a natural or legal person, or confirmation of the origin and integrity of data in electronic form. The concept is consequently broader than "electronic identification" because it covers not only so-called entity authentication (recognizing a natural person, for example) but also data authentication (checking the origin and integrity of data, for instance via an electronic seal).

An "electronic identification scheme" means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons. This is what Member States will notify and which will be included in the list. Besides identification means, a scheme contains the whole ensemble of tools and procedures necessary for the creation, management and use of these means.

2.3. Cooperation

Setting up a system of mutual recognition of eID schemes in Europe necessitates a high degree of cooperation. Member States have to trust each other's electronic identification schemes, which is not evident. Therefore, the eIDAS Regulation introduces a procedure of peer review. Member States are requested to inform each other about the eID scheme they are planning to notify. As will be described hereafter more in detail, this information needs to be provided six months prior to the actual notification. A Member State that has a security concern affecting a scheme which has been notified or which is in the process of being notified, may request information related to the security concern

To avoid language problems, information between Member States will be exchanged in English. These and other procedural arrangements have been issued by the Commission in an Implementing Decision of 25 February 2015.[13] The Implementing Decision requests the Member States, for example, to designate a single point of contact for the application of the mutual recognition system introduced by the eIDAS Regulation. The Decision also establishes a Cooperation Network with a representative from every Member State or EEA country. This body, chaired by the Commission, examines the outcome of the filled draft notification forms and the outcome of the peer reviews. A peer review process may be initiated in one of the two ways: a) a Member State requests its electronic identification scheme to be peer reviewed,

[12] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, *OJ* L 235, 9.9.2015, p. 1–6.

[13] Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, *OJ* L 53, 25.2.2015

or b) Member State or Member States express the wish to peer review the electronic identification scheme of another Member State.

2.4. Eligibility

Not every identification scheme is allowed for being notified to the European Commission and for being included in the list held by the Commission. Electronic identification schemes are only eligible for notification provided that all of the following six conditions are met:

- the electronic identification means under the electronic identification scheme are issued by the notifying Member State, under a mandate from the notifying Member State, or independently of the notifying Member State but recognised by that Member State; identification schemes rolled out by private companies, for example by banks, can consequently meet this first condition if they are recognized – in one form or another - by the notifying Member State;
- the electronic identification means under the electronic identification scheme can be used to access at least one service which is provided by a public sector body and which requires electronic identification in the notifying Member State; "public sector body" means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;
- the electronic identification scheme, the electronic identification means, the attribution of the person identification data and the attribution of the identification means have to meet the requirements of at least one of the assurance levels defined in the Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 (see later).
- the notifying Member State ensures the availability of authentication online, so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form. For relying parties other than public sector bodies the notifying Member State may define terms of access to that authentication. The cross-border authentication shall be provided free of charge when it is carried out in relation to a service online provided by a public sector body. Member States shall not impose any specific disproportionate technical requirements on relying parties intending to carry out such authentication, where such requirements prevent or significantly impede the interoperability of the notified electronic identification schemes;
- at least six months prior to the notification pursuant to Article 9(1), the notifying Member State provides the other Member States a description of that scheme in accordance with the procedural arrangements established by the Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification (see later).
- the electronic identification scheme meets the requirements set out in the Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework (see later).

2.5. Assurance levels

As mentioned before, the eIDAS Regulation distinguishes between three assurance levels for electronic identification means issued under an electronic identification scheme.: low, substantial and high. The

distinction refers essentially to the degree of confidence in the claimed or asserted identity of a person. Each level is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity. The lower this risk of misuse or alternation is, the higher the assurance level will be.

The assurance levels have been defined in the Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015.[14] This Implementing Regulation is to a large extent inspired by the international standard ISO/IEC 29115,[15] which is the principle international standard available in the domain of assurance levels for electronic identification means, and by the specifications developed in the STORK large pilot project.[16]

The reliability and quality of a notified identification scheme is essentially determined taking into account four criteria:

- enrolment: for example, which evidence is verified at the enrolment for determining whether or not the identity claimed by an applicant is his real identity and which means are used to verify this?
- electronic identification means management: for example, how are the electronic identification means protected against duplication, tampering, or against use by others, how are these means delivered to the applicant?
- authentication: for example, which security controls for the verification of the electronic identification means have been implemented in the authentication mechanism in order to avoid activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker?
- management and organisation: for example, which facilities are used for monitoring, which data are retained for investigation after security breaches, etc.?

If a Member State decides to notify an electronic identification scheme, it will have to indicate to which assurance level that scheme belongs. A description of the scheme, including the assurance level, has to be provided to all other Member States six months prior to the actual notification.[17] This information is necessary to enable peer review as set out in Article 10(2) of Implementing Decision (EU) 2015/296 (see later).

---

[14] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance), OJ L 235, 9.9.2015, p. 7–20

[15] ISO/IEC 29115:2013, Information technology -- Security techniques -- Entity authentication assurance framework, **http://www.iso.org/iso/catalogue_detail.htm?csnumber=45138**

[16] Both the ISO standard and the STORK specifications distinguish between 4 assurance levels (low, medium, high and very high).

[17] Article 7 (g) of the eIDAS Regulation

2.6. Notification

In an Implementing Decision (EU) 2015/1984 of 3 November 2015 the Commission laid down the circumstances, formats and procedures of the notifications of electronic identification schemes.[18] The Annex of this Implementing Decision contains a notification template which needs to be completed in English.

