Security guidelines on the appropriate use of qualified electronic seals

Guidance for users

VERSION 2.0

FINAL

DECEMBER 2016

www.enisa.europa.eu

European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use trust@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN 978-92-9204-213-4, DOI 10.2824/352342

Table of Contents

Executive Summary

On July 1st 2016, Regulation (EU) 910/2014 (hereafter called the eIDAS Regulation), which lays down the rules on electronic identification and trust services for electronic transactions in the internal market came into force covering across Europe in all 28 Member States. It defines trust services for supporting electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services and website authentication.

The eIDAS Regulation represented a big step forward in building a Digital Single Market as it provides one common legal framework for all parties relying or providing on those kind of services. Indeed, various sectors of the economy (e.g. finance, banking, transport, insurance, health, sharing economy, trading, etc.) where obligations exist for security, reliable identification, strong authentication, legal certainty of evidences, will clearly be positively affected by the eIDAS Regulation. This latter will indeed allow citizens, businesses and public administrations to meet such obligations for any (cross-border) electronic transaction as they will now be able to use the recognised eID means and (qualified) trust services. In particular, a qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked. When based on a qualified certificate issued in one Member State, it shall be recognised as a qualified electronic seal in all other Member States.

This document addresses qualified electronic seals and is one out of a series of five documents which target to assist parties aiming to use qualified electronic signatures, seals, time stamps, eDelivery and website authentication certificates to understand the subject correctly as-well-as the potential benefits, amongst others, by giving examples of possible application. This series of documents also targets to give those parties some advice on how to correctly use the related qualified trust services.

After explaining what a qualified electronic seal is and what properties/function it does and does not provide, concrete examples of use are given for inspiration to the readers. Next to that, and as even the most secure / trusted service becomes insecure and unreliable if not being integrated or used correctly, some key recommendations are given for correct integration and use, pertaining :

- Both the signatory and the relying party should look for the EU trust mark for qualified trust services when selecting providers.
- The relying party shall follow the applicable Certification Authority's terms and conditions and/or other contractual documentation.
- The first level of augmentation consists in time-stamping the seal
- In a seal with Long-Term Validation Data, the set of validation material or references to it should be sufficient to ascertain the validation status of all end-entity certificates contained in the seal.
- Before algorithms, keys, and other cryptographic data used at the time a seal was built become weak and the cryptographic functions become vulnerable, or the certificates supporting previous time stamp tokens expire or are revoked, the sealed data, the seal as well as any additional information should be protected by applying time stamp tokens.
- QESeal services should be further supported by ancillary qualified trust services
- The relying party should verify that the provider is duly qualified is to check its presence in the trusted list of the Member State where it operates.

1. Introduction

1.1 General context/the eIDAS Regulation on eID and trust services

Regulation (EU) No 910/2014[1] ([1], hereafter the **eIDAS**[2] Regulation), on electronic identification and trust services for electronic transactions in the internal market, provides a predictable regulatory environment for electronic identification and a set of electronic trust services, namely electronic signatures, seals, time stamps, registered delivery services and certificates for website authentication.

It is possible to use these trust services as well as electronic documents as evidence in legal proceedings in all EU Member States contributing to their general cross-border use. Courts (or other bodies in charge of legal proceedings) cannot discard them as evidence only because they are electronic but have to assess these electronic tools in the same way they would do for their paper equivalent.

Whether you are a large company, a SME or a citizen willing to complete an electronic transaction in another EU country, e.g. submit a call for tender or register as a student in another EU Member State (MS), besides reducing time and costs, the eIDAS Regulation will ensure cross-border recognition of national eID and electronic trust services supporting your electronic transaction. Hence it will boost trust, security and convenience.

Since 1st July 2016, most provisions of the eIDAS Regulation are directly applicable in the 28 EU Member States' legal framework overcoming problems of fragmented national regimes. It provides legal certainty and fosters the usage of eID means and electronic trust services for online access and online transactions at EU level.

The eIDAS Regulation will ensure that people and businesses can use their national eIDs to access public services in other EU countries where eIDs are required for such an access at national level. It also creates an EU wide internal market for electronic trust services by ensuring their recognition and workability across borders and are considered equivalent to traditional paper based processes.

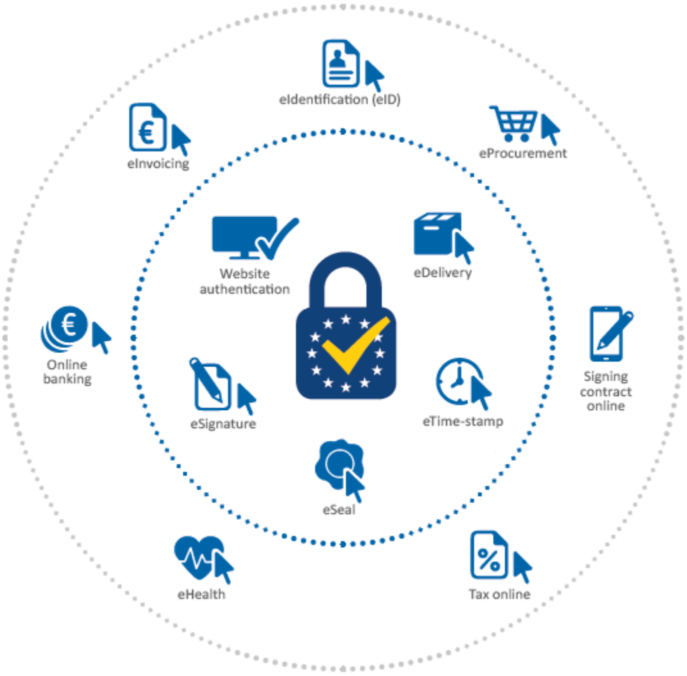
1.2 Opportunities introduced by the eIDAS Regulation

An array of opportunities resides in leveraging eID and electronic trust services as key enablers for making national and cross-border electronic transactions more secure, more convenient, trustworthy and benefiting from legal certainty.

