DATASHEET

Using GlobalSign Digital Signature Solutions for eIDAS Compliance

What is eIDAS?

eIDAS is a European Union (EU) regulation focused on enhancing trust in electronic transactions between citizens, businesses and public authorities cross-borders. A major component of the regulation was the creation of a common framework for secure electronic signatures, including standardized assurance levels, to facilitate interoperability and acceptance across EU and European Economic Area (EEA) member states.

eIDAS Electronic Signature Definitions and Classes

Under eIDAS, an electronic signature cannot be denied legal effect and admissibility just because it is electronic. However, the regulation acknowledges that, depending on the technology and validation behind the signature, some types of signatures are inherently more trustworthy than others and withstand higher legal scrutiny. That is, they are more reliably linked to the person signing the document, can protect the integrity of the document and, at the highest level, can carry the same legal effect as a handwritten signature.

- Electronic signatures - the most basic and broadest electronic signature classification, eIDAS defines these 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.”

- Advanced electronic signatures (AdES) – must meet additional requirements specifically set out by the regulation, including the ability to uniquely link to the signer, validate the signer’s identity, and detect subsequent changes to the signed data. PKI-based digital signatures, those applied with a digital certificate, meet these requirements.

- Qualified electronic signatures (QES) – must meet the AdES requirements, but also must be created with a qualified certificate that itself has to be stored on a qualified signature creation device (QSCD). A QSCD is a purpose-built device that ensures:

  - The generated signature creation data is managed by a qualified trust service provider (QTSP).
  - Only the signatory has control over their private key.
  - The signature creation data is unique, confidential and protected from forgery.

  Qualified certificates can only be issued by an eIDAS-accredited, qualified trust service provider (QTSP). QES have the equivalent legal effect of a handwritten signature and must be recognized across borders (i.e., a QES based on a qualified certificate issued in one Member State must be recognized as a QES in all other member states).

GlobalSign offers a range of digital signing solutions and can support advanced and qualified electronic signatures.

Electronic Seals

Electronic seals are similar to electronic signatures, but instead of an individual person signing, it is an organization or other corporate body signing or “sealing” the document to ensure its origin and integrity. The same assurance levels and associated legal effects apply to seals, with PKI-based digital signatures generally meeting the requirements for advanced electronic seals and a qualified certificate from a qualified trust service provider required for qualified electronic seals.

GlobalSign supports advanced and qualified electronic seals.

GLOBALSIGN PRODUCTS

- QUALIFIED ELECTRONIC SIGNATURES AND SEALS
  GlobalSign is a qualified trust service provider and has undergone the appropriate eIDAS audits to be able to provide qualified certificates that can be used to create electronic signatures and qualified electronic seals

- ADVANCED ELECTRONIC SIGNATURES AND SEALS
  GlobalSign’s standard range of digital signature products and solutions meet the eIDAS-specified requirements for advanced electronic signatures

See next page for more details on these offerings.

GlobalSign®
GMO INTERNET GROUP

Qualified Certificates for Electronic Signatures and Seals from GlobalSign

As a qualified trust service provider (QTSP), GlobalSign is able to provide certificates for qualified electronic signatures and seals.

- Qualified electronic signatures have the same legal effect as handwritten signatures and must be recognized and accepted across all member states of the EU.
- Qualified electronic seals presume the integrity and origin of the document and must be recognized and accepted across all member states.

Qualified certificates for electronic signatures and seals are available to individuals and organizations through GlobalSign's token-based deployment. In keeping with eIDAS requirements, each signing identity, whether individual or corporate body, is verified and issued a qualified certificate stored on a qualified signature creation device (the token).

What It Means to Be a Qualified Trust Service Provider (QTSP)

Being a QTSP means GlobalSign's qualified trust services, in this case qualified electronic certificates used for qualified signatures and seals, ensure a higher level of security and legal assurance that is standardized and accepted across the EU. In order to become a QTSP, GlobalSign underwent a stringent conformity assessment to ensure all associated processes meet the requirements established by eIDAS.

Only QTSPs can provide qualified trust services and appear on the EU's Trust List. If an entity is not on that list, they are not entitled to provide qualified trust services.

Advanced Electronic Signatures and Seals from GlobalSign

GlobalSign's standard line of digital signature certificates and solutions meet the requirements for advanced electronic signatures and seals because they are:

- uniquely linked to the signatory,
- capable of identifying the signatory,
- created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control, and
- linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Advanced electronic signatures and seals are available to individuals and organizations through GlobalSign's standard range of deployment options, including:

- Token-based – individual or organization identity signing certificates are stored on cryptographic USB tokens.
- HSM-based – organization identity signing certificates are stored on on-premises or service provider (e.g., AWS hardware) security modules (HSMs). This option is for organizations who want to integrate with an internally developed or off-the-shelf automated document application and internal PKI expertise is required to configure the integration between the HSM and document workflow.
- Digital Signing Service (DSS) – completely cloud-based service integrates directly with document workflows and applications, eliminating the need for hardware altogether. Organizations can leverage existing integrations (e.g., Adobe Sign) or build digital signatures into their own custom workflows using the DSS REST API.

About GlobalSign

GlobalSign is the leading provider of trusted identity and security solutions enabling businesses, large enterprises, cloud service providers and IoT innovators around the world to secure online communications, manage millions of verified digital identities and automate authentication and encryption. Its high-scale Public Key Infrastructure (PKI) and identity solutions support the billions of services, devices, people and things comprising the Internet of Everything (IoE).

US: +1 877 775 4562
UK: +44 1622 766766
EU: +32 16 89 19 00

sales@globalsign.com
www.globalsign.com

GlobalSign® GMO INTERNET GROUP