Member States notifying an electronic identification scheme need to provide the following information to the Commission:

- a description of the electronic identification scheme, including its assurance levels and the issuer or issuers of electronic identification means under the scheme;
- the applicable supervisory regime and information on the liability regime with respect to the the party issuing the electronic identification means and to the party operating the authentication procedure
- the authority or authorities responsible for the electronic identification scheme;
- information on the entity or entities which manage the registration of the unique person identification data;
- a description of how the requirements set out in the implementing acts are met;
- a description of the cross-border online authentication process;
- arrangements for suspension or revocation of either the notified electronic identification scheme or authentication or the compromised parts concerned.

The first list of notified identification schemes will be published by the European Commission at the end of September 2016. Most schemes will of course be notified after that date. The Commission will publish these later notifications in the form of amendments to the initial list, within two months from the date of receipt of the notification.

2.7. Liability

Liability provisions in European legislative texts are often extremely difficult to interpret. This is not different in the eIDAS Regulation. Article 11 of the Regulation contains provisions with regard to liability for damage. Such damage could occur, for example, if an online public service in Member State A is accessed by someone using false identity means under a scheme notified by Member State B. The notifying Member State, in such case, will be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligation to ensure that the person identification data uniquely representing the person in question is attributed, in accordance with the technical specifications, standards and procedures for the relevant assurance level, to the natural or legal person concerned at the time the electronic identification means under that scheme is issued. In more simple terms this means that a notifying Member State will be liable if there is something wrong with the notified scheme and in particular if, in practice, the scheme doesn't correspond to the assurance level under which the scheme has been notified.

Electronic identification means issued under a notified scheme are, however, not necessarily issued by the notifying Member State but possibly by another entity, for example a private company. In that case this party will be liable for damage caused intentionally or negligently to any natural or legal person due

[18] Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance), OJ L 289, 5.11.2015, p. 18–25

to a failure to comply with the technical specifications, standards and procedures for the relevant assurance level.

Notifying Member States can also be liable if damage occurs due to the non-availability of authentication online. Such damage could occur if a relying party established in the territory of another Member State is unable to confirm the person identification data received in electronic form because of the non-availability of the authentication service. If the non-availability is intentional or due to negligence the notifying Member State will be liable for the damage. Again if the authentication service is provided by another entity, the latter will be liable.

These rules are probably identical to already existing liability rules in the Member States. In any case, Article 11.4 states that they need to "be applied in accordance with national rules on liability". Recital (18) explains that the provisions of Article 11 don't affect national rules on, for example, definition of damages or relevant applicable procedural rules, including the burden of proof.

Last but not least the rules established by Article 11 "are without prejudice to the liability under national law of parties to a transaction in which electronic identification means falling under the notified electronic identification scheme are used".

2.8. Interoperability

Mutual recognition of eID schemes is not possible without minimal agreement and cooperation on cross-border interoperability. For example, national schemes are not necessarily using identical sets of data to identify a natural or legal person. Exchange of identification data also means that countries have to agree on certain technical standards or on security provisions. Electronic identification schemes moreover often require specific hardware or software to be used by relying parties. In that case appropriate solutions should be discussed and developed within the scope of an interoperability framework.

Article 12.8 of the eIDAS Regulation has therefore mandated the European Commission to adopt implementing acts on the interoperability framework. Following this delegation, the Commission has issued an Implementing Regulation on this topic on 8 September 2015.[19] This Implementing Regulation lays down technical and operational requirements in order to ensure the interoperability of the electronic identification schemes which Member States notify to the Commission. Those requirements include in particular:

- minimum technical requirements related to the assurance levels and the mapping of national assurance levels of notified electronic identification means;
- minimum technical requirements requesting Member States a) to set up nodes able to connect with nodes of other Member States and to differentiate between public sector bodies and other relying parties, and b) to use common message formats to exchange data between these nodes;
- the minimum set of person identification data uniquely representing a natural or legal person (data listed in the Annex of the Implementing Regulation) and the character set used for the transmission (original characters but, where appropriate, also transliterated into Latin characters);

[19] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance), OJ L 235, 9.9.2015

- common operational security standards, for example, with regard to the storage of data which, in the event of an incident, enable reconstruction of the sequence of the message exchange for establishing the place and the nature of the incident;
- arrangements for dispute resolution: negotiation between the concerned Member States and, if this is not successful, resolution by the Cooperation Network.

2.9. Evaluation

Mutual recognition of notified electronic identification schemes enables persons to use the identification means issued in the Member State where they usually live, each time they wish to access a online public service in another Member State. By way of example, a Dutch eID issued under a scheme notified by The Netherlands, will be "recognised" by online public services in Belgium, or vice versa.

To "recognise" is, however, in most cases only the very first step in the process leading to the actual access and use of an online service. User and access management of such a service comprises many other elements, besides the mere recognition of an eID. In addition, there are many other obstacles for cross-border access and use of online public services.

One of such obstacles may be the language. Online public services are usually provided in the national language and they rarely offer a translated version for foreign users. In some cases, these services also request the user to provide specific data which refer to the own nationals, sometimes in formats typical for a national context and in a specific format (not accepting, for example, foreign postal codes).