The broader adoption of EU-wide recognised eID means and of electronic trust services will facilitate and boost the digital transformation of organisations, be it public administrations or businesses, enhance customer experience, improve the security of electronic transactions and stimulate the provisioning of new and innovative services.

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014, p. 73–114.
[2] See Glossary.

To this end, various sectors of the economy (e.g. finance, banking, transport, insurance, health, sharing economy, trading, etc.) where obligations exist for security, reliable identification, strong authentication, legal certainty of evidences, will be positively affected. The eIDAS Regulation indeed allows citizens, businesses and public administrations to conveniently meet such obligations for any cross-border electronic transaction using the recognised eID means and (qualified) trust services of their choice. Without undergoing identity verification based on physical presence, but by using MS notified eID means of a level "high", one should for example be able to use public services in another country or banks may accept such eID to open a bank account[3]. By relying on a qualified time stamp, one will benefit, across the EU, from the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.



1.3 Specific role of the qualified trust services

To further enhance in particular the trust of small and medium-sized enterprises (SMEs) and consumers in the internal market and to promote the use of trust services and products, the eIDAS Regulation introduces the notions of qualified trust service and qualified trust service provider with a view to indicating requirements and obligations that ensure high-level security of whatever qualified trust service or product is used or provided and, as a consequence, are granted a higher presumption of their legal effect.

Therefore, when looking for trust services, selecting qualified services ensures benefiting from a high level of security and legal certainty of trust services. E.g., qualified electronic time stamp shall enjoy, all over the EU, the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.

1.4 Initiation and supervision of qualified trust services

In order to ensure high-level security of qualified trust services, the eIDAS Regulation foresees an active supervision scheme of qualified trust service providers (QTSP) and the qualified trust services (QTS) they provide (hereafter referred to as a QTSP/QTS) by the national competent supervisory body (SB) that supervises, ex ante and ex post, fulfilment of the **QTSP/QTS requirements and obligations**[4].

[3] National legislations on prevention of money laundering may currently may force identity verification to be based on physical presence. Furthermore, the use by the private sector of electronic identification means under a notified scheme is on a voluntarily basis only (see Recital 17 of the eIDAS Regulation).

[4] See glossary

All those requirements must be met by the QTSP/QTS before providing the very first qualified trust service output, e.g. before issuing the very first qualified time stamp in the case of QTSP providing qualified time stamping services.

Before a TSP/TS is granted a qualified status (QTSP/QTS), it will be subject to a pre-authorisation process – the so-called initiation process. QTSPs may only begin to provide the qualified trust service after the qualified status has been granted by the competent supervisory body and indicated in the national **trusted list**[5]. From there, the supervision scheme covers the full life cycle of each QTS and each QTSP, from inception until termination.

In practice, where TSPs, without qualified status, intend to start providing qualified trust services, they shall submit to the supervisory body a notification of their intention together with a conformity assessment report issued by an “eIDAS” accredited conformity assessment body. Before notifying the competent supervisory body of their intention to start providing qualified trust services, the future QTSP/QTS must hence successfully pass an external assessment (audit) to confirm it fulfils the eIDAS requirements. That audit must be conducted by a conformity assessment body specifically accredited to carry out assessments of QTSP/QTS. The audit results in a formal conformity statement confirming - if such is the case - that the QTSP/QTS meets all the applicable requirements of the eIDAS Regulation. Based on the notified information including the report of such an audit, the competent SB will formally verify that the candidate QTSP/QTS meets the applicable eIDAS requirements and, in case of positive verification, it will undertake the publication of the grant of the qualified status for that QTSP/QTS in the national trusted list.

It is only when its qualified status is published in the corresponding national trusted list that the QTSP/QTS is authorised to provide the corresponding QTS.

Note: A TSP cannot be qualified without providing at least one qualified trust service (cfr Art.3.20 of the eIDAS Regulation). A TSP is granted a qualified status separately for each type of qualified trust service covered by the eIDAS Regulation. E.g. a QTSP qualified for the provisioning of qualified certificates for electronic signatures is not per se granted a qualified status for the issuance of qualified time stamps; it must first complete the full pre-authorisation process and have its granted qualified status for the provision of qualified time stamp published explicitly in the national trusted list before issuing qualified time stamps in addition to the provision of qualified certificates for electronic signatures. There are nine different types of QTSs defined by the eIDAS Regulation for which a qualified status is granted separately: provision of qualified certificates for electronic signatures, provision of qualified certificates for electronic seals, provision of qualified certificates for website authentication, qualified preservation service for qualified electronic signatures, qualified preservation service for qualified electronic seals, qualified validation service for qualified electronic signatures, qualified validation service for qualified electronic seals, qualified electronic time stamps services, and qualified electronic registered delivery services.[6]

For marketing purposes, once qualified, a QTSP/QTS may use the EU Trust Mark for qualified trust services when promoting its QTS. This trust mark (shown in Figure 1) can only be used by a QTSP to “label” its QTS. It can be used on any support provided it meets requirements from Art.23 of the eIDAS Regulation (e.g. a link to the corresponding national trusted list where consumers may verify the granted qualified status

[5] See glossary.

