WAVESTONE

eIDAS
HEADING TOWARDS A DIGITALLY TRUSTWORTHY EUROPE

AUTHORS

FLORIAN FEUILLARD
florian.feuillard@wavestone.com

MATTHIEU GUILLAUME
matthieu.guillaume@wavestone.com

SUPPORT FROM LUXEMBOURG

DEBORA DI GIACOMO
debora.digiacomo@wavestone.com

ROSITSA BONEVA
rositsa.boneva@wavestone.com

Legislation concerning eIDAS (Electronic IDentification And trust Services) came into effect on July 1st, 2016. The aim of the new legislation is to "build trust in the on-line environment" by delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions between citizens, businesses and public authorities.

eIDAS introduces numerous changes vis-à-vis the 1999 EU directive concerning the regulatory framework for electronic identification and trust services. This climate of trust covers secure electronic identification and authentication as well as other services such as time stamps and electronic registered delivery services. The implementation of this framework will make it possible to carry out administrative procedures in all EU Member States and require their mutual acknowledgement.

The text sheds light on one of the major problems encountered today: "In most cases, citizens in one Member State cannot use their electronic identification for authentication purposes in another Member State because the national electronic identification schemes in their country of origin are not recognized in other Member States". This issue of non-recognition stems from the different interpretations and technical implementation of the directive by each Member State which cause problems of interoperability and divergences in the controls carried out. Concerning "trust services" such as time stamps and electronic seals, divergence stems from the lack of a coherent legal framework at the European level, which is a real obstacle in building cross-border digital trust.

A COMMON FRAMEWORK

While this regulation covers most of the dispositions contained in the 1999 directive, it proposes several modifications and some new dispositions designed to strengthen European recognition of trust services. The present regulation notably defines:

/ **The conditions governing Member State recognition of the means of electronic identification of citizens and legal entities** (businesses and local authorities) attached to the notified electronic identification scheme of another Member State;

/ **The applicable rules for trust services**, particularly electronic transactions;

/ **The legislative framework for electronic signature, seal, time stamp**, document, registered delivery and Internet-site authentication certificate services.

Contrary to Directive 1999/93EC, the text of **eIDAS cannot be adapted at the national level but applies to all Member States**.

MOVING TOWARDS EUROPEAN HARMONIZATION: THE KEY POINTS

The current regulation introduces a certain number of new notions, notably:

/ **The acceptance of electronic documents as legal proof**;

/ **The creation of an EU trust mark for a more transparent market;**

/ A framework for the methods used to validate qualified electronic signatures by trusted services providers;

/ A qualified preservation service for qualified electronic signatures to guarantee the trustworthiness of signatures and, hence, their validity over time;

/ At the European level, the date recognition, digital data integrity and thus the legal validity of electronic time stamps issued in one Member State shall be recognized in all Member States of the EU;

/ The obligation of the Member States to maintain, and give consumers access to, lists of trusted services and qualified service providers bearing the EU trust mark;

/ Greater flexibility concerning electronic signatures; recognition of the remote creation of electronic signatures by trusted service providers on behalf of the signatory, to facilitate mobility usages.

Another novelty worth noting is the introduction of a **new legal principle: the electronic signature of legal entities**. Companies and public sector bodies may now use electronic seals to electronically sign documents as a means of certifying their origin. In real terms, a French judge cannot refuse an electronic seal or signature endorsed by an Italian with a German solution. Also worthy of note is the **introduction of the notion that qualified signatures can be used to authenticate servers**; a measure that will notably pave the way for the development of new offers (SaaS), which is clearly the objective of this new regulation.

As such, eIDAS defines **3 levels for grading consumer electronic signatures** (summarized in the table below), **compared with 2 levels previously** for companies.

3 levels for grading consumer electronic signatures

SIGNATURE VALUES

		Simple signature	Advanced signature		Qualified signature	
Signature level		Simple	Advanced LCP ETSI 319 411 LCP level	Advanced QCP ETSI 319 411 QCP level	Qualified QCP + QCSD ETSI 319 411 QCP level + QCSD	
Certificate level		Simple certificate	LCP certificate	Qualified software support certificate	Qualified material support certificate	
					Smart card	Qualified server
Enlisting requirement		None	Remotely identity verification	Physical identity verification	Identity verified physically or remotely, or through proof of a qualified electronic signature delivered in accordance with (a) or (b)	
Signature device requirement		None	None	None	Qualified signature device	
Advantage		Integrity	Integrity and non-repudiation	Integrity and non-repudiation	Integrity and non-repudiation	

LCP : Lightweight Certificate Policy   QCP : Qualified Certificate Policy   QCSD : Qualified Signature Creation Device   ⬚ : In process

IN CONCRETE TERMS, WHAT WILL THIS CHANGE?

One notable point concerns compliance with a view to obtaining eIDAS qualification for Trusted Services Providers (TSP). Service providers wishing to be included in the qualified TSP list (which should be published regularly) and thus be recognized by all Member States must respect all security requirements (technical and organizational measures, etc.) and notably ensure assurance of the verification of the connection between the identity of the bearer and the certificate delivered. To this end, these services providers must comply with standards concerning the security measures to be implemented: risk analysis, termination of service plans, one-on-one issuing processes, security violation notifications, controls, responsibilities, etc. While these measures are not new in themselves, the regulation defines specific requirements expected of each level and introduces some new notions (for example: "the TSP shall state in its practices the provisions made for termination of service". The technical interoperability of systems requires a review of the national security frameworks, such as the Référentiel Général de Sécurité (RGS) in France, and the cooperation between other member States.

