THE REGULATORY FRAMEWORK OF DIGITAL IDENTIFICATION SERVICES ACROSS THE EUROPEAN UNION AS A GUARANTEE OF SUCCESS FOR THE DIGITAL SINGLE MARKET

Cristina Timón López, Ignacio Alamillo Domingo, Julián Valero Torrijos
Department of Administrative Law. OLYMPUS project. University of Murcia

ABSTRACT: Digitalized societies require mechanisms to identify individuals across the operations that take place therein. Electronic identification plays a key role in the realization of the Digital Single Market as the establishment of trustworthy relationships is based on the knowledge of the parties involved. Nevertheless, the regulation of electronic identification means across the EU is complex due to the inherent link to Members States' sovereignty. Consequently, different regulations have emerged, but, at the same time, this diversity has led to the fragmentation of the regulatory framework depending on the scope of the identification and authentication processes, as well as the nature of the activity (i.e., public or private) of the entity providing the electronic identification service.

The aim of this paper is to offer a general overview of the regulations applying to electronic identification and authentication processes across the EU. For that purpose, we refer to the main applicable regulations to electronic identification and authentication in the EU, highlighting their scope of application as well as the main drawbacks detected. In addition, this paper refers to the liability sources that might arise in the context of electronic identification and authentication processes, as well as three context-specific regulations.

KEYWORDS: Digital Identity, Regulatory framework, eIDAS Regulation, e -Commerce Directive.

1. INTRODUCTION

The transition to digitalized societies as well as the increase of the activities that take place in the online environment requires individuals to be identified through new means, the Internet. The Internet has evolved in the past twenty years from a reduced group of people to a countless number of participants (including natural persons and legal entities) interconnected between themselves [1]. Consequently, the task of assuring the identity of a person in online operations represents one of the main challenges of the Internet era and is a fundamental piece in the realization of the Digital Single Market [2].

However, the regulation of identification services is behind the development of the markets for two main reasons. On the one hand, because the quick development of the market makes difficult to offer regulatory answers in such a short time [3]. On the other hand, because identification services are inherently linked to Member States' sovereignty. The consequence has been the emergence of a panorama where the regulation of identification services is split depending on the nature (i.e., public or private activity) of the entity providing that service and the scope of the provision of the service (i.e., before public or private services). The Regulation (EU) no 910/2014

of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [4] (hereafter, the eIDAS regulation), has been an excellent first example of a legal framework for digital identities across the European Union (hereafter, EU). However, its scope of application is very limited as it only refers to cross-border public services among the Member States. Indeed, although its Recital 17 establishes that the eIDAS Regulation aims to encourage the use of notified electronic identification means across public and private entities, its scope of application is in principle exclusively limited to public services. Consequently, regulations differ depending on the scope of the identification and authentication process. In this sense, the level of assurance required for identification and authentication of a user at a common website or in an administrative transaction (e.g., the request of a social aid) is different. In the second scenario the level of assurance required has been thought as higher and identity providers of different nature have emerged.

The aim of this paper is to offer an overall perspective of the regulatory framework of digital identity systems across the EU. For that purpose, we will refer to the legal framework of digital identities par excellence, that is to say, the eIDAS Regulation, as well as its main limitations or constrains. On the other hand, we will refer to other regulations that apply to entities providing electronic identification services such as the e-Commerce Directive [5], the Anti-money laundering and Payment Services Directives [6] [7], or the coming modification of the Directive concerning measures for a high common level of security of network and information systems across the Union [8].

2. THE EIDAS REGULATION

2.1. Content and scope of application

The eIDAS Regulation is the EU law that established a legal framework to facilitate cross-border recognition in the access, at least, to public services in other Member States. More specifically, it responds to two principal objectives [9]. On the one hand, to remove existing barriers for cross-border authentication in the Member States (Recital 12). On the other hand, encourage the private sector to use electronic identification means under notified scheme (i.e., uniform the validity of trust services) (Recital 17) [4]. For that purpose, besides procedural rules, it establishes a set of common high-level rules or principles and technical standards, completed by technical specifications that allow different national eID schemes in the EU to interoperate [10]. Indeed, Article 6.1 envisages the requirements for mutual recognition, in particular, the Member State must notify the electronic identification means to the European Commission and the electronic identification means must have a level of assurance (hereafter, LoAs) equal or higher than the one required for accessing a public service in the Member State and this LoA must be qualified as substantial pursuing the eIDAS Regulation.

