



eIDAS Regulation



Questions & Answers on rules applicable to Trust Services as of 1 July 2016

The eIDAS Regulation ([Regulation \(EU\) N°910/2014](#)) on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted by the co-legislators on 23 July 2014 is a milestone as it provides a predictable regulatory environment for electronic identification and trust services, including electronic signatures, seals, time stamps, registered delivery and website authentication.

As of 1 July 2016, the provisions applicable to trust services apply directly in the 28 Member States. This means that trust services under eIDAS are no longer regulated by national laws. As a result, the qualified trust services are recognised independently of the Member State where the Qualified Trust Service Provider is established or where the specific qualified trust service is offered.

What's new? What changes with regard to the former eSignature Directive? What must be done at national level? How does it impact market operators? How does it benefit the users (citizens, businesses and public administrations)? What has the Commission done to facilitate the switchover? These questions and many others have been asked along the road since the adoption.

We have compiled this Q&A document to help those of you who need to fully understand the new legal framework in order to implement it or reap the benefits of electronic transactions, as well as those of you who are curious about the Regulation's various implications.

I. What is new?

How will the legal effect of electronic signature change under eIDAS (compared to the regime under the eSignature Directive) as from 1 July 2016?

Since 1 July 2016, when the trust services' provisions under the eIDAS Regulation entered into application, an electronic signature can only be used by a natural person to "*sign*", i.e. mainly to express consent on the data the electronic signature is put. This represents a significant difference from the eSignature Directive where the electronic signature, which could also be used by legal persons, was defined as a means for authentication.

Under eIDAS, the "*signatory*" will be a natural person who creates an electronic signature. Therefore, certificates for electronic signatures cannot be issued to legal persons anymore. Instead, legal persons can use certificates for electronic seals (whose aim are not to sign but are means to ensure the integrity and origin of data).

What happens to qualified certificates for electronic signature issued to legal persons under the eSignature Directive as from 1 July 2016?

Former qualified electronic signatures certificates issued to legal persons cannot be used anymore to create a legally valid (qualified) electronic signature as of 1 July 2016.

In addition to electronic signature, which other trust services fall under eIDAS?

eIDAS regulates at EU level additional trust services which have emerged in a number of Member States since the eSignature Directive was adopted in 1999.

1. Electronic seals

These can only be issued to and used by legal persons to ensure origin and integrity of data/documents. An electronic seal is therefore **NOT** an electronic signature of the legal person.

When a legal entity makes use of electronic seals, it is recommended to set up an internal control mechanism ensuring that only the natural persons entitled to act on behalf of the legal entity can make use of the electronic seals (push the button on behalf of the legal entity).

Electronic seals can be also used by information systems, hence being a powerful tool for supporting secured automated transactions; in this case, again, internal control mechanisms to assure that only authorised uses are allowed should be put in place.

2. Time Stamping

Electronic time stamps are issued to ensure the correctness of the time linked to data / documents.

3. Verification and validation

Validation is an ancillary service to electronic signatures and electronic seals. It is the process of confirming the validity of a (qualified) electronic signature or electronic seal, that is, that the certificate used to create the signature or the seal was valid at the moment of creation (it was not revoked, suspended, or expired). Such a process entails the verification that the requirements of the Regulation are met by a (qualified) electronic signature or electronic seal in order to confirm its validity. The Regulation also covers the verification and validation of certificates for website authentication.

4. Preservation of electronic signatures, electronic seals or certificates related to trust services

The eIDAS Regulation sets rules for the preservation of electronic signatures, electronic seals or certificates related to trust services. Preservation is different from electronic archiving (which is NOT a trust service under eIDAS). The objectives and targets of the process will make a distinction between the two activities:

- Preservation under eIDAS aims at guaranteeing the trustworthiness of a qualified electronic signature or qualified electronic seal through time. The technology underpinning such trust service therefore targets the electronic signature or seal;
- Electronic archiving aims at ensuring that a document is stored in order to guarantee its integrity (and other legal features). The technology underpinning electronic archiving therefore targets the document. Electronic archiving remains the competence of Member States.

In other words, electronic archiving of documents and preservation of electronic signatures and electronic seals are different in nature, are based on different technical solutions (attached to the document or to the electronic signature/electronic seal) and differ in their finality (conservation of the document vs preservation of electronic signature/electronic seal).