More important is that the intended result of the eIDAS Regulation, if ever achieved, remains limited to the recognition of an identity. It enables a public service provider in Member State A to control whether or not the identity of the foreign user is known in Member State B. In practice, however, the public service provider needs much more information before it can give access to the service. Is the foreign user a medical professional who can access the electronic patient record? Does the user have the claimed legal mandate to represent a company? Is the foreign user, who wishes to register online as a student in a university, really a student who has the diplomas necessary to enter the requested study level?

The conclusion is therefore that the (first part of the) eIDAS Regulation establishes the initial basis for the provision of cross-border online public services. This initial basis is necessary but many more efforts will be needed in the future to produce practical results on a large scale.

3. Trust services

3.1. Background

The current legal framework is often not very clear on the type of evidence that is required when dealing with electronic transactions. It provides a much lower degree of legal certainty and security than the evidentiary framework for paper-based transactions. What is the legal value of an e-mail? How should I prove that a customer ordered this product in my online web shop?

It seems therefore necessary to foster more trust in the new environment. The most obvious solution is to promote the use of electronic signatures in all situations where we formerly used handwritten signatures. Electronic documents can be secured with electronic signatures and parties can exchange signed copies, just as they used to do it in the paper-based context.

From the legal side, it seems obvious to support this practice via equivalency rules. If the law states that sufficiently secure electronic signatures are equivalent to handwritten signatures, people will no longer be reluctant to enter into electronic transactions.

However, this approach does raise a number of questions. For one, what is regarded as "sufficiently secure" in an electronic environment? As long as the legislator is not able to clarify this, will the equivalency rule not fail to provide sufficient legal certainty? And what about the steering effect of this equivalency approach? Is it wise, in the new online environment, to push people to continue to behave as before? Should the law not better first observe how people tend to behave spontaneously in this new environment and only subsequently determine what kind of evidence is best suited for legal purposes?

When, back in the late nineties, the European Union adopted its legal framework for electronic signatures and certification services, the equivalency approach was the only option seriously considered.[20] One of the reasons probably is that the online environment was much less developed, complex, evolving and heterogeneous as it is today. Another reason is that, at that time, it was much more difficult than today to abandon the traditional paper-based paradigm and to imagine a world where information processing and exchange consequently makes use of all the possibilities of digital technology.[21]

The European Directive 1999/93/EC thus essentially stipulated that, if electronic signatures are sufficiently secure – "qualified" in the terminology of the directive – they should be considered as equivalent to handwritten signatures. One difficulty has been the necessary further clarification on what "sufficiently secure" exactly means. Some high-level criteria for evaluating this were adopted together with the text of the Directive and included in four annexes. The European standardization bodies received a mandate to further develop these criteria in technical specifications or other standardization documents.[22] The whole exercise was getting increasingly complex and it became apparent, as could be expected, that complexity rarely leads to legal certainty.

[20] Within the EU, the legal framework on electronic signatures is mostly set by Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, *OJ* L 13 of 19 January 2000, 12-20.

[21] J. Dumortier, Legal Status of Qualified Electronic Signatures in Europe, in S. Paulus, N. Pohlmann, H. Reimer, (ed.), ISSE 2004-Securing Electronic Business Processes, Vieweg (2004): 281-289.

[22] Article 9 Directive 1999/93/EC.

Many stakeholders, including the European Commission, have recognized that the Electronic Signatures Directive has not been a major success.[23] Authors regretted that the "qualified" electronic signatures, recommended by the legislator, were not sufficiently used in practice.[24]

What are the main reasons for this lack of success? One hypothesis is that it is due to the incompleteness of the legal framework. In order to inspire more trust in digital transactions, it is not sufficient to regulate electronic signatures. One should regulate the entire lifecycle of electronic transactions and consequently all kinds of trust services intervening in that lifecycle. This is exactly what has been done in the second part of the eIDAS Regulation. As it is stated in Recital (21), the Regulation establishes "a general legal framework for the use of trust services".

3.2. Scope of application

The term "trust service" in the context of the eIDAS Regulation has a very specific and limited scope. It includes only electronic services normally provided for remuneration which consist of:

- the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
- the creation, verification and validation of certificates for website authentication; or
- the preservation of electronic signatures, seals or certificates related to those services.

As a consequence, the term mainly refers to PKI-related services. These services can consist in the issuance of digital certificates for one or more of the five mentioned purposes: signatures, seals, time stamps, registered delivery and web authentication. They can further consist in creating, verifying or validating signatures, seals, time stamps, messages related to registered delivery services or web authentication certificates. Preservation of electronic signatures – not, as such, of electronic documents - is also included. According to Recital (24) Member States may maintain or introduce national provisions, in conformity with Union law, relating to trust services as far as those services are not fully harmonised by this Regulation. However, trust services that comply with this Regulation should circulate freely in the internal market.[25]

The eIDAS Regulation doesn't create a general obligation to use trust services. In particular, it doesn't cover the provision of services used exclusively within closed systems between a defined set of participants, which have no effect on third parties. For example, systems set up in businesses or public administrations to manage internal procedures making use of trust services aren't subject to the Regulation. Only trust services provided to the public having effects on third parties should meet the requirements laid down in the Regulation. Moreover, it doesn't cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form laid

[23] This became apparent during the impact assessment: Commission staff working document of 7 June 2012 impact assessment accompanying the document proposal for a regulation of the European Parliament and of the Council on electronic identification and tryst services for electronic transactions in the internal market, *SWD(2012) 135 final*, 9-12.