From a technical point of view, the interoperability framework eIDAS covers different interfaces named as the “Proxy-configuration” or the “Middleware-configuration”. Nevertheless, the proxy approach is the usual configuration as the eIDAS Regulation is clearly envisaged in the context of delegated Identity Management (hereafter, IdM) through the use of “nodes” which assure communication between the different parties involved [11]. Definitely, the proxy approach has important advantages in terms of interoperability, but also raises privacy concerns due to these “bridges” created that

could control cross-border authentication processes taking place therein. Conversely, in the middleware approach, envisaged in the case of the German nPA, the communication takes place directly between devices, avoiding such control or surveillance. However, since this approach is based on the communication between software, it will raise more important problems in terms of achieving a unified technology across all Member States, which must also, pursuing Article 7 of the eIDAS Regulation, being provided free of charge.

2.2. Limitations of the eIDAS Regulation as legal framework for digital identity services across the European Union

The eIDAS Regulation has represented a first great example of a legal framework for identification services in the EU. However, the increasing number of electronic transactions and procedures, the arrival of extensive data protection regulations and the fast development of technology are increasing the need to review this Regulation to respond to current needs and be consistent with other EU Regulations.

The first limitation concerns the subject or entity providing identification services. Pursuing Article 7 (a) of the eIDAS Regulation, the electronic identification means must have been issued by the notifying Member State as the request thereof, or independently of the Member State, but notified and recognized by the Member State [11]. Consequently, we can distinguish three possible legal regimes of identification depending on the issuing subject. First, it could be the State itself who issues the electronic identification means as administrative activity. Second, it could be a private entity but under the mandate of the State which would also qualify as administrative activity. The third possibility would be the issuance of the electronic identification means by a private entity itself, in whose case the activity will qualify as private. These legal regimes have in common the necessary prior intervention of the State for cross-border recognition.

Although from the perspective of the eIDAS Regulation, electronic identification refers to a collection of public services, it does not close completely the door to its provision on the part of private entities as in the last category of services we can include trust services. The main reason for the exclusion of private entities in the provision of identification services is the eIDAS liability regime and the role of the State as a guarantor of notified electronic identification means. It must be noted, however, that electronic identification does not constitute itself a trust service, therefore, in theory, electronic identification issued by the private sector would depend on the agreement or voluntary cross-border recognition by the parties.

Nevertheless, in practice it is possible to provide electronic identification services by private entities by means of the issuance of electronic certificates. Indeed, according to what established in Article 26 (b) of the eIDAS Regulation, advance electronic signature is capable of identifying the signatory and a certificate represents an electronic attestation which links electronic validation data to a natural person and confirms at least the name or the pseudonym of that person [4]. In addition, when this certificate is qualified, the information contained therein is presumed to be legally true.

Public entity		Private entity		
Members State	Entity under the mandate of the Member State	Legal entity	Trust service	
			Qualified	Non-qualified
Electronic identification means under eIDAS		e-Commerce Directive 2000/31/EC	Electronic certificate to sign and for authentication purposes under eIDAS	

Table 2.1. Possibilities for the provision of identification services and applicable regulations Source: authors,2021

However, it seems an excessive requirement to constitute a trust service for the only purpose of providing identification services. Likewise, it must be noted that electronic certificates are in principle conceived for signing, therefore, to be covered by eIDAS they must be effectively used for signing besides for identification or authentication purposes. Consequently, as noted in Table 1, the provision of identification services by part of legal entities that do not qualify as trust services is subject to the Directive 2000/31/EC or the eCommerce Directive that we will refer in the following section.

Secondly, the technical standards envisaged by the eIDAS Regulation, more specifically in this case, the Annex of the 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 [12], limits the possibilities for cross-border recognition of IdM systems that differ from multi-factor authentication. As we have noted above, for cross-border recognition, electronic identification means need to achieve at least a substantial LoAs. Nevertheless, when we refer to the technical requirements to achieve a substantial LoAs a dynamic authentication method is required, which pursuing the definition contained in the article 3 of this text refers to multi-factor authentication[1] [12].