[6] See Annex A.7 for further details.

must be displayed on the QTSP's website) and rules of Commission Implementing Regulation (EU) 2015/806.[7] Basically, this secondary legislation sets the form, colour and size of the EU trust mark, sets the obligation to clearly indicate the qualified services that the EU trust mark pertains to, and allows association with other graphical or textual elements provided that certain conditions are met.

Figure 1: EU trust mark for qualified trust services

The use of the EU trust mark[8], which is voluntary, aims to foster transparency of the market and help consumers to distinguish between qualified trust services and non-qualified ones.

Once granted a qualified status, QTSPs and their QTSs have the obligation to pass, and submit the competent supervisory body with a two-yearly conformity assessment report (CAR) issued by an accredited CAB confirming that the QTSP and the QTSs it provides fulfil the requirements laid down in the Regulation. Competent supervisory bodies are also allowed, at their own discretion and at any time, to audit themselves any QTSP/QTS for which they are competent or to request an accredited CAB to perform an ad hoc audit.

QTSPs and their QTSs are supervised for their entire lifecycle, from their genesis to their termination. In particular, in order to ensure sustainability and durability of QTSs, as well as to ensure proper termination and user's confidence in their provision, QTSPs must maintain, at all times, an up-to-date termination plan. That plan is to be agreed by the SB upon initiation and regularly checked for compliance during the life of the QTSP/QTS.

1.5 A focus on qualified electronic seals

Since a few years it is possible to **electronically sign data** and to achieve the same effects as when using a hand-written signature. The equivalence with "hand" written signatures works pretty well for human beings, but was difficult to **extend to legal persons** (that basically has no hand). However legal persons (companies, organisation, etc.) needed to officialise electronic documents they issued, in order to ensure the origin of the document. Today the eIDAS Regulation supports this need thanks to the legal recognition of **electronic seals**, which serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity. In addition to

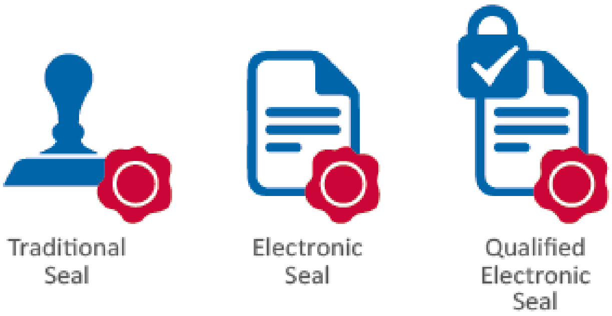


Figure 2: Types of seals

[7] Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services (Text with EEA relevance). OJ L 128, 23.5.2015, p. 13–15.
[8] See https://ec.europa.eu/digital-single-market/en/news/eu-trust-mark for more guidance on the use of that trust mark, downloadable images, user manual and answers to frequently asked questions.

authenticating the document issued by the legal person, electronic seals can be used to authenticate any digital asset of the legal person, such as software code or servers (eIDAS Regulation).

A **qualified electronic seal** shall enjoy the **presumption of integrity of the data** and of **correctness of the origin** of that data to which the qualified electronic seal is linked.

Beside the legal framework, the technical framework is nowadays very mature as it heavily relies on the technical framework developed over the years for electronic signature.

The use of qualified electronic seals should help the development of online business and services in Europe by securing online transactions and services in Europe and beyond in many sectors: e-business, e-administration, e-banking, e-services, e-archiving, etc.

1.6 Scope of the present document and relationship with other recommendations

This document proposes a set of **security guidelines on the appropriate use of qualified electronic seals**. The objective of the document is to support relying parties and end users of qualified electronic seal services to securely use these services.

The target audience of the document are end users and relying parties of qualified electronic seal services. This could comprise individuals, businesses and public administrations. For example, it could be a public administration that wishes to use qualified electronic seals providing official documents to citizens, and which would like to ensure it is utilizing these services:

- In compliance with the eIDAS Regulation.
- In a proper and secure manner that guarantees that the security properties of the service are maintained.

The structure of the document, from the next sections, is organised to provide information and guidance with regards to the following aspects of qualified electronic seal:

- What is it?
- What key properties does it provide?
- What properties can it not provide?
- What are the potential use cases?
- What are the usage best practices?
- Example of tools & practical usage aspects.

Four other linked documents propose security guidelines on the appropriate use respectively of qualified electronic signatures, qualified electronic time stamps, qualified website authentication certificates and qualified electronic registered delivery.[9]

Although each of these qualified trust services share some technical backgrounds or tools and thus provide some common functionalities, such as those illustrated below, each of them has its own objectives and core functionalities as summarised in the following table:

[9] See https://www.enisa.europa.eu/topics/trust-services/qualified-trust-services.

Qualified Trust Service	Data Integrity	Confidentiality	Authenticates Origin *(Natural Person)*	Authenticates Origin *(Legal Person)*	Authenticates Time
QTS	✓	✗	✗	✗	✓
QES	✓	✗	✓	✗	✗
QESeal	✓	✗	✗	✓	✗
QWAC	✓	✓	✓	✓	✗
QeDel	✓	✓*	✓	✓	✓

*not a core functionality but is usually provided as part of a greater solution

Table 1: Comparative table of functionalities offered by the various types of qualified trust services

If each (qualified) trust service can be used as a stand-alone service, some (qualified) trust services may support other (qualified) trust services.