5. Electronic registered delivery service

This is a secure channel for the transmission of documents bringing evidence of (the time of) sending and receiving the message. Nevertheless, the Regulation does not make the equivalence between (qualified) electronic registered delivery services and registered postal mail (registered items) defined under the Postal Directive. Member States remain free to establish such equivalence at national level. In other words, when the law requires fulfilling a specific procedure by sending a registered postal mail, using (qualified) electronic registered delivery services would meet this requirement only if the national law has established the equivalence.

- **Who is the sender? Who is the addressee?**

The sender (as well as the addressee) is the one identified by the qualified trust service provider, most likely the owner of the mail box. When the mail box belongs to a legal (or a different natural) person, the rules applicable to representation of legal (or natural) persons need to be followed (it is up to the legal/natural person to set up the appropriate management system for the mail box).

- **Should the identification of the sender and/or addressee be electronic?**

The identification is neither limited to electronic identification of the sender and the addressee, nor to notified eID means under eIDAS when identifying electronically. The conformity assessment report must show that the identification process set by the qualified trust service provider meets the requirements of the Regulation and the Supervisory Body must verify it during the *“initiation of qualified trust services”* set in article 21 of the Regulation. One should note that such identification also depends on the economic/business model of the qualified trust service provider. Indeed, a qualified trust service provider providing qualified electronic registered delivery services may decide to provide it on its own or in cooperation with other qualified trust service providers. In addition, the trust service provider might decide to identify and register its customers once and for all or, conversely, to allow each customer to identify for each message it would like to send. Regarding notified eIDs, qualified trust service providers may rely upon them, should they deem it appropriate with regard to their business model and provided that the conformity assessment body and the supervisory body consider that such identification process meets the requirements set by the Regulation.

6. Website authentication

Certificates for website authentication are issued to ensure users (in particular citizens and SMEs) that behind the website there is a legal person identifiable by trustworthy information. The Regulation sets clear requirements for website authentication certificates to be considered trustworthy together with minimal obligations for providers of such certificates with regard to the security of their operations, their liability and their (light-touch) supervision regime. As a consequence, the Regulation ensures transparency regarding the quality of the service offered to users, accountability of providers with regard to security of their services, trustworthiness of the data associated to authenticated websites and technological neutrality of services and solutions.

- **Can companies apply their own policies?**

As a matter of principle, the industry is obliged to in the first place apply the law and only then (where compatible) apply its own policies.

- **What is the added-value of qualified certificates for Website Authentication compared to existing SSL/TLS certificates?**

Qualified certificates for website authentication are similar to (extended validation) EV certificates. The added-value comes from the requirements of the Regulation regarding:

- (1) Risk management and strict security obligations applicable to the qualified trust service provider together with a clear liability regime;
- (2) Legal obligations regarding the proper identification of the person requiring the certificate; and
- (3) A supervision model that ensures the proper implementation of the requirements by qualified trust service providers.

An additional difference is that qualified certificates for website authentication may be issued to natural persons while existing certificates can only be issued to legal ones (according to the [EV guidelines](#)). In the EU, a Regulation applies before corporate policies. This difference is of legal nature and is not linked to technical aspects or trustworthiness of the issued certificate.

Is electronic archiving a trust service under eIDAS?

No, electronic archiving is not a trust service under eIDAS. However, the Regulation sets rules for the preservation of electronic signatures, seals or certificates related to trust services.

Do trust service providers need to provide all the trust services together?

No, it is a business decision of the trust service providers on whether to provide one, more than one or all trust services.

What are the rules on electronic documents under the eIDAS Regulation?

The eIDAS regulation sets the principle of non-discrimination of the legal effects and admissibility of electronic documents in legal proceedings. This is the first time that non-discrimination of electronic documents is regulated at EU level.

How is the qualified status granted?