[24] H. Graux, Rethinking the e-signatures directive: on laws, trust services and the digital single market, Digital Evidence & Electronic Signature Law Rev. 8 (2011): 9-24.

[25] Consequently nothing will prevent Member States to introduce national rules applicable to services which are not regulated by the eIDAS Regulation, such as archival services, pseudonymisation services, etc.

down by national or Union law. In addition, it will not affect national form requirements pertaining to public registers, in particular commercial and land registers.[26]

3.3. Rules applicable to all trust service providers

Non-qualified trust service providers are only subject to a light touch and reactive ex post supervision. The supervisory body doesn't have a general obligation to supervise non-qualified service providers. It should only take action when it is informed (for example, by the non-qualified trust service provider itself, by another supervisory body, by a notification from a user or a business partner or on the basis of its own investigation) that a non-qualified trust service provider does not comply with the requirements of the Regulation.

These requirements are extremely limited. The Regulation contains a very general provision with regard to security requirements but this obligation doesn't seem to go further than what is commonly requested from every service provider. The main provision applicable to non-qualified trust service providers relates to security breach notification.

All trust service providers – qualified or not - shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein. Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA. The notified supervisory body shall inform the public or require the trust service provider to do so, where it determines that disclosure of the breach of security or loss of integrity is in the public interest.

The supervisory body shall provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers. The Commission may, by means of implementing act, further specify the security measures for all trust service providers and define the formats and procedures, including deadlines, for the security breach notifications.

3.4. Rules only applicable to qualified trust service providers

Introduction

A qualified trust service provider is a trust service provider who provides one or more qualified trust services and is granted the qualified status by the designated supervisory body in the Member State where it is established. In the first place qualified trust services relate to one or more of the five purposes explicitly mentioned in the Regulation: signatures, seals, time stamps, electronic delivery and web authentication.

Recital (25), however, states that "Member States should remain free to define other types of trust services in addition to those making part of the closed list of trust services provided for in this Regulation, for the purpose of recognition at national level as qualified trust services". The Regulation introduces

[26] Recital (21) of the Regulation

consequently a distinction between qualified trust services that are recognised on a European-wide scale and qualified trust services that are only recognised on a national level.

The eIDAS Regulation contains specific quality requirements for qualified service providers. Some of them are only addressed to providers issuing qualified certificates. Others affect all qualified trust providers.

The most important characteristic of a qualified trust service provider is to supervised by a national public authority. If a trust service provider decides to provide one or more of his services under such a supervision scheme, a series of other obligations will become applicable. These include the submission of a conformity assessment report, a bi-annual audit and – most importantly – a much stricter liability regime if an incident causing damages occurs. In return for these efforts, the provider will receive a EU trust mark. The value of this label will depend on the market. From a legal point of view, it should be clear from the start that the Regulation doesn't impose the use of qualified trust services. Again, this doesn't prevent Member States or even the Union to impose such use for particular transactions or procedures. Recital (22) specifies that "it is for the national law to define the legal effect of trust services, except if otherwise provided in this Regulation".

As will be explained later, the Regulation introduces a general obligation "to recognise" qualified trust services. What happens, however, if one receives a document with a qualified electronic signature but is unable to read or verify it due to technical reasons? Recital (23) states that "to the extent that this Regulation creates an obligation to recognise a trust service, such a trust service may only be rejected if the addressee of the obligation is unable to read or verify it due to technical reasons lying outside the immediate control of the addressee. However, that obligation should not in itself require a public body to obtain the hardware and software necessary for the technical readability of all existing trust services."

Requirements for qualified trust service providers

Article 24 of the Regulation contains a series of general requirements to be met by qualified trust service providers. These requirements are to a large extent similar to those already listed in Annex 2 of the 1999/93 Electronic Signature Directive. Besides duties related to, for instance, employment of qualified staff, sufficient financial resources, precise terms and conditions, record keeping, termination plan, etc. the main requirement relates to the use of trustworthy systems and products. The Commission may, by means of implementing acts, establish reference numbers of standards for trustworthy systems and products. Compliance will then be presumed where trustworthy systems and products meet those standards.

Specific requirements are addressed to qualified trust service providers which issue qualified certificates for trust services. These requirements are mainly related to the registration process: face-to-face identity or attribute verification and, if this is not possible, other identification methods which provide equivalent assurance in terms of reliability. The other requirements, for instance with regard to the revocation process and the availability of certificate status information, are quite evident.

Overall the quality requirements to be met by qualified trust service providers are far from being exceptional and correspond more or less to what is generally considered as the state-of-the-art in this domain. The difference between qualified and non-qualified is therefore much more related to procedural elements, such as formal conformity assessment, periodical external audits and administrative duties related to the supervision by public authorities

Initiation of a qualified trust service

Article 21.1 of the Regulation states that a non-qualified trust service provider that decides to start providing qualified trust services, should first notify the supervisory authority of its intention together

with a conformity assessment report issued by a conformity assessment body.[27] The supervisory body subsequently verifies whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation. If the result of this verification is positive, the supervisory body grants qualified status to the trust service provider and the trust services it provides.[28] The provider can effectively start to provide the qualified service once the qualified status is indicated on the trusted list. Compared to the situation under the 1999/93 Electronic Signature Directive, this *a priori* control procedure before accessing the market as a qualified service provider, is probably one of the principle novelties introduced by the eIDAS Regulation.