2. Qualified electronic seal – what is it?

2.1 Legal definition of (qualified) electronic seals

The eIDAS Regulation defines an **electronic seal** as "*data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity*". A **qualified electronic seal** shall enjoy the **presumption of integrity of the data** and **of correctness of the origin** of that data to which the qualified electronic seal is linked.

A seal is "**generated**" by a **creator of the seal,** possibly "**augmented**" (i.e. completed with related proofs or evidences – see section 6), "**validated**" by the receiver of the sealed data (so-called "relying party"), and possibly **preserved,** in some cases for a long term.

The way these features are used determines the level of strength, assurance and longevity of the qualified seals. In particular, TSPs, qualified or not, can be called for the qualified **seal creation, validation** and/or **preservation**.

Electronic seals are **created** by an electronic **seal creation device**, which is defined in the eIDAS Regulation as "*a configured software or hardware used to create an electronic seal* by means of an **'electronic seal creation data'** (i.e. *"a unique data which is used by the creator of the seal to create an electronic seal")*".

In these definitions, the "unique data" is to be seen as a personal element that belongs to the creator of the seal. It can be compared to the rings with engraved design used for stamping a seal in wax in the old times. Official mails, from a kingdom e.g., were easily recognised because everybody knew the official engraved design. The ring was a hand-made artefact, a priori not (easily) reproducible, making the royal seal difficult to imitate and difficult to steal because worn by the kind. In the same way that creator of the seal keeps his/her ring secure in the paper world, the electronic seal creation data also needs to be protected in the electronic world. Typically, it will be securely stored on a device (e.g. a smart card like a bank card) that can be activated by its owner only, e.g. by means of a PIN code, or biometry (e.g. fingerprint). Because the seal represents an organisation, it some cases there may be more than one physical persons authorised to create seals on behalf of the organisation; there may be more than one PIN codes or fingerprint registered to activate a seal creation data.

Electronic seals in general shall not be denied legal effect and admissibility as evidence in legal proceedings. Within the electronic seal family, the eIDAS Regulation defines subsets of electronic seals that provide increasing legal predictability up to a level, the qualified electronic seal**,** that benefits from an automatic presumption of integrity of the data and of correctness of the origin (like any qualified service, it benefits from an automatic recognition):

- the electronic seal (presented above)
- the **advanced electronic seal** **(AdESeal)** – which requires security features that ensure it is uniquely linked to the signatory, it is capable of identifying the signatory entity and it is linked to the data in such a manner that any subsequent change of the data is detectable.
- the **qualified electronic seal** **(QESeal)** – which is an advanced electronic seal which provides additional level of assurance on the identity of the creator of the seal and an enhanced protection and level of assurance on the seal creation. A special device is required for the creation of QESeal (a **qualified seal creation device**, **QSealCD**).

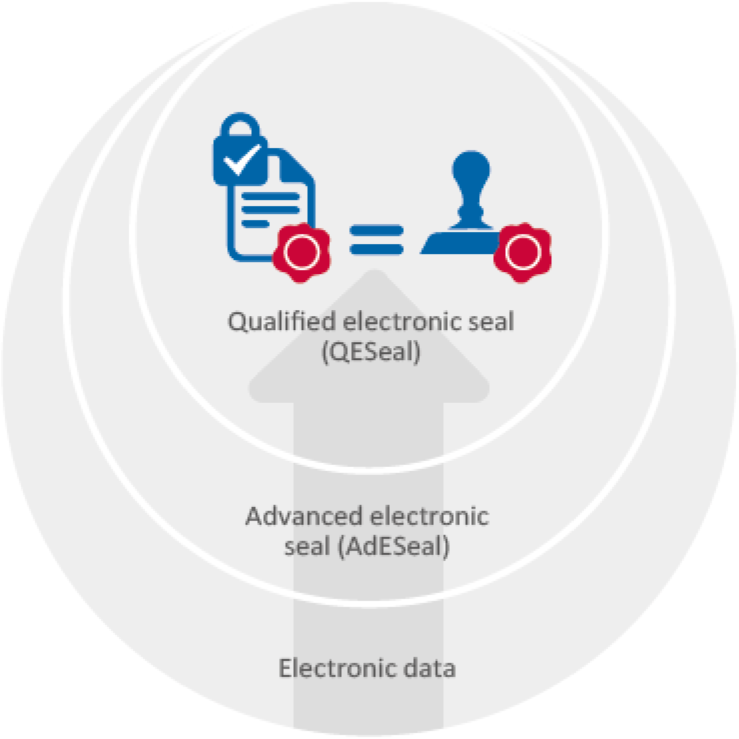


Figure 3: Types of electronic seals

A QESeal shall be recognised as a qualified electronic seal in all Member States.

This equivalence is gained from the fact that qualified electronic seals are supported by i) trustworthy process technology, similar to advanced electronic seals, ii) qualified electronic seal creation devices and iii) qualified trust service providers (QTSPs) which are supervised by EU MS appointed supervisory bodies.

2.2 Public Key Cryptography as technical foundations for (Q)ESeal

In the current state of the art, QESeal are implemented by means of asymmetric cryptography. With this technology, each seal's owner has a key pair made of a private and a public key (the technology is called public key cryptography) and the electronic seals so produced are called **digital signatures** (not to be confused with 'electronic signatures' that rely on the same technology but is a legal concept dedicated to natural person).

