idertec.
Innovación
Derecho y Tecnología

Contribution to the "EU digital ID scheme for online transactions across Europe" initiative consultation

Authors: Dr. Ignacio Alamillo-Domingo & Dr. Julian Valero-Torrijos, iDerTec Research Group, Universidad de Murcia (Spain).

Murcia, September 3rd 2020

iDerTec is a legal research group working in different initiatives, including electronic identity, notably H2020 ARIES and OLYMPUS projects. We welcome the proposed initiative and want to make the following general remarks.

First. The legal institutionalization of the accreditation of electronic agency responds to a functionalist approach, with at least two different legal regimes; we must distinguish between the wider category of trust services and the narrower one of electronic identification schemes.

This distinction is not justified in objective or technical criteria, but it is rather of a political nature, in the sense that trust services have been privatized, while a majority of Member States do not seem to be, at least for the moment, willing to admit this possibility with respect to electronic identification schemes.

In many cases, these identification services are considered public services, frequently in a strict sense and with activity reservation to public authorities (e.g. law enforcement agencies), as in the case of official electronic identity documents.

Thus, the eIDAS Regulation is a fundamental but incomplete basis of legal experience in relation to electronic agency institutions, especially from the perspective of the private sector. Although at the national level, however, the Member States may subsequently shape these institutions, if they deem it necessary or appropriate, establishing the suitable legal requirements or effects, this option may not facilitate the Digital Single Market.

This situation could be corrected by regulating electronic identification as a trust service. The revised version of the eIDAS Regulation should create a legal rule allowing natural and legal persons to use a qualified electronic signature or seal certificate where the law imposes the requirement to identify their selves.

Second. Although the electronic signature fully responds to the principle of functional equivalence, the eIDAS Regulation only establishes legal effects with respect to qualified electronic signatures, leaving it to the Member States to stipulate the legal effects of the remaining electronic signatures.

This approach is to be criticized as affects negatively the possibility of using non-qualified electronic signatures based on the autonomy of the will of the parties, as frequently occurs (for example, in the case of authorization of payment order pursuant to PSD2 , in which strong customer authentication is required, but not a specific type of electronic signature).

Therefore, it would be convenient to modify Article 25 of the eIDAS Regulation, in the sense of incorporating a general functional equivalence rule of the electronic signature, in line with article 6 of the 2001 UNCITRAL Model Law of Electronic Signature (https: // uncitral .un.org / en / texts / ecommerce / modellaw / electronic_signatures).

Furthermore, the status of the qualified electronic signature should be aligned with article 7 of the Model Law, in the sense that a qualified electronic signature is treated as a method to consider an electronic signature as reliable.

This approach would ensure that all electronic signatures may be equivalent to handwritten signatures (something not granted by the non-discrimination principle currently provided for by Article 25 of the eIDAS Regulation), while maintaining the legal certainty and incentive associated to qualified signatures. The same considerations apply to electronic seals, while it is true that electronic seals do not have any functional equivalence to a "traditional" institution, such as a physical seal.

Third. In our view, the legal regime for cross-border authentication in the eIDAS Regulation is excessively limited, since it only refers to systems the Member State intends to extend their use to access to public services provided by entities in other Member States.

For the proper development of the Digital Single Market, Member States should be required to ensure that the means of electronic identification which they notify can also be used for transactions between private parties.

The latter statement must be understood, however, without prejudice to the fact that the electronic certificate of the electronic signature of a natural person and the electronic seal of a legal person also constitutes an electronic identification institution, since its legal function is precisely to confirm identity. Normally we will find the authorization of the use of certificates for this purpose in the sectoral regulations, as can be seen, for example, in the Spanish legislation regulating administrative procedure. It is essential to evolve this system so that it could be applied to identification systems for accessing private services.

Fourth. The eIDAS Regulation has not exhausted, by express decision of the legislator, the list of institutions used for the accreditation of electronic agency, allowing the Member States to maintain or create other trust services.

This option must be valued positively, since experience shows that the Member States are the laboratories where these institutions are created, which are subsequently harmonized and later incorporated into the *acquis communautaire*. This was initially the case initially with the electronic signature, and it has happened again with electronic seals, electronic time stamps, or registered electronic delivery.

But this is a relevant problem for a Digital Single Market as it entails a significant level of heterogeneity and fragmentation that can hinder its achievement. Various legislations have already regulated the electronic archive as an institution based on the corresponding trust service, to which the legal effect of presuming the correct conservation is associated, even in the case of the substitute digitization of original documents on paper.

It would be convenient for these institutions to join the harmonized regulation at the Union level. As long as this does not happen, important differences remain in the management of documents in support of business processes that may affect the competitiveness of some companies seeking to operate throughout the territory of the Union.

Fifth. One of the main constraints of the eIDAS Regulation is that the intervention of a service provider in relation to sources of evidence that receive reinforced legal effects is required, since only in these cases is it possible to create a source of qualified electronic evidence.

This regulatory option excludes from the qualification mechanism several technological possibilities, such as distributed ledger technologies and, more specifically, blockchain technologies. In this case, a centralized provider does not intervene, but rather a collection of infrastructure nodes that replicate the information, so that it cannot be arbitrarily eliminated by one or both parties to the transaction.

The qualification is, in some situations, excessively specific, as in the case of the qualified electronic signature and the qualified electronic seal, showing a strong dependence on public key technology, which again leads to the intervention of a provider services. This option negatively affects the requirements of technological neutrality, which is limited to very few aspects of the system, tremendously constrained by the standards of the public key infrastructure.

Indeed, the qualification should be more abstract, so that any electronic signatures, electronic seals or other institutions of accreditation of electronic performance that are not based on the use of cryptographic keys (such as the handwritten signature captured electronically), can be qualified. This is a technology that has revealed the logical limitations of the eIDAS Regulation, which does not allow a handwritten signature captured electronically to be considered as a qualified electronic signature. Given that the legal effect of a qualified electronic signature is to be equivalent to the handwritten signature, It is remarkable that a handwritten signature captured electronically does not acquire the legal effect of being equivalent to itself, a real paradox that, in our opinion, has put the system in evidence.

To meet the standards of technological neutrality, any electronic source of evidence should be able to be qualified. This is not possible with the current regulatory model as this qualification only serves to define those technologies that, due to their technical conditions and prior verification by the Administration, can obtain the corresponding reinforced legal effect.

This is particularly relevant for emerging electronic identity and trust services technologies, such as Distributed Ledger Technologies (e.g. blockchains) supporting the so-called Self-Sovereign Identities, currently being explored by the European Commission in the EBSI project. A full analysis of the interplay between these emerging technologies and the eIDAS Regulation is available at https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/document/ssi-eidas-legal-report

Sixth. Taking into consideration the aforementioned remarks, and the analysis of the SSI eIDAS Legal report, we think the most valuable scenario is option 2, as it leverages the strong electronic identification capabilities of Member States, while creating wider markets for private providers.

We will be pleased to provide you with any clarification you may require with regard to this contribution. You can contact us at ignacio.alamillod@um.es for this purpose.

Yours sincerely