A certification-service-provider issuing qualified certificates under Directive 1999/93/EC shall submit a conformity assessment report to the supervisory body as soon as possible but not later than 1 July 2017. Until the submission of such a conformity assessment report and the completion of its assessment by the supervisory body, that certification-service-provider shall be considered as qualified trust service provider under this Regulation.[29]

The Regulation is not very precise on the initiation process and this could lead to substantial differences between the Member States. Therefore Article 21 gives the European Commission a possibility, by means of implementing acts, to further define the formats and procedures to be followed.

Supervision of qualified trust service providers

Qualified trust service providers will have to be audited at their own expense at least every 24 months by a conformity assessment body. The qualified trust service providers should submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.

In addition, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers. Where personal data protection rules appear to have been breached, the supervisory body informs the data protection authorities of the results of its audits.

Where the supervisory body requires the qualified trust service provider to remedy any failure and where that provider does not act accordingly, the supervisory body may withdraw the qualified status of that provider or of the affected service it provides.

Trusted lists

In order to validate advanced electronic signatures supported by qualified certificates, a receiving party would first need to check their trustworthiness. This means that the receiving party has to be able to verify whether the signature is an advanced electronic signature supported by a qualified certificate issued by a supervised certification service provider. Although the information necessary to verify these signatures should in principle be retrievable from the signature itself and from the content of the qualified certificate

---

[27] "Conformity assessment body" means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides. Conformity will be assessed against ETSI standards EN 319401, 319411 and 319421.

[28] If the verification is not concluded within three months of notification, the supervisory body informs the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded.

[29] Art. 51.3 of the Regulation.

supporting it, this process can be rather difficult. Publicly available Trusted Lists make it much easier for signature recipients to verify the e-signatures by complementing the data that can be retrieved from the e-signature and the qualified certificate and by providing also information on the supervised/ accredited status of Member States' certification service providers and their services.

Already under the 1999/93 Electronic Signatures Directive Member States had the obligation to establish and publish their Trusted List of supervised/accredited certification service providers issuing qualified certificates to the public.[30] Member States had to establish and publish their Trusted List by 28 December 2009 at least in a "human readable" form but were free to produce also a "machine processable" form which allowed for automated information retrieval. The Trusted Lists had to be made available by all Member States, including those who have no certification service providers issuing qualified certificates; the fact that a national Trusted List is empty will then indicate the absence of certification service providers issuing qualified certificates. In order to allow access to the trusted lists of all Member States in an easy manner, the European Commission has published a central list with links to national "trusted lists".[31]

The obligation to establish, maintain and publish trusted lists has been inserted and extended in the eIDAS Regulation. Article 22 of the Regulation states that "each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them". There is also an obligation for Member States to publish an electronically signed or sealed version of this list in a form suitable for automated processing and a similar obligation for the European Commission with regard to the compiled list.[32]

EU trust mark

After the qualified status of a trust service provider has been indicated in the Trusted List the provider may use a EU trust mark to indicate in a simple, recognisable and clear manner the qualified trust services it provides. When using the EU trust mark for the qualified trust services the provider is requested to put a link to the relevant trusted list on its website. is made available on their website.

The form and presentation of the trust mark has been further specified in a Commission Implementing Decision of 22 May 2015.[33]

[30] Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the points of single contact under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market, OJ L 274, 20.10.2009, p. 36–37

[31] In accordance with the ETSI TS 102 231, the compiled list is available on a secure web site in two formats: a human readable format PDF and a format suitable for automated processing XML (see further https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-certification-service-providers)

[32] Article 22.5 of the Regulation mandates the European Commission to further define the technical specifications and formats for trusted lists and the information to be provided by Member States in this context. This has been done in Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists, OJ L 235, 9.9.2015, p. 26–36.

[33] Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services, OJ L 128, 23.5.2015, p. 13–15

Liability and burden of proof

Liability for damage from the side of non-qualified trust service providers doesn't in practice deviate from normally applicable liability rules. In essence this means that the person claiming the damage has the burden of proving the damage, the negligence or faulty intention and the fact that the damage was caused by this negligence or intention.

In the case of a qualified trust service provider, the situation is different. The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage occurred without his intention or his negligence. The reversal of the burden of proof in case of damage is one of the important consequences trust service providers have to bear if they choose to act under the "qualified" regime.

In order to facilitate the assessment of financial risk that trust service providers might have to bear or that they should cover by insurance policies, this Regulation allows trust service providers to set limitations, under certain conditions, on the use of the services they provide and not to be liable for damages arising from the use of services exceeding such limitations. Customers should be duly informed about the limitations in advance. Those limitations should be recognisable by a third party, for example by including information about the limitations in the terms and conditions of the service provided or through other recognisable means.

As usual these European rules on liability have to be applied "in accordance with national rules on liability". The Regulation does not affect national rules on, for example, definition of damages, intention, negligence, or relevant applicable procedural rules.