The signature creation and verification process as follows:

1. The creator of the seal uses the private key to seal (or in technical terms, to digitally sign) a text:

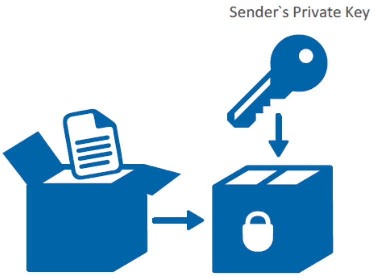


Figure 4: Digitally signing data with a private key to produce an electronic seal

The private key is in fact a secret code used by a mathematical function in order to render a data unintelligible (i.e. encrypt data). In the illustration the data is put in a box closed by the padlock. The private key corresponds to the so-called 'seal creation data' as defined in the eIDAS Regulation.
In the paper world the "private key" concept can be compared to the ring with engraved design used for stamping a seal in wax presented above, that is in theory only reproducible by the owner of the ring, i.e. the creator of the seal.

2. The verifier (also called relying party in the eIDAS Regulation) uses the creator of the seal's public key to verify the digital signature:

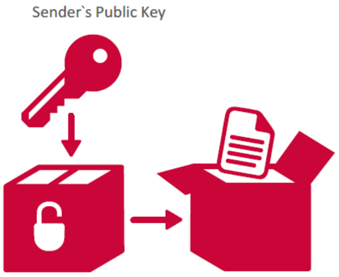


Figure 5: Verifying a seal with a public key.

The public key is in fact a code used by the reverse mathematical function to retrieve the initial data from the encrypted data. In the illustration the data is retrieved from the box thanks to the public key.
In the paper world, the "public key" concept can be compared to an "official" example of a seal that a verifier can compare with a received seal.

The verification of a seal with a certain public key means that the seal was computed with the corresponding private key (in the illustration the public key can only open one particular padlock). Only the creator of the seal in possession of the private key can be at the origin of the seal. As a consequence the person that owns the private key matching the public key (i.e. the creator of the seal) cannot deny to be at the origin of such seal; this **correctness of origin** feature is the foundation of any seal (electronic or paper-based).

Another characteristic of the digital signature technique used to seal data is that if the sealed text has been modified after the creation of the seal, the verification of the seal will fail (because the seal computation mixed the private key and the data to be sealed, the verification computation will always disclose the very same data). (In the illustration the data in the box cannot be retrieved or replaced or modified by other data until the box is opened). As a consequence, successful seal verification also ensures **data integrity**.

Of course, there are some technical tricks to ensure that only the person that owns the private key matching the public key is able to create the signature (and a third person would not be able to imitate the creator of the seal's seal):

- it is assumed to be computationally impossible to discover the private key from the knowledge of the public key. Any stakeholder in possession of a public key is able to verify that a signed data has been made by the corresponding private key, without being able to play the role of the creator of the seal since (s)he cannot guess the private key. The size of the key is an important parameter for the security of the algorithm.
- A different unique key pair is allocated to each creator of a seal.
- The creator of the seal shall protect the private key (in the same way as (s)he would not explain to third party how to imitate her seal).

2.3 Certification services as trust foundation for (Q)ESeal

The technical foundations presented above, alone, are not sufficient to ensure the full confidence in the system. Indeed, trust in seals relies on the guarantee that a certain Public Key belongs to a particular creator of the seal, owner (and sole controller) of the corresponding private key. For this purpose, an entity, trusted by the community, called a **certification authority** (also called a Certification Service Provider, CSP**,** which is a particular type of TSP as defined in the eIDAS Regulation), certifies the link {public key – creator of the seal} in a public key **certificate**. In general, one finds the information on the identity of the creator of the seal in the certificate.

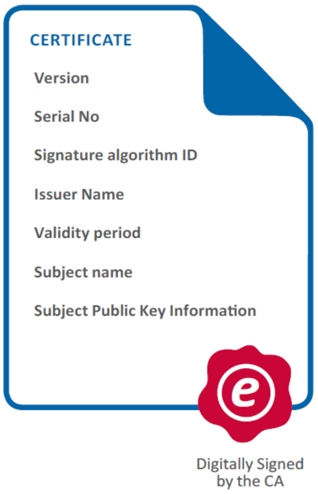


Figure 6: A digital certificate

The certificate is a signed or sealed statement by the CA; the CA's signature or seal is trusted because the CA's key is published in a media trusted by the community (e.g. the official journal). The procedures, techniques and mechanisms put in place to realise such certification services are commonly called **Public Key Infrastructure** (or PKI). The certificate officialises the link between a creator of a seal and its key pair in the same way that an identity card officialises the link between a citizen and his/her handwritten signature represented on the card.

The trust in certificates relies on the quality of the CA and its certification services. The CA must follow sound policies: strong cryptography, secure CA premises and devices, seal creation devices for creators of seals of a good quality, trusted personnel, insurances, etc.

It also relies on the possibility to **revoke** certificates that are not trusted anymore and to publish **revocation status** (i.e. black list of revoked certificates) to verifying parties (i.e. **validation services**). This can happen for instance if the creator of the seal has lost his/her seal creation device and fears that someone uses it in his/her place.

Finally, trust in CA policies relies on the level of assurance that the CA indeed correctly implements these policies. For this purpose the CA can be **audited**.