These requirements were devised in the year 2015, given the state of the art. However, the fast development of the technique requires their adaptation. In this sense, electronic identification means which are not based on multi-factor authentication, regardless their level of security, are not admitted. These restrictions would contravene nowadays the principle of technology neutrality as organizations and individuals would be prevented from using other electronic identification means than multi-factor authentication methods for cross-border operations, contravening what stated in Recital 16 of the eIDAS Regulation, “the requirements established should be technology-neutral” and “it should be possible to achieve the necessary security requirements through different technologies”. In consequence, it is clear that it is necessary to review this requirement and adapt it to nowadays technological possibilities to allow different technological designs which offer the same or even a higher protection than multi-factor authentication.

The third limitation refers to a possible inconsistency between the eIDAS Regulation and the General Data Protection Regulation (hereafter, GDPR). Despite the general rule of the eIDAS Regulation is that it must comply with data protection rules and facilitate privacy by design [4], in practice, it is arguable whether the eIDAS Regulation lowers the level of privacy achieved by data protection regulations or at least limits the

[1] “Dynamic authentication” means an electronic process using cryptography or other techniques to provide a means of creating on demand an electronic proof that the subject is in control or in possession of the identification data and which changes with each authentication between the subject and the system verifying the subject's identity.

deployment of privacy-preserving technologies. The clearest example is the case of claim-based IdM systems[2] which cannot be deployed with all their privacy features. Indeed, one of the main benefits offered by this schema is the possibility of sharing attributes in a privacy-preserving way, so the service provider does not obtain more information than the strictly necessary for the authentication purposes[3] [13]. However, the limited disclosure of data or user attributes would not comply with the minimum data set established in Section 1 of the Annex[4] of the Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [14]. Consequently, the attribute would have to be transmitted with all the other data that conform the minimum data set and this requirement would not comply with what established in Recital 39 and Article 5) of the GDPR, "the personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed" [15]. For the same reason, the pseudonymization described in the GDPR will not be achieved since alongside the pseudonym, each dataset has to contain the rest of mandatory identifiers [16] which would raise privacy concerns due to the possibilities of linkability [17].

In any case, it must be noted that the eIDAS Regulation does not really constitute the legal basis for the regulation of electronic identification systems, but only for their mutual recognition between Member States in the EU. Therefore, it does not mean that the electronic identification systems that do not meet the requirements established in Article 6.1 lack of recognition, but they will be subject to other regulations, such as the eCommerce Directive, or will rely on voluntary recognition by other Member States.

3. E-COMMERCE DIRECTIVE

In those cases where IdM services are provided by a private entity that does not qualify as trust service, we could consider whether the definition of Information Society Service (hereafter, ISS) contained in the Directive 2000/31/EC of 8 June on certain legal aspects of information society services applies. The e-Commerce Directive was born in the context of the beginning of digitalization of societies for the purpose of stimulating cross-border trade by removing legal obstacles in the freedom of establishment and the freedom to provide digital services in the different Member States despite the existence

[2] Claim- based IdM systems are a type of delegated/outsourced IdM. In this model the user obtains claims (normally in form of credentials) from the IdP, that he/she can store in his/her mobile device to authenticate before a service provider in a later moment in time. In this model communication between the identity provider and the service provider does not exist.

[3] This is technically possible through the implementation of techniques such as the p-ABCs or zero-knowledge proofs. Attribute Based Credentials are a form of authentication that allow to select different authentication attributes without revealing additional information. Zero-knowledge techniques are mathematical methods used to verify things without sharing or revealing underlying data. More information available at the following websites: https://privacypatterns.org/patterns/Attribute-based-credentials; https://www.wired.com/story/zero-knowledge-proofs/

[4] Section 1 of the Annex to the eIDAS Regulation imposes the obligation to use the following attributes for the identification of a natural person: a) surname or current surnames; b) current name or names; c) the date of birth and d) a unique identifier drawn up by the issuing Member State in accordance with the technical specifications for cross-border identification purposes and as constant as possible over time. Likewise, the following additional attributes are authorized: a) name or names and surname or surname of birth; b) place of birth; c) current address and d) sex.

of different regulations. At the same time, it aimed to promote the development of the information society by defining minimum rules on the roles and responsibilities of intervening parties. Nevertheless, the e-Commerce Directive has a very broad scope as it contains a wide definition of ISS covering "any service normally provided for remuneration[5], at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service" [18].