International aspects

According to Art. 14.1 of the eIDAS Regulation, "trust services provided by trust service providers established in a third country shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union where the trust services originating from the third country are recognised under an agreement concluded between the Union and the third country in question or an international organisation in accordance with Article 218 TFEU". It is evident that the qualified trust service provider recognised under such an agreement, needs to meet all the requirements of the Regulation applicable to EU-based qualified trust service providers.

Recognition via international agreement between the Union and a third country or an international organisation, seems only possible for services making part of the closed list of trust services provided for in the Regulation. Equivalence of third country based trust services with qualified trust services that are only defined and recognized at a national level would be excluded.

3.5. Electronic signatures

With regard to electronic signatures the eIDAS Regulation doesn't drastically change the existing rules, already applicable under the 1999/93 Electronic Signature Directive. An electronic signature remains defined by Art. 3(10) as "data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign". As before this definition refers to all kinds of methods, more or less secure, whereby electronic data are used by a natural person to sign. "To sign" implicitly refers to an analogy with handwritten signatures and to the intention of a natural person to perform "something similar" in an electronic context.

Continuity, except for part of the terminology, is also ensured with regard to the requirements of "advanced electronic signatures", listed in Art. 26 of the Regulation: (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.

Under the 1999/93 Electronic Signature Directive there has been a discussion about the third requirement – data under sole control of the signatory – and its meaning in respect to server-based signature solutions. This point is now clarified in Recital (51) of the eIDAS Regulation. According to Recital (51) "It should be possible for the signatory to entrust qualified electronic signature creation devices to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control over the use of his electronic signature creation data, and the qualified electronic signature requirements are met by the use of the device".

As before, under the Electronic Signature Directive, a "qualified electronic signature" means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures". Annex 1 of the Regulation contains a list of requirements to be met by qualified certificates, more or less identical to the one of Annex 1 of the Electronic Signature Directive. Annex 2 contains the list of requirements for qualified electronic signature creation devices. Conformity with these requirements should be certified by appropriate public or private bodies designated by Member States. Member States will notify to the Commission the names and addresses of the designated bodies and information on the qualified electronic signature creation devices that have been certified by these bodies. On the basis of the information received, the Commission will establish, publish and maintain a list of certified qualified electronic signature creation devices.[34] Such a list didn't exist under the Electronic Signature Directive and is without any doubt a factor that will provide more clarity in this field.

Recital (52) explicitly refers to "remote electronic signatures", where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory. It confirms that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, as long as remote electronic signature service providers apply "specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory". Overall it is important to emphasize that the eIDAS Regulation, in order to remain open to innovative signing methods, doesn't impose a particular security standard for the certification of electronic signature creation devices.

On the other hand, it should not be forgotten that, order to recognise a qualified electronic signature, a court or an expert will need to look at more than only the certificate and the creation device. Recital (56) clearly states that "this Regulation should not cover the entire system environment in which such devices operate. Therefore, the scope of the certification of qualified signature creation devices should be limited to the hardware and system software used to manage and protect the signature creation data created, stored or processed in the signature creation device. As detailed in relevant standards, the scope of the certification obligation should exclude signature creation applications".

[34] Article 51 contains some transitional measures. Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall be considered as qualified electronic signature creation devices under this Regulation. Qualified certificates issued to natural persons under Directive 1999/93/EC shall be considered as qualified certificates for electronic signatures under this Regulation until they expire.

Another novelty introduced by the eIDAS Regulation relates to the recognition of advanced electronic signatures. In practice it is not easy to verify whether or not each of the four requirements listed in Art. 26 have been met. To overcome this difficulty Art. 27.4 provides that the Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic signatures. Compliance with the requirements for advanced electronic signatures shall be presumed when an advanced electronic signature meets those standards.

Article 32 of the eIDAS Regulation furthermore clarifies the link between the validation and the validity of a qualified electronic signature. Validation is a to large extent a technical process. It is usually carried out on the device used by the relying party or delegated to a service provider.[35] The system used by the relying party needs to fulfil a series of requirements listed in Art. 32.1. The Commission may, by means of implementing acts, establish reference numbers of standards for the validation of qualified electronic signatures. Compliance with the requirements of Art. 32.1 shall be presumed where the validation of qualified electronic signatures meets those standards. In practice this means that, if a relying party uses a validation system or service meeting recognized technical standards, this party can reasonably assume that what it received, is a qualified electronic signature.

Article 25.1 of the Regulation states that "an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures". The scope of this so-called non-discrimination rule is however very limited in the eIDAS Regulation. This can be concluded from Recital (49) which says that the principle doesn't affect the competence of national legislators to define the legal effect of electronic signatures. As a consequence, Art. 25.1 doesn't prevent Union or national legislators to impose the use of qualified electronic signatures for particular transactions or in specific administrative procedures. In such case, if a court rejects a non-qualified signature, it doesn't so "solely" on the grounds that it is not a qualified electronic signature but (also) on the grounds that it doesn't meet legally imposed formal requirements.

The limited scope of the non-discrimination principle also affects the interpretation of Art. 25.2 of the Regulation. This provision states that "a qualified electronic signature shall have the equivalent legal effect of a handwritten signature". Recital (49) adds that, notwithstanding the competence of national legislators to define the legal effect of electronic signatures, they are not competent to modify the requirement according to which a qualified electronic signature should have the equivalent legal effect of a handwritten signature. Apparently Art. 25.2 has merely to be interpreted in the perspective of the internal market and in particular the cross-border recognition of qualified electronic signatures. It doesn't prevent national legislators to link other legal effects to qualified electronic signatures – other than the equivalence to handwritten signatures.

