White Paper

eIDAS in a Nutshell

By Utimaco

Background

In the past, only handwritten signatures had legal validity. With the rise of global digital markets, it became necessary to use electronic signatures to transact online. The 1999 Electronic Signatures Directive established the European legal framework for electronic signatures and certification services. Although there was no dispute over the directive in its 16-year history, it was hardly a success. It did not achieve its primary goal — to ensure widespread use of electronic signatures across EU borders.

There are **three critical reasons for electronic signature deficiencies in the old directive:**

1. *Very few EU Member States have any laws requiring specific forms of eSignatures for commercial contracts.*
2. Many corporate decision-makers did not understand the legal validity of the earlier directive's advanced electronic signatures. Many people mistakenly assumed that any legal value would require a digital certificate for an electronic signature. The preceding Electronic Signatures Directive stated the exact opposite — each court can choose to recognize any eSignature as legally binding; however, all Member States ' courts have no choice but to accept it when an electronic signature is qualified.
3. The wide variations in electronic signature or certification legislation produced in one Member State risked compliance and interoperability in the other Member States.

Therefore, the EU Commission concluded that the lack of harmonization between the Member States was a significant obstacle to the internal market.

Legal Validity and Effect of the eIDAS Regulation

Regulation eIDAS is a significant milestone for the EU Single Digital Market, as it enables Trust service providers of all kinds to offer cross-border certificates to support eSignatures. For example, electronic signatures can be used in public procurement to certify that the company that sent an offer is indeed the company it claims to be. In many cases, an electronic signature is also used to protect the content of what was signed (encryption).

What are the Trust Services regulated by eIDAS?

Electronic Signatures

According to eIDAS, an electronic signature is defined as any data in electronic form attached to or logically associated with other electronic data, used by the signatory. Technically, natural persons use them to ensure the authenticity, integrity, and non-repudiation of electronic documents.

Advanced Electronic Signatures

Ades Baseline Profiles, developed by the European Telecommunications Standards Institute (ETSI), sets technical standards for advanced electronic signatures. This signature must find a signatory uniquely; binding specific data attributes to an advanced digital certificate. The signatory must have sole signature data control. Users keep authority over the private keys used to create advanced signatures. The signature must detect any changes made to the certificate or signed message data. Every time the data changes, the signatory must restart the signing process.

Primarily, advanced electronic signatures exist in the following three file types:

Electronic signatures exist in the following three file types:

XML Advanced Electronic Signatures(XAdES) — a set of extensions to XML-DSig recommendation making it suitable for Advanced Electronic Signatures.

PDF Advanced Electronic Signatures(PAdES) — a set of restrictions and extensions to PDF and ISO 32000-1 for Advanced Electronic Signatures.

CMS Advanced Electronic Signatures(CAdES) — a set of extensions to Cryptographic Message Syntax signed data making it suitable for advanced electronic signatures.

What are the Trust Services regulated by eIDAS?

In addition to the three file types, there are container structures:

> **Associated Signature Containers (ASiC)** — Container structures bind one or more signed objects to a single digital container with an advanced electronic signature or tokens.

Qualified Electronic Signatures

A Qualified Electronic Signature (QES) is the digital equivalent of a natural person's handwritten signature in terms of legal assurance. QES must meet all the requirements of an "advanced" e-signature, with added requirements being applied to the signature creation device by which it was created.

The legal backbone of such qualified electronic signatures cannot be underestimated as it gives legal assertion to the users, even at court. This gives the European area of jurisdiction a head-margin against jurisdiction in other areas, i.e. in the USA. The DocuSign case of 2016 caused an éclat among experts. An American lawyer used electronic signatures to sign legal documents like bankruptcy petitions. Judge Bardwill of the U.S. Bankruptcy court ruled that an electronically signed legal document can only be used when a handwritten-signed copy is also available. The benefits in terms of procedural effectiveness and simplification of QES are striking.

But that is not all. Electronically generated transactions and legal agreement reach a legally and technically backed level of non-repudiation of origin and of emission. The advantage of the technical protection makes it less vulnerable to fraud than a wet signature. Whereas a handwritten signature could be faked relatively easy, the technical conception of the QES makes fraud virtually impossible.

What are the Trust Services regulated by eIDAS?