This definition is complemented with two major conditions envisaged in the e-Commerce Directive. On the one hand, the Clause of Internal Market forbids Member States to impose prior authorization or any requirement for the provision of ISS. Therefore, on the other hand, the provider of ISS can offer the service in all the other Member States by merely complying with the rules of the country of establishment (coordinated field) [5]. Pursuing these two conditions, in principle private providers of identification and authentication services before other private service providers could qualify as ISS and cross-border recognition effects and obligations would apply. However, this is not the most suitable solution for various reasons. On the one hand, because it causes the fragmentation of the regulation of identification and authentication services. On the other hand, because the e-Commerce Directive deals with a vast range of services in different areas [3]. In addition, in the cases of IdM, many services deploy internal or "silo model"[6] IdM systems. Therefore, in those cases where the service provider is not covered by the scope of this Directive, it will be the Member State who will freely regulate the service and it will not benefit from the effect of automatic cross-border recognition. Consequently, this Directive would apply in principle to IdM as a service in those cases where the private entity, provider of the service, is not qualified as trust service.

Nevertheless, the Internal Market Clause is one of the great successes of the e-Commerce Directive and is the cornerstone of the Digital Single Market [19]. It also highlights the need of trust and harmonization between the main protection rules in the Member States and cooperation between national authorities. In any case, the regulatory framework of electronic identification is not limited to the eIDAS Regulation or the e-Commerce Directive, but it also includes other regulations, which directly or indirectly refer to electronic identification services imposing a set of requirements or conditions in the provision of these services.

4. EID LIABILITY SOURCES

The existence of liability that covers potential damages or risks is an essential component in the achieving of trust. In the scenario of IdM systems, there exist two main risks: that the user accesses to a service or content that he/ she is not entitled to access, or the opposite case, that the user is denied that access [10]. In addition, other risks can appear such as those arising from inadequate security, that can lead to the unauthorized access and misuse of personal data. The determination of the damage might come from the part of the service provider, when he acts in reliance on false or compromised credentials, or from the user, when his/her personal data are compromised, cannot access a specific service, or is impersonated.

There are different regulations involved in the determination of liability in eID systems. First, the eIDAS Regulation envisages a tripartite liability regime. Pursuing this

[5] It the case Papasavvas and McFadden the Court of Justice of the EU decided that the ISS does not have to be paid by the recipient of the service, but the service can be paid with income generated by advertisements. Case C-291/13 *Papasavvas* EU:C: 2014:2209, paras.29-30.

[6] In identity silo model, the digital identities allow us to interact with the person or organization that has provided us with them.

regulation (Article 11), the notifying Member State shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligations. Indeed, the Member State holds a role of guarantor, ensuring that the person identification data uniquely represents the corresponding person, as well as assuring the availability of the authentication means without imposing disproportionate or excessive requirements that hamper the interoperability of the notified electronic identification means. In addition, the eIDAS Regulation also envisages the liability of the party issuing the electronic identification means, in particular in assuring that the identification means complies with the required LoA. In the case the party providing the identification services is qualified as a trust service we should also consider regulation applicable to thereof and the distinction in case of qualified or non-qualified trust services[7] [4].

Secondly, the Directive on Electronic Commerce will apply in those cases that the IdM services are provided by a private entity that does not qualify as a trust service. In this case, it would be necessary to determine whether the exemptions envisaged in the Articles 12 to 15 of the Directive apply. These exemptions refer to [5]: a) Mere conduit or transfer; b) Caching, that is, automatic, intermediate and temporary storage of information; c) Hosting, or information storage by the request of the service provider. Considering that the provision of IdM services goes beyond the activities exempt of liability according to this Directive, we can conclude that the exemptions shall not apply. However, the Directive does not establish a general liability regime applicable to the ISSs, but it just provides for a system of specific liability exemptions. Therefore, the identity provider liability will be determined by the national laws of the respective Member States[8] where the ISS is established.