Art. 25.3 further states that "a qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States". This provision should not be misinterpreted. It doesn't mean that qualified electronic signatures will have the same validity throughout the European Union. The legal effect of qualified electronic signatures will be different for every Member State and this in both cases: a) when their legal effect is automatically

[35] Art. 33 introduces the concept of a "qualified validation service". This is a validation service provided by a qualified trust service provider. Using a qualified validation service leads to a legal presumption regarding the validity of a qualified electronic signature. Art. 34 of the Regulation contains a similar provision regarding the qualified preservation services for qualified electronic signatures.

deducted from the equivalence to handwritten signatures, and b) when their legal effect is explicitly determined by national law.[36]

Rules about electronic signatures can of course also be imposed by Union law. According to Art. 27.3 of the Regulation "Member States shall not request for cross-border use in an online service offered by a public sector body an electronic signature at a higher security level than the qualified electronic signature". In addition, as public authorities in the Member States currently use different formats of advanced electronic signatures to sign their documents electronically, it is necessary to ensure that at least a number of advanced electronic signature formats can be technically supported by a Member State's public administration when it receives documents signed electronically from another Member State. This problem was already tackled in the context of the Services Directive.[37] Giving implementation to Art. 27 of the eIDAS Regulation the Commission has issued an implementing Decision laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies.[38]

3.6. Electronic seals

An "electronic seal" is defined by the eIDAS Regulation as "data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity". This definition is very wide because it covers almost all applications of PKI-based technologies. Apparently, however, the European legislator essentially wanted to address seals issued by legal persons. This can be deducted from Recital (59) which states that "electronic seals should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity."

Recital (58) mentions that "when a transaction requires a qualified electronic seal from a legal person, a qualified electronic signature from the authorised representative of the legal person should be equally acceptable". According to Recital (60), "trust service providers issuing qualified certificates for electronic seals should implement the necessary measures in order to be able to establish the identity of the natural person representing the legal person to whom the qualified certificate for the electronic seal is provided, when such identification is necessary at national level in the context of judicial or administrative proceedings. Finally, Recital (65) specifies that "in addition to authenticating the document issued by the

[36] Recognition of qualified electronic signatures based on qualified certificates issued in other Member States doesn't prevent a Member State to impose the use of a specific creation device – for example a national electronic identity card – for particular transactions or procedures.

[37] Commission Implementing Decision 2014/148/EU amending Decision 2011/130/EU establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market, OJ L 80, 19.3.2014, p. 7. This Implementing Decision defined a number of the most common advanced electronic signature formats to be supported technically by the Member States, where advanced electronic signatures are required for an online administrative procedure.

[38] Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, OJ L 235, 9.9.2015, p. 37–41. The Implementing Decision establishes e.g. that Member States requiring an advanced electronic signature or an advanced electronic signature based on a qualified certificate shall recognise XML, CMS or PDF advanced electronic signature at conformance level B, T or LT level or using an associated signature container, where those signatures comply with the technical specifications listed in the Annex of the Decision.

legal person, electronic seals can be used to authenticate any digital asset of the legal person, such as software code or servers."

Similar to the concept of "qualified electronic signature", the Regulation introduces the concept of "qualified electronic seal". Such a seal is based on a qualified certificate meeting the requirements of Annex III of the Regulation. Essentially this Annex lists the items that should be included in a qualified certificate for an electronic seal. This list is exhaustive and no other mandatory requirements should be added. However, additional non-mandatory items, for instance attributes, are permitted as long they do not affect the recognition or the interoperability of the certificate. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic seals. Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal meets those standards.

In practice electronic seals are today mainly used for so-called "code-signing". Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed by use of a cryptographic hash. It is not impossible that market players in this field, driven by competition, will find it worthwhile to upgrade themselves to "qualified trust service providers", simply in order to obtain the EU trust mark and use it as a competitive advantage.

From a legal point of view, the use of qualified electronic seals doesn't provide substantial added-value. The eIDAS Regulation simply states that "a qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked." If one uses services provided by a well-known company with an established reputation of complying to generally recognised best practices, such a presumption exists, however, anyhow.

3.7. Electronic time stamps

Article 3(33) of the eIDAS Regulation defines an "electronic time stamp" as "data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time". The evidence is established by sending a fingerprint of a file to a time stamp provider. The provider returns the return a signed electronic timestamp certificate that contains the file's fingerprint.

According to Article 42 a qualified electronic time stamp shall meet the following requirements: a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably; b) it is based on an accurate time source linked to Coordinated Universal Time; and c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method. The Commission may, by means of implementing acts, establish reference numbers of standards for the binding of date and time to data and for accurate time sources. Compliance with the requirements laid down in Article 42 shall be presumed where the binding of date and time to data and the accurate time source meets those standards.

Recital (62) specifies that "in order to ensure the security of qualified electronic time stamps, this Regulation should require the use of an advanced electronic seal or an advanced electronic signature or of other equivalent methods. It is foreseeable that innovation may lead to new technologies that may ensure an equivalent level of security for time stamps. Whenever a method other than an advanced electronic seal or an advanced electronic signature is used, it should be up to the qualified trust service provider to demonstrate, in the conformity assessment report, that such a method ensures an equivalent level of security and complies with the obligations set out in this Regulation".

