FACT SHEET

eIDAS Regulation

Using Gemalto Smart Cards for eIDAS compliance

What is eIDAS?

eIDAS is the European Regulation aimed at creating a framework for cross-border electronic identification and transactions across EU member countries.

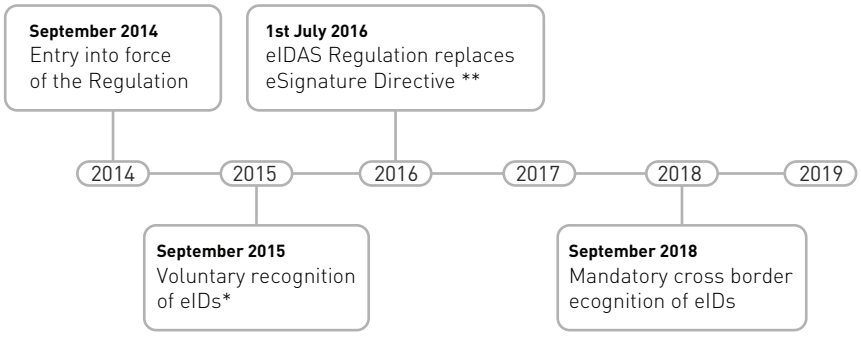
What are the primary mandated practices of eIDAS?

- **Interoperability of government issued ID:** EU Member States are required to mutually recognize each other's electronic identification (eID) systems when accessing online services.
- **Single digital market:** Electronic Trust Services (eTS), including electronic signatures, electronic seals, time stamps, electronic registered delivery service and website authentication, will work across borders and will have the same legal status as paper-based processes.

What are the goals of eIDAS?

- Open up access to public services and ensure secure online transactions across borders of EU member countries.
- Enable cross-border trust.
- Improve security and convenience when doing business online.
- Encourage digital transaction growth and dematerialization.

eIDAS Timeline



*Adoption of 6 implementing acts on:
MS cooperation
Interoperability framework
eID levels of assurance
Formats of advanced electronic signature & seals
Technical specifications of the national trusted lists
EU Trust mark

**Certificates issued to natural persons under the eSignature Directive remain valid until expiry and Certification Service Providers are allowed a 1 year time frame to submit a conformity assessment report and as consequence are considered as qualified Trust Service Providers under the new eIDAS regulation.

eIDAS and Electronic Signature

eIDAS recognizes electronic signatures as legally binding and identifies different levels of electronic signature.

- **Electronic Signatures—**basic signatures in electronic form. With eIDAS, eSignatures are recognized legally and can't be denied legal acceptance because they are digital.
- **Advanced Electronic Signatures (AdES)—**require a higher level of security typically met with certificate-based digital IDs. AdES must be uniquely linked to the signatory, can authenticate the signer and the document, and enable the verification of the integrity of the signed agreement.
- **Qualified Electronic Signatures (QES)—**also must be uniquely linked to the signatory, but are further required to be based on qualified certificates. Qualified certificates can only be issued by a certificate authority (CA) accredited and supervised by authorities designated by EU Member States. Qualified certificates must also be stored on a qualified signature creation device (QSCD), such as a USB token, smart card or a cloud-based hardware security module (HSM). In order to provide qualified eSignature services, a trust service provider must be granted qualified status

How to Prove Digital Signature Compliance with eIDAS

Common Criteria is an international set of guidelines and specifications for evaluating information security products, specifically to ensure they meet an agreed-upon security standard for government deployments. Common Criteria (CC) certification is a pre-requisite for qualified digital signatures under the eIDAS Regulation.

Gemalto offers several products that provide state-of-the-art security and are fully compliant with eIDAS regulations.

- IDPrime MD 840, contact interface smart card
- IDPrime MD 3840, dual interface (contact and contactless with NFC) smart card
- SafeNet eToken 5110, USB Token

These products are all CC EAL5+ / PP QSCD certified, based on the Protection Profiles EN 419211 part 1 to 6, as mandated by eIDAS Regulation.

Becoming a Qualified Trust Service Provider

Once a TSP can show their trust service is compliant using Gemalto smart cards, the TSP can apply to be a Qualified Trust Service Provider (QTSP). There are many benefits of becoming a QTSP in the wake of eIDAS including:

- Trust services provided by QTSP have a **higher legal certainty and higher security** of electronic transactions than non-qualified trust services, because of stringent process to become a QTSP.
- Only QTSPs are part of the **EU's Trusted List**, which contains the providers and services that are given qualified status. If an entity is not on that list, they are not permitted to provide qualified trust services.
- Only QTSPs may use the powerful **Trust Mark** to advertise or market their services.
- Only QTSPs have a standard level of security in Europe and comply with the requirements defined in the eIDAS Regulation.

What are the steps to become a QTSP?

1. Business needs to get an assessment report issued by an accredited conformity assessment body. This assessment will verify the business and the services it provides meet the requirements to be qualified.
2. Trust Service Provider sends the report with letter of intent to the national supervisory body in the Member State where the business is located. Supervisory body has three weeks to determine if the report proves compliance.
3. If qualified status is granted, the Trust Service Provider, together with the qualified trust services it provides are added to the Trusted List. These Lists are established, published and maintained by the Member States.
4. After the Trust Service Provider is deemed Qualified, the Trust Mark is provided and clearly differentiates them from other trust services.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com

Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free