Third, liability rules applying to IdM systems are also contained in data protection regulations (in the case of the EU, the GDPR). This liability directly applies when a data processing activity takes place in the territory of the EU without prejudice the scope thereof. In this case, we find the responsibility and liability of the controller for any processing taking place on its behalf (proactive approach) and the liability arising from any unlawful processing who has resulted in a material or non-material damage toany person (reactive approach) [15] [20].

The liability arising from these regulations must be understood without prejudice to any claims for damage deriving from the violation of other rules in the EU or Member State law. In some cases, Criminal Law will be the appropriate mechanism to limit and punish these actions. However, its requirements in terms of the burden of proof make in most of the cases Tort Law the most appropriate tool to protect user's privacy or other rights. Tort Law is differently regulated in the Member States, but its core lies on three basic criteria: a) The basis for liability, typically a negligent action or some sort of unlawful behavior; b) Harm; c) Causation between the basis of liability and the harm. In consequence, Tort Law could be an excellent mechanism to assure at least some right to compensation in those cases where the damage is not covered in other forms. In the end, "the internet is a global creature, but the laws of responsibility are rooted in national jurisdictions" (Schultz, 2014) [21].

Finally, liability might be extended thorough contractual law in order to encourage confidence or allocate responsibilities [10]. However, in this last case limitations will also be restricted to internal relationships without affecting users' rights established by

[7]Article 13 of the eIDAS Regulation establishes that "in the case of qualified trust services the burden of proving intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage".

the applicable law to claim for a compensation.

5. CONTEXT-SPECIFIC REGULATIONS

The regulatory framework of digital identities is also integrated by some context-specific regulations. We could highlight three specific regulations. First, the EU Revised Directive on Payment Services (PSD2) within the European Economic Area is a regulation that applies to service providers that offer their services, for remuneration, online. This regulation introduces in its Article 4 (30) the concept of Strong Consumer Authentication (SCA) [7]. The SCA aims to increase security in electronic payments and for that purpose it requires electronic payments to be performed with multi-factor authentication. More specifically, the factors must be independent in such a way that the compromise of one of them does not compromise the reliability of the other.

Second, the Anti-Money Laundering Directive (AML6) is a context-specific regulation that applies to financial entities in the provision of their services [6]. This regulation introduces the term Know Your Customer (KYC) that defines controls and procedures in the supervision of financial entities, the validation of their clients' identity and the origin of their founds with the purpose of avoiding commercial relationships with persons or entities committing crimes of type money laundering, financing terrorism or other illegal businesses. More specifically KYC requirements imply that during digital onboarding identification processes (i.e., at the moment of opening an account), it will be necessary to perform a formal identification where the financial entity assures that the person behind is real and the information declared is true. This formal identification will normally take place through the submission and collation of identification documents [22].

Third, the new version of the Directive for a high common level of cybersecurity across the Union (NIS Directive), will also have an impact on the regulatory framework of electronic identification providers. The NIS2 Directive has been presented at the end of 2020 [23] and introduces some modifications that will definitely have an impact on the provision of identification services [24]. More specifically, the scope of entities subjected to this Directive has included trust services, as well as the providers of electronic communications as Operators of Essential Services (OES). In addition, banking institutions, public administrations and health care providers, that usually count on in-house identification systems are included in this qualification and therefore are subject to the obligations contained in thereof [25]. Consequently, there exist high chances that a legal entity that provides electronic identification services (as in-house service or identity as a service) will be subject to these obligations. Nevertheless, as noted along this paper, identification services can be provided by a wide variety of legal entities. Consequently, besides the regulations cited, depending on the entity that provides the electronic identification service, specific regulations applying to them must be consulted.

6. CONCLUSIONS

Electronic identification represents one of the pillars in the realization of the Digital Single Market. However, as we have explained along this article, the regulatory framework of digital identities across the EU is fragmented depending on the scope of the authentication process, as well as the entity providing the service. Indeed, as we have noted, the eIDAS Regulation represents par excellence the main regulatory instrument for digital identities across the EU, but its mandatory scope of application is limited to the access to public services. Furthermore, private entities will not be covered by this regulation unless they constitute as a trust service and issue electronic certificates for signing, besides identification purposes. In addition, the current eIDAS

Regulation suffers from inconsistencies with other EU regulations and is not adapted to technological developments [26].