- (1) An “eIDAS” accredited conformity assessment body assesses the conformity of the trust service provider and the qualified trust service it intends to start providing with the applicable requirements of the Regulation.
- (2) The trust service provider notifies the national supervisory body its intention to become qualified together with a conformity assessment report issued by a conformity assessment body. The conformity assessment report must prove the compliance with the requirements of the Regulation, and not with standards. Standards might nevertheless be a tool used by trust service providers to demonstrate their compliance with the requirements of the Regulation.
- (3) The supervisory body verifies whether or not the trust service provider and the qualified trust service it intends to start providing meet the requirements of the Regulation in order to be granted the qualified status. Upon positive verification, the qualified status is granted and the qualified trust service provider, together with the qualified trust service it provides, are added to the Trusted Lists that are established, published and maintained by Member States (therefore at national level, not at EU level).

It is worth emphasising that the final decision is in the hands of the supervisory body. The latter may rely upon the information provided in the conformity assessment report but is equally entitled to request further information and may take a duly justified decision that goes against the conformity assessment report.

Is it possible for all trust services listed in the Regulation to be granted the qualified status?

No. Only those trust services for which there are applicable requirements in the Regulation can benefit from the qualified status.

What are the main differences between qualified and non-qualified trust services?

From a legal point of view, **both qualified and non-qualified trust services benefit from a non-discrimination clause** as evidence in Courts. In other words, trust services cannot be discarded by the judge only on the grounds that they are in an electronic form.

However, because of the more stringent requirements applicable to qualified trust service providers, qualified trust services provide **a stronger specific legal effect** than non-qualified ones as well as a higher technical security. Qualified trust services therefore provide **higher legal certainty and higher security** of electronic transactions.

Can anyone deny the validity of a qualified trust service issued by a qualified trust service provider solely on the grounds that it was issued by a trust service provider established in another Member State?

No. According to the internal market principle (article 4), a qualified trust service based on a qualified certificate issued in one Member State shall be recognised as a qualified trust service in all other Member States.

What happens with the status and use of a qualified trust service issued by a qualified trust service provider if after the issuance of such a certificate, the qualified status is withdrawn by the national supervisory body?

If a qualified trust service provider loses the qualified status, the qualified trust services, i.e. the qualified certificates, already issued do not lose automatically their qualified status as well. The qualified trust service provider that no longer exists as a qualified trust service provider cannot provide new qualified trust services anymore i.e. qualified certificates for electronic signatures, but the qualified certificates already issued by such a qualified trust service provider might be used to create a qualified electronic signature unless they have unambiguously been revoked, either as direct implementation of the qualified trust service provider's termination plan or at the request of the supervisory body. The EU Trusted List provides such information on whether the trust service provider and an identified trust service it provides were qualified both at the time of issuing the certificate as well as at the time at which it is believed a signature was created.

When issuing a qualified certificate, can a qualified trust service provider verify the identity of the natural or legal person to whom the qualified certificate is issued via videoconference?

Yes. Qualified trust service providers can identify a person to whom they issue a certificate via videoconference, as long as the procedure is foreseen at national level and complies with the eIDAS Regulation. More specifically, under eIDAS (article 24(1) d), videoconference could be an identification method if recognised as such at national level and with the precondition that it provides equivalent assurance in terms of reliability to physical presence (e.g. data checked against an authoritative source, for example, population register, etc.), confirmed by a conformity assessment body.

To which “national law” does article 24(1) refer, especially in cross-border situations where the trust service provider provides trusted services in another Member State than where the trust service provider is established?

“National law” in article 24(1) refers to the national law of the Member State where the qualified trust service provider is established. Even when a trust service provider established in a Member State provides trust services in another Member State, the applicable “national law” is the one of the Member State where the qualified trust service provider is established.

What do the eIDAS non-discrimination clauses mean?

The eIDAS Regulation sets the principle of non-discrimination of the legal effects and admissibility of electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services and electronic documents as evidence in legal proceedings. Courts (or other bodies in charge of legal proceedings) cannot discard them as evidence only because they are in an electronic form. Nevertheless, Courts must check whether there are any procedures to be followed according to the EU or national (general or sectorial) law for a given document (including possible requirements on the use of specific levels of electronic tools) and might discard them on these grounds. In other words, the non-discrimination clause does not mean that each and every procedure can be carried out electronically. It means that Courts have to assess these electronic tools in the same way they would do for their paper equivalent.

What is a closed system?