2.4 The electronic seal process

The seal creation workflow

A seal owner, to create a seal in a document, works in a certain environment (e.g. a laptop) to access sealing functionalities made of:

a. the seal creation application (e.g. a pdf application residing on the laptop) and
b. the seal creation device *that*
   i. holds the seal creation data (private key);
   ii. shall be able to authenticate the creator of the seal (to guarantee his/her control on the private key);
   iii. computes the seal (using the sealer's seal creation data);
   iv. may hold the sealing certificate (or unambiguous references to it).

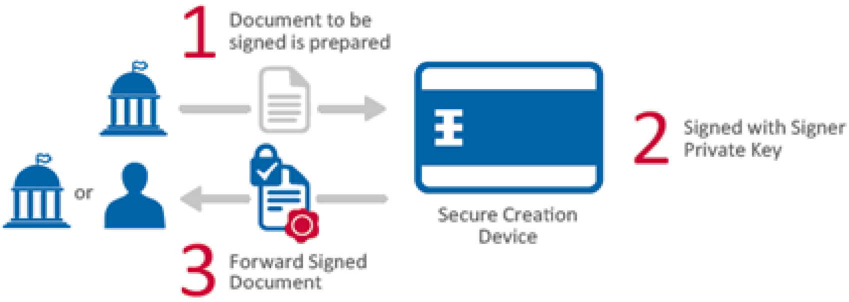

1 Document to be signed is prepared
2 Signed with Signer Private Key
Secure Creation Device
or
3 Forward Signed Document

Figure 7: Seal creation process

Concretely, how does it work?

1. The creator of the seal prepares the document to be sealed (e.g. a PDF file).

2. The application prepares the data to be sealed (i.e. the PDF) in a condensate (called a ***hash***) and present it to the secure seal creation device.

3. The seal creation device asks the authorisation to the creator of the seal to seal the data, in general, through a windows that pops up on the screen. The creator of the seal authenticates to the device (e.g. (s)he enters a PIN code, or a fingerprint). As explained later on, the seal creation data can be remotely managed (e.g. on a secure server) and there may be more than one persons authorised to activate it in order to create a seal on behalf of an organisation.

4. The seal creation device computes the seal and sends the result to the application that integrates the seal into the document.

At this stage, it is important to note that in general, the seal's certificate is provided with the sealed data. This enables the identification of seal owner and the verification of the seal since the public key is immediately available from the certificate.

The augmentation for more resilience

Augmenting seals is the process by which certain material (e.g. time stamps, validation data and even archival-related material) is incorporated to the seals for making them more resilient to change or for enlarging their longevity.

The augmentation can be done either by the creator of the seal, or by the relying party or by a **TSP that validates or preserve the seal** on behalf of the creator of the seal or the relying party. E.g. if someone asks a company to seal a credit note, it is likely to be the case that the first person has some interest in the preservation of the seal (which is not necessarily the case of the creator of the seal). On the contrary, if the seal is not verified immediately by the relying party, the creator of the seal may have some interest in completing the seal, e.g., with a trusted time stamp in order to provide a trusted evidence of the sealing time. By this way it will be difficult for the relying party to reject the seal in case of a subsequent problem with regard to the seal (e.g. expiration of the sealing certificate).

2.5 Qualified electronic seals

As mentioned above, qualified electronic seals enjoy, all over the EU, the equivalent legal effect of a handwritten seal.

To achieve a QESeal, the eIDAS Regulation requires a qualified seal creation device (i.e. a seal creation device that follows the requirements listed in the eIDAS Regulation and will be certified accordingly).

In addition, the eIDAS Regulation also requires a qualified certificate for electronic seals: the **qualified certificate** follows the requirements listed in the eIDAS Regulation, and the issuing **CA** will be a **qualified trust service provider**. Pursuant to the eIDAS Regulation, the CA will be audited and if the Member State in which the CA is established receives a suitable audit report and verifies the eIDAS requirements, the CA will be listed as qualified trust service provider in the corresponding **national trusted list**.

- **Qualified certificates for electronic seals provides high assurance of the identity of the creator of the seal.** E.g. it will be difficult for a malicious user to get a qualified seal certificate in the name of an Administration or a big company, because the qualified CA will be responsible to check that such seal is issued to the persons representing the Administration or the company and not to unauthorised persons.
- **QSealCDs provide high assurance on the security of the seal,** whether the seal creation data is to be used by one physical person representing the organisation owning the seal, or by more than one authorised persons.

Moreover, the eIDAS Regulation offers the possibility to use **qualified** trust services (QTS) for the **validation** and/or the **preservation** of QESeal. Such services are offered by QTSPs.

There is no obligation to call such QTS for the validation or the preservation of (qualified) seal, but as any other qualified service, their use provides the users with a pretty good legal protection (i.e. in case of litigation the burden of the proof lies on the QTPS).

3. Qualified electronic seal – what key properties does it provide?

3.1 Legal properties

Enjoying the presumption of integrity of the data and of correctness of the origin of that data

As presented above, QESeals benefit from a full legal recognition thanks to the eIDAS regulation.

As a result of the obligations set by the eIDAS Regulation on both the TSP managing them (in particular the CAs) and on the underlying technologies, such electronic seals warrant data integrity, identify the creator of the seal with a high level of certainty, and ensure the correctness of origin of the seal (making it difficult for the creator of the seal to deny having sealed data).

At this stage, it is important to recall that (qualified) electronic **seals are created by legal persons**. Indeed, under the eIDAS Regulation, a natural person is not legally permitted to electronically seal data. Rather, the eIDAS Regulation allows natural persons to electronically sign data. So, as stated by the eIDAS Regulation, when a transaction requires a qualified electronic seal from a legal person, a qualified electronic signature from the authorised representative of the legal person should be equally acceptable.