For these reasons, the eIDAS Regulation is currently under review and a new draft will probably become public in the following months. In this sense, different possibilities are being studied. The extension of the scope of application of the eIDAS Regulation to private operators seems an urgent need to encourage digital transactions across Member States. However, this will require a new regulation that allows this possibility. Different scenarios could be envisaged such as the State to acquire the right to use electronic identification means as a type of potential service contract, the possibility of an innovative partnership, or the recognition by the State of specific private providers who meet certain conditions for this. The definition of a new trust service for identification and authentication purposes could be another possibility [26].

What is clear is that the eIDAS Regulation, despite having come into force just a few years ago, due to the enormous increase of electronic activities (e-commerce, remote work and others) is too limited to offer an answer to current needs. In addition, the exclusion of those private providers that do not qualify as trust service, place these entities under the regulation of the e-Commerce Directive that, for the wide number of services it is thought for, does not include any specific regulation concerning identification services and the developments of this Directive (case law, academic articles…) have taken place in other areas such as the removal of illegal content and the right to freedom of speech. The fragmentation of regulations also has consequences concerning liability rules. In this sense, an electronic identification service provided by a trust service will be covered by the tripartite liability envisaged by eIDAS, while in the opposite case, it will rely on the national law where the ISS is established.

In conclusion, the eIDAS Regulation is probably the key piece in the enhancement of the regulatory framework of digital identity across the EU. The new version of the eIDAS Regulation will hopefully widen its scope of application to include private entities as well as it will achieve a better consistency with other regulations, but also with emerging technological developments, in particular the case of Self-Sovereign Identity. Consequently, an extended eIDAS Regulation, conjointly applied with context-specific regulations will probably represent a crucial step and will be decisive in the success of the Digital Single Market. Definitely, all trustworthy relationships begin with “meeting” the other party involved.

BIBLIOGRAPHY

[1] PREUKSCHAT, A. & REED, D. (2021) Why the Internet is missing an identity layer—and why SSI can finally provide one. At *Decentralized digital identity and verifiable credentials*. Manning Publications Co., pp.1-3.

[2] European Commission. Shaping the Digital Single Market. European Commission website. [Date of access: 1st May 2021]. Available at the following address: https://ec.europa.eu/digital-single-market/en/shaping-digital-single-market

[3] DE STREEL, A., & HUSOVEC, M. (2020) The e-commerce Directive as the cornerstone of the Internal Market. *IMCO Committee Study*, May, pp.45 & 46. [Date of access: 1st May 2021] Available at the following address: https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2020)648797

[4] 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. *Official Journal of the European Union* (28th August 2014), L 257/73-257/114. Available at the following address: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=ES

[5] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). *Official Journal of the European Union* L 178/1 (8th June 2000). Available at the following address: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

[6] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC. *Official Journal of the European Union* (20th May 2015) L 141/73. Available at the following address: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN

[7] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. *Official Journal of the European Union* (23rd December 2015), L 337/35. Available at the following address: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN

[8] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. Brussels, 16.12.2020 COM (2020) 823 final 2020/0359 (COD). Available at the following address: Brussels,16.12.2020 COM (2020) 823 final 2020/0359 (COD)

[9] ANDRAŠKO, J. (2017) Mutual recognition of electronic identification means under the eIDAS Regulation and its application issues. *Ad Alta: Journal of Interdisciplinary Research*, *7*(2), 9-13 [Date of access: 1st April 2021] Available at the following address: https://www.researchgate.net/publication/339973932_MUTUAL_RECOGNITION_OF_ELECTRONIC_IDENTIFICATION_MEANS_UNDER_THE_EIDAS_REGULATION_AND_ITS_APPLICATION_ISSUES/link/5e708f00458515eb5aba8e1e/download

[10] CUIJPERS, C & SCHROERS, J. (2014) eIDAS as guideline for the development of a pan European eID framework in FutureID, 23-38 [Date of access: 1st April 2021] Available at the following address: https://core.ac.uk/download/pdf/34614563.pdf