The eIDAS Regulation does not apply to “*the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants*” (article 2.2). The concept of closed systems is further clarified in recital 21 of the Regulation by specifying that services used exclusively within closed systems between a defined set of participants must “have no effect on third parties” and that “*only trust services provided to the public having effects on third parties should meet the requirements laid down in the Regulation*”. As a concrete example, systems set up in businesses or public administrations to manage internal procedures making use of trust services are explicitly referred to. It has to be noted that the exception for closed systems is at the benefit of providers which would not be subject to the requirements of the Regulation. Users may always opt-in by buying (qualified) trust services from (qualified) trust service providers instead of going for a closed system (regardless whether or not the trust service is used between a defined set of participants).

II. What must/can be done at national level?

Can Member States regulate other trust services than those under eIDAS at national level?

Yes, Member States can do that. The eIDAS Regulation (recital 25) allows Member States to define other types of trust services in addition to those provided for in the eIDAS Regulation. However, such “*additional*” trust services fall outside the scope of the eIDAS Regulation and have no legal effect across borders. Such trust services defined at national level may also be “*qualified*” and, if Member States decide so, may also be indicated as a national “*qualified*” trust service in the National Trusted List.

Can Member States restrict the type of electronic signature required for a given online public service or transaction?

This covers scenarios like allowing only qualified electronic signatures for signing a request to initiate legal proceedings addressed to a competent court or signing a renting contract online. Member States remain free to decide which type of electronic signatures is required for a given online public service or transaction without prejudice to obligations stemming from other legislations. Nonetheless, certain obligations exist when Member States require advanced electronic signatures or advanced electronic signatures based on a qualified certificate to use online services offered by public sector bodies (article 27).

The above principle of Member States remaining free to decide on the level of security for a given online public service or transaction also applies to the other trust services in the eIDAS Regulation.

Can a Member State put administrative measures in addition to those foreseen under eIDAS in place?

Additional national administrative measures, whose adoption at national level mainly depends on the existing administrative practices in place, or legal implementing measures might be considered appropriate provided that the national approach does not hinder the legal recognition of the trust services provided in a different Member State and does not hamper technical interoperability.

If there is a national law imposing a maximum validity period for qualified certificates in a specific Member State, would that affect the recognition of qualified certificates issued in other Member States which have longer validity?

No. Qualified certificates should not be subject to any mandatory requirements exceeding the requirements laid down in this Regulation. Therefore, if they meet the requirements of the Regulation they should be recognised across borders.

Can Member States impose a specific business/technical model or a standard to be followed?

No. Member States cannot impose either the business/technical model to be set up by qualified trust service providers or a specific standard to be followed. The trust service provider has to demonstrate its compliance (building upon standards if it deems it appropriate) with the requirements of the Regulation while the supervisory body cannot refuse to grant the qualified status solely on the grounds that the proposed model does not comply with a given standard or a given business/technical model.

Should Member States lay down rules on penalties regarding the incorrect use of the EU trust mark?

There are currently no specific penalties for the incorrect use of the EU trust mark or its use by unauthorised entities. Nonetheless, according to article 16 of the eIDAS Regulation, "Member States shall lay down the rules on penalties applicable to infringements of this Regulation. The penalties provided for shall be effective, proportionate and dissuasive". This comprises all types of infringements of the Regulation, thus also including the incorrect use or misuse of the EU trust mark. Enforcement is part of the role of supervisory bodies in line with article 17(3) of the eIDAS Regulation. For further details, a [user manual](#) together with [frequently asked questions](#) on the EU trust mark are available [on-line](#).

III. Transitional measures

How is the smooth transition from the eSignature Directive of 1999 and the eIDAS regime ensured?

The eIDAS Regulation provides transitional measures (article 51) to ensure the continuity and legal certainty of products and services associated to electronic signatures under Directive 1999/93/EC. In a nutshell, secure signature creation devices and qualified certificates for electronic signatures for natural persons that are deemed compliant with the eSignature Directive before 1 July 2016 will be deemed compliant with the Regulation until they expire. Similarly, if deemed compliant with the eSignature Directive before 1 July 2016, certification-service-providers issuing qualified certificates for electronic signatures benefit from a 1 year transition period to adapt their systems to the new requirements (i.e. until 1 July 2017) during which they are deemed compliant with the Regulation.