Digital Certificates

A key goal of eIDAS is to enable Trust Service Providers of all kinds to offer cross-border certificates to support e-signatures. All Electronic signature depends strongly on digital certificates. Creating an electronic certificate involves agreement on a set of attributes included in the signature certificate; the standard way to secure electronic signatures, e-documents, and certificate metadata. Electronic signatures based on qualified certificates are the necessary part for cross-border interoperability.

Other Trust Services

Regulation eIDAS covers multiple elements of electronic services to help the creation, issuance, revocation, preservation, or delivery of electronic services of the following trust services:

Electronic sealing is like that of electronic signing, with the difference that a person who creates a seal is a legal entity. The eIDAS Regulation provides "should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity."

- Intended for legal persons to ensure data and documents origin and integrity.
- Reduces costs by streamlining critical business processes
- Trust in the origin of a document

Further, the regulation allows an authorized legal person representative to use his or her qualified electronic signature instead of the respective electronic seal. **For example:** An electronic seal can be used in public procurement to certify that the company that sent an offer is indeed the company it claims to be. In many cases, an electronic signature is also used to protect the content of what was signed (encryption)

What are the Trust Services regulated by eIDAS?

Other Trust Services

Timestamping is an important trust service throughout the life cycle of e-Document. Companies use this trusted service to record, at a particular date, the validity or lifecycle phase of an electronic document, signature, or accompanying certificate

- Enhanced document tracking
- Greater accountability
- Ensures the correctness of the time linked to data and documents

Time stamping a long-term electronic signature is also used to preserve e-documents in the for an extended time period. Re-time stamping an electronic signature confirms a document using an updated electronic signature, thus protecting the signed data from outdated algorithms' vulnerabilities.

Electronic registered delivery service is a service that enables data to be transmitted between third parties and offers evidence of the processing of transmitted data, including proof of sending and receiving information, and protects the information against the danger of loss, robbery, or any unauthorized alteration.

- Reduced time and costs in document exchange
- Increased efficiency and trust enhanced document tracking

Utimaco HSM Industry Examples

To be recognized as signature generation tools under eIDAS, HSMs have to fulfill strict requirements and must undergo a conformity test. In the following we list examples of a successful implementation.

Exceet

Exceet is a European expert for secure IT solutions, focusing on securing electronic business processes with the aid of qualified electronic signatures. Exceet Secure Solutions also extends to HSMs, PKI solutions, as well as products and services for qualified time stamps, including Trust Centre operations

Deploying Utimaco'sHSMs satisfies the high-quality demands,which Exceet relies on to develop and expand eIDAS-compliant solutions.

"The extensive expertise of Exceet in using security modules and the company's long-standing experience in the signature market lets us develop joint use cases for HSMS – across Europe," says Malte Pollmann, CEO of Utimaco.

Halcom-CA

Halcion, a digital banking solution provider, based in Slovenia, is implementing Utimaco's CryptoServer CP5 after extensive and successful testing. Head of Halcom-CA, Luka Ribičič, had this to say about the HSM solution:

"To be able to offer our clients eIDAS-compliant solutions, cooperating with a trustworthy HSM provider was crucial. The CryptoServer CP5 simulator, as well as the affordable price point, as key factors in our decision for Utimaco."

Utimaco HSM Industry Examples

Ascertia

Another notable example is the development of signature activation modules for remote signing solutions by Utimaco partners such as Ascertia. Ascertia implemented these modules i.e. for banking applications with Bank-Verlag. This service will enable end customers to generate electronic signatures remotely for use in financial transactions.

It will also speed up and ease the processes of signing contracts, opening accounts, and buying banking products or services. HSM offers directly the kind of force multiplier that FinTech and even banks of all sizes would like to leverage.

About

About HSMs

HSMs are essential in protecting, managing and securing sensitive cryptographic assets, such as digital encryption keys, custom IP and asset access. Utimaco is now driving a new era as its HSMs are facilitating digital transformation in many key areas including, but not limited to, banking and payments, encryption and blockchain. Utimaco's goal is to protect sensitive data assets in the eventual wake of quantum computing.

About Utimaco

Utimaco is a leading manufacturer of Hardware Security Modules (HSMs) that provide the Root of Trust to many industries, from financial services and payment to the automotive industry, cloud services and the public sector. We keep cryptographic keys and digital identities safe protecting your critical digital infrastructures and high value data assets. Founded in 1983, today Utimaco HSMs are deployed across more than 80 countries in more than 1,000 installations. Utimaco employs a total of 200 people, with sales offices in Germany, the US, the UK and Singapore. For more information, visit https://hsm.utimaco.com/.