[11] ENGELBERTZ, N., ERINOLA, N., HERRING, D., SOMOROVSKY, J., MLADENOV, V., & SCHWENK, J. (2018) Security analysis of eIDAS–the cross-country authentication scheme in Europe. In *12th {USENIX} Workshop on Offensive Technologies ({WOOT} 18)* [Date of access: 1st April 2021] Available at the following address: https://ris.uni-paderborn.de/publication/15914

[12] 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. *Official Journal of the European Union* (9th September 2015) L 235/7 (. Available at the following address: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1502&from=GA

[13] HANSEN, M., OBERSTELLER, H., RANNENBERG, K., & VESELI, F. (2015) Establishment and prospects of Privacy-ABCs. *Attribute-based Credentials for Trust*, 345-360. Springer, Cham.

[14] 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. *Official Journal of the European Union* (8th September 2015), L 235/1. Available at the following address: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1501&from=EN

[15] Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) *Official Journal of the European Union* (4th May 2016) L119/1. Available at the following address: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[16] TSAKALAKIS, N., STALLA-BOURDILLON, S. & O'HARA, K. (2016) What's in a name: the conflicting views of pseudonymisation under eidas and the general data protection regulation. *Hühnlein, D., Roßnagel, H., Schunck, C. H. & Talamo, M. (Hrsg.), Bonn: Gesellschaft für Informatik e.V.*. (S. 167-174). [Date of access: 3rd May 2021] Available at the following address: https://dl.gi.de/handle/20.500.12116/598;jsessionid=C79C907B5E99FA15B767E169D9FD5ECF

[17] TSAKALAKIS,N. & STALLA-BOURDILLON, S. (2018) Documentation of the legal foundations of trust and trustworthiness: Deliverable D2.8. *FutureTrust* 160pp.). [Date of access: 3rd May 2021] Available at the following address: https://eprints.soton.ac.uk/431138/

[18] Directive 98/34 of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations. *Official Journal of the European Union* (22nd June 1998). L 204/37. Available at the following address: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31998L0034&from=EN

[19] European Commission (2011) A coherent framework for building trust in the Digital Single Market for e- commerce and online services Communication from the Commission of 11 January 2012, COM, 942, p.5. Available at the following address: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0942&from=en

[20] BERTOLINI, A., EPISCOPO, F, & CHERCIU, N. (2021) Liability in online platforms. *European Parliamentary Research Service Scientific Foresight Unit (STO*A) [Date of Access: 4th May 2021]. Available at the following address: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU(2021)656318_EN.pdf

[21] SCHULTZ, M. (2015) The responsible web: How tort law can save the internet. *Journal of European Tort Law*, *5*(2), 182-204. [Date of access 4th April 2021]

[22] Thales website. Know your customer in banking. [Date of access 4th April 2021]. Available at the following address: https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/issuance/id-verification/know-your-customer#:~:text=KYC%20means%20Know%20Your%20Customer,who%20they%20claim%20to%20be

[23] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. Brussels, 16.12.2020 COM (2020) 823 final 2020/0359 (COD). Available at the following address: Brussels, 16.12.2020 COM (2020) 823 final 2020/0359 (COD)

[24] NEGREIRO, M. (2021) The NIS2 Directive A high common level of cybersecurity in the EU. European Parliamentary Research Service*. BRIEFING EU Legislation in Progress*. [Date of access: 4th April 2021] Available at the following address: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

[25] Annexes to the Proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148. Brussels, 16.12.2020 COM (2020) 823 final Annexes 1 to 3. Available at the following address: file:///Users/cris/Downloads/com2021_823_en_annexe_proposition_cp_part1_v7_-_copy_2EBD3F2F-FD36-A918-EF55CCD20D8B99F1_72172.pd

[26] PONTE, N., TIMÓN LÓPEZ, C., ET AL. (2020) D5.3 OLYMPUS support for extended eID models. *OLYMPUS research project* [Date of access: 5th May 2021]. Available at the following address: https://olympus-project.eu/wp-content/uploads/2020/10/Olympus_pu_d5_3_v1_0.pdf