What happens to valid qualified certificates for electronic signature issued to natural persons under the eSignature Directive after the eIDAS regime enters into effect?

In article 51(2) of the eIDAS Regulation a transitional measure is foreseen for qualified certificates for electronic signatures issued to natural persons under Directive 1999/93/EC. The latter will be considered as qualified certificates for electronic signatures under the eIDAS Regulation until they expire.

What will not be covered under the transitional measures?

A few cases are not covered by the transitional measures set in eIDAS Regulation, such as:

- Existing certificates (qualified or not) for eSignatures issued to legal persons: as under the eIDAS Regulation, eSignatures can only be issued to and used by natural persons, such former valid certificates are not valid anymore.
- Existing trust service providers providing other trust services but eSignature ones which were recognised as "qualified" under national regimes: as from 1 July 2016, such trust service providers are considered as non-qualified ones under eIDAS unless they would have undergone the initiation process for qualified trust services set in the eIDAS Regulation.

Can the transitional measure in article 51(1) of the eIDAS Regulation apply to qualified electronic seal creation devices?

According to the eIDAS Regulation, both qualified electronic signature creation devices and qualified electronic seal creation devices shall meet the requirements laid down in Annex II. The requirements set out in Annex II of the eIDAS Regulation are actually the same with those set out in Annex III of the Directive 1999/93/EC. Nevertheless, since the concept of the creation of “*electronic seals*” was introduced by eIDAS Regulation, no transitional measures may apply to electronic seals or certificates related thereto. Moreover, there is not such an explicit reference within the Regulation. However, the Commission services have recognised certain merits to an interpretation of article 51(1) on the basis that devices certified under the Directive might also be used for the creation of electronic seals. Article 51(1) may not allow the conclusion according to which devices that were certified under the Directive may clearly be used for the creation of electronic seals under the Regulation, but it does not completely rule out the opposite interpretation. In any case, the interpretation of Union law falls within the exclusive competence of the Court of Justice.

IV. Actions taken by public bodies, including Member States and EU institutions

A. Member States

What measures had to be implemented at national level before 1 July 2016?

The Regulation is directly applicable in all 28 EU Member States. However, before 1 July 2016 Member States had to ensure that:

- A competent national authority in charge of supervising trust service providers has been designated (i.e. a Supervisory Body);
- Effective sanctions / fines have been set;
- The [National Accreditation Body](#) accredits conformity assessment bodies (according to [Regulation 765/2008](#));
- A national Trusted List is published and maintained in line with the [Commission Implementing Decision \(EU\) 2015/1505](#);
- Public sector bodies are able to recognise the formats of advanced electronic signatures and electronic seals (according to the [Commission Implementing Decision \(EU\) 2015/1506](#)) whenever they require an advanced electronic signature or electronic seal.

Can conformity assessment bodies accredited according to eIDAS be included in the NANDO database?

No. The [NANDO](#) (New Approach Notified and Designated Organisations) database lists only notified bodies that carry out conformity assessment for manufactured products where the legislation requires third-party intervention using Decision 768/2008/EC as the reference legislation. While the eIDAS Regulation does refer to a system of accreditation, it does not provide a framework for a system for notification of notified bodies. This is why, from a legal point of view, only notified bodies can be listed in the NANDO database. In order to provide a publicly available list of CABs accredited in accordance with the eIDAS Regulation, the Commission has already invited the National Accreditation Bodies (NABs) to provide information about the CABs that have been accredited by them in accordance with the eIDAS Regulation. In addition, a functional mailbox (CNECT-EIDAS-TS-NOTIFICATIONS@ec.europa.eu) has been set up to receive notifications by NABs on CABs accredited by them in accordance with eIDAS.

Is there a list of the conformity assessment bodies accredited under eIDAS?

Based on information provided by the national accreditation bodies in the Member States, the Commission compiled a [list of conformity](#) assessment bodies as defined in point 18 of article 3 of the eIDAS Regulation. Please note that this list is only an informative tool. In order to collect this information, the European Commission has set up a [functional mailbox \(CNECT EIDAS TS NOTIFICATIONS\)](#) where national accreditation bodies can notify the conformity assessment bodies accredited according to the eIDAS Regulation. This mailbox can be used for all notifications related to electronic trust services under eIDAS.

What is the role and use of Trusted Lists?