The concept of electronic signature for natural persons is very similar to the concept of electronic seal for legal persons and is the topic of dedicated security guidelines within this series of documents.

3.2 Security properties

Data integrity

As mentioned in the introduction, the use of public key cryptography to implement QESeal (and AdESeal in general) ensures data integrity (i.e. any change in the sealed data after the seal process is detected).

Data origin authentication

The use of public key cryptography to implement QESeal (and AdESeal in general) warrants the proof of origin of the sealed data since only the person in possession of the private key can be at the point of origin of data sealed with the corresponding public key. For QESeal, in addition, there is a high level of assurance on the identity of the person owning such private key (see below).

3.3 Functional Properties

Non-repudiation of sealing (or correctness of origin)

As mentioned in the introduction, the use of public key cryptography to implement QESeal (and AdESeal in general) provides for non-repudiation of having sealed.

Secure identification of the creator of the seal

The qualified digital certificate ensures the identification of the creator of the seal with a very high level of assurance, due to the controls of the TSP on one hand, but also due to the requirements on the content of the creator of the seal's certificate imposed by the eIDAS Regulation. It shall be noted that the eIDAS Regulation strongly encourages Trust service providers issuing qualified certificates for electronic seals *"to implement the necessary measures in order to be able to establish the identity of the natural person representing the legal person to whom the qualified certificate for the electronic seal is provided"*.

Creating large amount of seals and/or seals on huge data

The involvement of a human being creator of the seal is not always needed when electronically sealing; sealing (it applies to QESeal but more broadly for any type of AdESeal) may be an automated process. E.g. a hospital, may have to seal hundreds of documents per day. To ease his/her life, his/her seal creation device may be implemented on a server where the private key stays activated for several hours; provided the data to be sealed submission process is secure, as well as the access to the server, a perfectly valid seal can be created without the need to enter the director's PIN code for each and every seal applied.

Also, a seal can be applied to data of any type and any size; a contract in a pdf format, e.g. will only require one single electronic seal to ensure the integrity and non-repudiation of the whole file. No need to seal each and every page like in the paper world, by virtue of the data integrity featured by the Public Key Cryptography technology underlying QESeal.

3.4 Other Properties

Sealing with a seal that is understood and verifiable worldwide

Basic seals, like non-qualified AdESeals, benefit from the non-discrimination rule. This means that a Court in an EU Member State cannot reject them automatically as being invalid simply because they are in electronic form. However, their dependability is still lower than that of a QESeal because the creator of the seal may be required to prove the security of the technology being used if the validity of the seal is disputed before a court. This requires significant costs and efforts that could be avoided with relative ease by opting for the more established and standardised advanced and qualified seal solutions. It may also be the case that the relying parties have no applications or tools to validate such seal, when not based on standards; in such a scenario, the seal may be legally valid and technologically robust, but of limited use.

For these **interoperability** reasons, **QESeals** that are based on recognised EU standards **are preferable** unless the parties operate purely in a local context where the acceptance and usability of the chosen seal solution is sufficiently certain.

Beyond the technical interoperability, the eIDAS Regulation also ensures the (international) recognition of electronic seals. See also the "FAQ" on this topic.

Managing sealing at the level of an organisation

As already mentioned, the (qualified) seal creation devices can be configured and managed (potentially by a TSP) in such a way that more than one authorised person is able to seal in the name of an organisation. E.g. the seal creation data can be stored on a secure server that requires the authentication of the authorised persons in order to allow the creation data to compute a seal.

4. Qualified electronic seal – what properties can it not provide?

4.1 Legal properties not provided by QESeals

"Seal" by a natural person

As mentioned above (qualified) electronic seals are performed by legal persons.

It is not possible for a human being to create a (qualified) electronic seal. Rather, they will use another concept introduced by the eIDAS Regulation, namely the **(qualified) electronic signature**.

Granting that the content of the sealed data is meaningful, fair or true

Exactly like in the paper world, it is not because a data (e.g. an invoice) is sealed that the content (e.g. figures in the invoice) are correct or fair.

4.2 Security properties not provided by QESeal

Confidentiality

The seal protocol used alone does not provide confidentiality, although the Public Key Cryptography can be used to offer encryption. Indeed, if the seal process presented above is reverted (i.e. someone is using the public key of a recipient to encrypt a text), then only the recipient that owns the correspondent private key can decrypt the text.

Like for electronic seal, a certificate attesting the link between the recipient and its key pair is to be provided by a TSP (i.e. a CA).

One needs to superpose the two protocols to achieve electronic seal and confidentiality. First the creator of the seal seals and then (s)he may encrypt the sealed document to the attention of a recipient, provided (s)he has the encryption certificate of this person. If the sealed document needs to be sent to many recipients, then the encryption protocol needs to be repeated as many times as there are recipients.

4.3 Functional properties not offered by QESeal

Time stamping

Although the technique underlying the (Q)ES can be used by a special sort of "creator of the seal" (i.e. a time stamping authority), a QESeal does not provide any proof on the sealing time; unless a trusted timestamp is added to the seal (see below), the time that is appended to a QESeal is a self-declaration from the creator of the seal and not an official proof.

4.4 Other properties not offered by QESeal

Eternal integrity

There is no guarantee that the content of the sealed document cannot be changed if (long term) preservation features are not implemented (see BASIC / RECOMMENED / ENANCED below).