In practice electronic time stamps are very rarely used. It is seldom necessary to establish the exact time of a transaction for legal purposes. Where needed, for example in the context of administrative or judicial

procedures, there are sufficiently secure alternatives. In most cases the receipt of a document in– generally web-based - official procedures is simply confirmed by the government office in charge.

It is therefore doubtful whether "qualified" time stamps will be used in the future. Besides the EU trust mark, a qualified electronic time stamp enjoys "the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound."[39] Consequently, in case of a legal dispute about the trustworthiness of an electronic time stamp, a qualified time stamp would have the benefit of a presumption, whatever this means in practice. Such disputes will clearly not occur every day. As for signatures, seals and other trust services, the only risk is that some Member States will impose the use of qualified time stamps in some of their procedures, either by law or in the context of their public procurement.

3.8. Electronic registered delivery services

Article 3(36) of the Regulation defines an "electronic registered delivery service" as "a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations". According to Art. 43.2 "data sent and received using a *qualified* electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service".

In practice electronic delivery services – often also called "electronic registered mail" – are not frequently used. The solution, entirely based on the model of traditional registered mail services provided by postal service providers, is very complex and expensive. In addition, such kind of service is seldom needed because it can easily be replaced by strong authentication combined with secure uploading of information on a website.

It is therefore questionable whether providers will risk additional investments necessary to meet the requirements imposed by the Regulation on qualified trust providers.[40]

3.9. Website authentication

Website authentication services provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website. The assurance is in general provided by using SSL certificates. These certificates digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser.[41]

The eIDAS Regulation introduces the concept of "qualified" website authentication services. Such authentication services have to meet minimum requirements laid down in Annex IV of the Regulation. Most of these requirements are related to the content of the certificates and the possibility to validate such certificates free of charge. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for website authentication. Compliance with the

[39] Article 41.2

[40] It is, however, not excluded that some Member States will impose the use of qualified electronic delivery services, for example by law or in the context of their public procurement.

[41] See also https://cabforum.org/

requirements laid down in Annex IV shall be presumed where a qualified certificate for website authentication meets those standards.

In addition, website authentication service providers are subject to all other provisions of the Regulation applicable to qualified trust service providers. These include, besides being submitted to the supervision by the national supervisory authority, the submission of a conformity assessment report, a bi-annual audit and – most importantly – a much stricter liability regime if an incident causing damages occurs. In return for these efforts, the provider will receive a EU trust mark. The value of this label will depend on whether or not Member States will impose the use of qualified web authentication services, for example in the context of public procurement.

Third country providers of website authentication services can only have their website authentication services recognised as qualified in accordance with the Regulation, if an international agreement between the Union and the country of establishment of the provider has been concluded. As a consequence, depending on the – perhaps not very probable - future success of the EU trust mark labelled SSL certificates, it is not excluded that some of these third country providers will open in the future an establishment in the Union.

3.10. Evaluation

The legal effects mentioned in the Regulation are meant to privilege the use of qualified trust services. Even if it doesn't force market players to use such services, the Regulation creates an impression that qualified trust services provide a higher level of legal certainty. In addition, it can be expected that some Member States will impose the use of qualified trust services for specific transactions or procedures.

The kind of trust services promoted by the Regulation are typically services which are inspired by the way people work in a paper-based environment. When using paper documents, exchanging signed copies of, for instance, a contract between parties, provides probably the most efficient form of proof. In the case of distant parties, the signed document needs to be physically transported, preferably using a registered mail service. This is simply due to the fact that, in a paper-based context, information can only be exchanged between parties by producing paper documents, authenticating them with handwritten signatures and transmitting the documents physically from one party to the other.

In a digital context, things are different. In order to exchange information between parties, we no longer need to create documents which need to be transmitted from point A to point B. Working digitally allows us to store the information on one location and subsequently to provide access to this information to anyone who needs it.

Providing evidence of a transaction in a digital context is no longer a matter of exchanging signed documents and sending them securely from point A to point B. On the contrary, distant parties have now access to the same electronic file and modern information systems keep secure logging of every access and every action, including the exact point in time of such access or action. If an incident occurs, we now have the means to "replay" what happened, much in the same way as we are using the "black box" when there is an incident in the aviation domain.

Creating a legal framework for "trust services" and promoting the use of "qualified trust services" as it is done by the eIDAS Regulation includes therefore a risk. Even if the Regulation doesn't impose the use of qualified trust services, it could negatively influence decisions by market players who otherwise would have chosen for a much more efficient path, better adapted to the digital context.

Instead of primarily striving for the most efficient and effective assurance solution in a given case, market players could get the impression that the only trustworthy solution consists in using the PKI-based toolbox

that is put forward by the Regulation. As a consequence, it is not excluded that the eIDAS will not only increase the level of uncertainty but also slow down the introduction of alternative innovations to provide more trust in online electronic transactions.

It has been suggested that on the positive side of the existing legal framework created by Directive 1999/93/EC has been its limited impact. It is not excluded that this will not be different as far as the (second part of the) eIDAS Regulation is concerned.