Trusted Lists are essential in ensuring **certainty** and building **trust** among **market operators** as they indicate the status of the service provider and of the service at the moment of supervision, while aiming at fostering **interoperability** of qualified trust services by facilitating the validation of, among others, electronic signatures and electronic seals.

What is the value of the Trusted Lists under eIDAS?

Under the eIDAS Regulation, national Trusted Lists have a constitutive effect. In other words, a provider/service will be qualified only if it appears in the Trusted Lists. Consequently, the users (citizens, businesses or public administrations) will benefit from the legal effect associated with a given qualified trust service only if the latter is listed (as qualified) in the Trusted Lists.

What is the Trusted List Browser?

The European Commission has launched the [Trusted List Browser](#) to enable anyone to browse Europe's Trusted Lists and look for available trust services in the EU. The Trusted List Browser is a mobile-friendly web application which complements the Trusted List (TL) Manager and [DSS](#).

Could Trusted Lists be used in connection with web browsers?

Under the eIDAS Regulation, there is no obligation for browser vendors to recognise, integrate or make use of the Trusted Lists in their products. Nonetheless, given the role of the eIDAS Regulation and Trusted Lists in unleashing the potential of the Digital Single Market, there certainly is a very high expectation that Trusted Lists will be used in/relied upon by existing browsers to ensure that trust in digital transactions are verified to the benefits of the EU citizens and businesses.

Given the constitutive value of Trusted Lists as a legal anchor for trustworthy transactions, any erroneous, misleading or imprecise communications regarding the result of a certificate validation may lead to liability.

B. Support from the EU Institutions

What has the Commission done to facilitate the switchover to the new trust services regime?

Since the adoption of the eIDAS Regulation in 2014, the Commission has been working in close cooperation with a variety of stakeholders from both public and private sector to ensure a smooth implementation of the new rules.

The regular stakeholder consultations focused on *awareness-raising*, understanding how the rapid technological developments may affect the service provision and what the needs of the industry and commerce are. In this context, the European Commission held a number of high-level events, published [blogs](#) and set up a [collaborative platform](#).

What is the Commission's plan concerning other implementing acts?

The Commission has not planned to adopt other implementing acts in the near future. Nonetheless, the Commission will take into utmost account the stakeholders' needs and will carefully review the results of more flexible approaches, such as the EU accreditation scheme developed by the [European Cooperation for Accreditation](#) or the guidelines on security breach notifications (article 19), developed by the [European Union Agency for Network and Information Security \(ENISA\)](#).

What about the international aspects related to trust services under eIDAS?

Non-qualified trust services provided by trust service providers established in non-EU countries can freely circulate in the EU under the eIDAS Regulation while not benefiting from the qualified status.

On the other hand, trust services provided by trust service providers established in a third country shall be considered legally equivalent to qualified trust services provided by EU qualified trust service providers where there is an agreement between the EU and the country of origin of the provider (or an international organisation), on condition that the same applies to the trust services provided by EU qualified trust service providers in the given third country (principle of reciprocity). In this regard, it must be highlighted that negotiations on such international agreement can be only initiated by authorities representing officially the EU, their State or their international organisation.

Is the eIDAS Regulation applicable to the EU Institutions?

The Regulation is not applicable to the EU Institutions which are governed by their own adopted rules of procedures. The European Commission is currently regulated in this field by [Commission Decision 2004/563/EC](#) (that has been integrated to its Rules of Procedure) setting Commission's own provisions on electronic and digitised documents to cover all electronic native documents and electronic documents resulting from the digitisation of documents originally on a physical medium. Moreover, recital 69 of the eIDAS Regulation encourages the Union institutions, bodies, offices and agencies "*to recognise electronic identification and trust services covered by this Regulation for the purpose of administrative cooperation ...*". In this regard, it must be highlighted that the identification system of natural or legal persons used by the Commission (called EU Login) already features the possibility of using the notified eID means while the Commission is working on the recognition of the new trust services referred to in the eIDAS Regulation.



For more information:

 ec.europa.eu/digital-single-market/trust-services-and-eid

 [@EU_eIDAS](https://twitter.com/EU_eIDAS)

eIDAS Observatory: ec.europa.eu/futurium/en/eidas-observatory