In this regard, the text of the present regulation highlights the need for cooperation:

"Cooperation by Member States should facilitate the technical interoperability of the notified electronic identification schemes with a view to fostering a high level of trust and security appropriate to the degree of risk. The exchange of information and the sharing of best practices between Member States with a view to their mutual recognition should help such cooperation."

However, qualification is still a voluntary process and an EU trust mark will be created to identify qualified TSPs. To obtain EU trust-mark qualification, trusted services providers must carry out a conformity assessment attesting that the measures defined in the standards underpinning the regulation are respected. In the coming months, trusted services providers seeking eIDAS qualification are expected to launch global compliance projects including the updating of documentation (PC, DPC, PH, DPH, CGU, etc.), as well as a review of their Public Key Infrastructure (PKI) architecture and certificate templates, etc. Note that services providers qualified within the framework of the 1999 directive will remain so under the present regulation until such time their qualification comes up for renewal but must . In all cases, however, they must submit a conformity assessment report before July 1st, 2017 at the latest to have their qualification renewed. This grace period should not be excessive. For example, in France there is at present only one operator qualification body which was recently officially accredited, a factor which could delay the launch of compliance projects.

EUROPE LOOKING TO ADOPT THESE TECHNOLOGIES IN ALL MEMBER STATES

European authorities and in particular the Directorate-General for Informatics (DIGIT), which is in charge of the building blocks such as eInvoicing, eDelivery, eSignature and eID, wish to carry out a detailed assessment of the key market players in each country.

To this end, they have called on Wavestone Luxembourg to conduct a study and surveying EU Member States, to identify key market players and their particular needs. The solutions needed to promote the adoption of these building blocks have been analysed and discussed already with all relevant stakeholders. The results of this study are due to come in shortly!

eIDAS qualification for services and provider

Security requirements to be respected → Certification process → Regulation compliance → Trusted service or services provider → Significant legal impact and presumption of reliability

COMPLIANCE REVIEW ONCE EVERY 24 MONTHS

FEEDBACK ON A COMPLIANCE PROJECT

The High Council of French Notariat (CSN) is one of the first players in France to undertake measures to become compliant with the new eIDAS regulation. In its capacity as a Trusted Services Provider, the CSN is a certification body notably authorized to issue eSignatures for notary certification of authentic acts.

Didier Lefèvre (ISD, CSN) and Yannick Thomassier (DSSI, Real.Not, PKI operator of the CSN) give their feedback on this regulation and the compliance project below.

Wavestone: What do you think about this new regulation?

Yannick Thomassier: With regard to Directive 1999/93/EC, the forerunner of the present regulation, an audit carried out ten years after its implementation revealed several limitations. In its communication dated August 26th, 2010, entitled "A Digital Agenda for Europe", the Commission to the EU Parliament clearly stated that, "the Commission had identified the fragmentation of the digital market, the lack of interoperability and the rise in cybercrime as the major obstacles to the virtuous cycle of the digital economy." The purpose of the present European regulation is to remedy several shortcomings in Directive 1999/93/EC by imposing the same legal base for all Member States. However, the regulation does not yet contain the implementing acts necessary to allow a unique technical transposition within Europe. Accordingly, each Member State must decide on how it will apply and therefore fix its own regulations, which is, in fact, the implementation scheme that is currently in place under Directive 1999/93/EC. In this respect, the regulation has not completely fulfilled its objectives.

Didier Lefèvre: Nevertheless, one of the positive elements of eIDAS is that it is designed to establish a framework for the entire trust chain, which is an improvement on the 1999/93/EC Directive whose scope was limited to eSignatures.

Why have you launched this eIDAS compliance program?

YT: We must be in compliance insofar as the notary signature is a qualified signature.

What opportunities does this regulation offer you?

YT: Cloud-based eSignature development is very interesting. Although the use of smart cards for signing notary acts is a first step towards dematerialization, it is still very limited. Today however, IT practices are not limited to computers but include smart-phones, tablets, etc. Notaries are becoming increasingly more mobile and must have access to signage devices and applications so that they can set themselves apart from their rivals and meet their clients' needs. The eIDAS regulation is a tremendous opportunity for the profession to be able to offer other means of providing qualified signatures.

What are the major difficulties that you have encountered?

YT: Concerning the agenda, we have opted for a maximum anticipation approach regarding compliance, since change is a fastidious and very long drawn out process which involves consulting and compiling numerous documents, defining new processes, sometimes implementing new products and coordinating all of these in an agenda that respects regulation deadlines. This is particularly relevant for us in the legal profession, since we must be ready at all times.

What advices would you give to those looking to launch a similar type of compliance project?

YT: Two points in particular are worthy of caution. Firstly, the need for agility regarding the new regulation since this is likely to change. The body of the French technical document, for example, has not yet been finalized. Secondly, the process should be set in motion as quickly as possible to be able to prepare the conformity assessment and certification audit under the best conditions.

How do you see the future of the European regulation?

YT: The technical implementation of the eIDAS regulation is subject to the interpretation of the national control bodies, the outcome of which could have an impact on its introduction. This may, therefore, lead to a second phase in order to clarify this, and enable the homogeneous implementation of the regulation throughout Europe.

Then what?

YT: We hope to obtain our eIDAS qualification within the time-frame: Next stage scheduled for July 1st, 2017!

WAVESTONE

www.wavestone.com