5. Qualified electronic seal – what are the potential use cases?

5.1 Overview and context of the given examples

In general, and to put qualified electronic seals into context, they only provide seals. As mentioned above, they do not establish the exact time on when the document was sealed, they do not ensure the meaningfulness of the sealed contend, and they do not confirm delivery of the sealed message. Hence, qualified electronic seals (QESeal) are most often seen coming in addition to other identification and/or trust services as part of a broader solution.

In this context, and although the properties of QESeal have been described in the previous sections, the following properties are key for the use case examples mentioned below:

- QESeal to establish the origin of a sealed document (and support the non-repudiation of having sealed document).
- QESeal to provide integrity of a sealed document.

Those properties allow several “types of use cases” which can be applied in many areas of application as show in the present section. The table below highlight the identified types of use cases. The mapping on areas of applications in no way tries to be exhaustive but only tries to indicate the huge potential of QESeal.

	C2C	C2B C2G	B2B	B2G B2A	G2G A2A
Sealing a document/message to confirm origin	●	●●	●●	●●	●●
Sealing data or evidences to preserve them		●●	●●	●	●
Sealing of a document/ declaration	●	●●	●●	●●	
Sealing of an official document /attestation					●●
Sealing of a legal consent / eMandate	●●	●●	●●	●●	

Table 2: QESeal application areas

5.2 Sealing a document/message to confirm origin

A first and often forgotten use case is (even if a QESeal might be considered excessive due to its qualified status) is simply to apply seals on documents and messages to give proof of origin and integrity. Indeed, in the days of phishing it is for many people very difficult to see if a document or a message really originates from where it seems to come from. Applying qualified electronic seals on documents/messages can easily and swiftly provide a solution for this.

Examples of concrete application are:

- B2B: Organisations can easily introduce as practice to start sealing, with QESeal, all their outgoing documents and messages and also validate incoming messages/documents.
- G2C: Governments should make it a standard to have outgoing documents/messages either using qualified electronic seals.

5.3 Sealing data or evidences to preserve them

Sealing data guarantees the integrity of this data. With a QESeal there is an automatic presumption of integrity. With the increasing amount of electronic data, and the increasing possibility to forge such data, it may be of great interest to seal evidences like proofs of payment, of purchase, etc.

Examples of concrete application are:

- B2G: the tax Administration may control companies with regards to the past years activities. More and more evidences are now in electronic form. It is interesting to seal them in order to be able to prove their genuineness.
- B2all – G2all: more and more applications are dematerialised. In case of litigation, the log files of the transactions may be analysed. However, it might be necessary to be able to prove that these files have not been tampered with to the advantage of the application provider. Sealing such files is a pretty elegant solution to do so thanks to the legal recognition of the integrity.

5.4 Sealing of a document/declaration

Organisations can use QESeal to seal documents/declarations when submitting them e.g. to government as proof of their authenticity/origin. This provides a significant amount of time as, in contrast to filling in forms and/or putting things on paper, people can now prepare their declaration fully electronically sealed (with QESeal) and

submit them in one single digital flow.

Examples of concrete application are:

- B2G: Submitting declarations to government (which needs to be sealed by the organisation).

5.5 Sealing of an official document/attestation

Certain government documents have to be sealed. In the day and age of qualified electronic seals, it is no longer needed to do all this on paper. Administrations can (depending on the specific form factors obliged by law) generate official documents/attestations and seal them electronically.

Examples of concrete application are:

- G2C: Creation/sealing of e-permits or an attestation of residence.
- G2B: Creation/sealing of VAT-attestations, sealing of custom documents, etc.
- B2C: hospital sealing invoices or attestations for patients (this case is illustrated in section 7).

5.6 Sealing of a contract

The number of cases in which contracts are being concluded between parties is very large. Such processes could be accelerated and rendered much more efficient if they could be digitized and supported by electronic seals ensuring legal certainty and equivalence to hand written seals. This is exactly what a qualified electronic seal now allows. Parties can seal contracts and exchange them 24/7 and across borders in Europe whilst being certain of the legal recognition of the electronic seals.

Examples of concrete application are:

- C2B: A person sealing a rental or buying agreement.
- B2B: A company subscribing to an insurance contract.
- B2G: Sealing off for a government project-start.

6. Qualified electronic seal – what are the usage best practices?

6.1 Security Guidelines & Levels

In this section, we propose recommendations, through existing best practices, according to three levels which represent the "strength/rigorousness" with which qualified electronic seal services should be applied in a specific context. This "strength/rigorousness" of course depends on the use case or type of application / environment in which qualified electronic seal services are being applied. Dimensions that could have an impact on the "strength/rigorousness" of applying the recommendations, are the criticality of the processes and/or data being involved in the business process which is being supported by the respective qualified trust service. This, every organization has to determine for itself based on a risk assessment. For inspiration possible mapping of basic/recommended/enhanced vs business criticality and/or data protection is being given in Annex B.

In short the three levels of recommendations are in increasing order (whereby the higher level suppose that the lower level is also taken into account):

BASIC for recommendations to be followed by entities or in processes dealing with normal levels of criticality of data and therefor can live with a lower maturity in implementing trust services (technology).

RECOMMENDED for recommendations to be followed by entities or in processes dealing with important business data and therefor need to be able to rely on a medium to higher maturity of implementation of trust services (technology).

ENHANCED for recommendations to be followed by entities or in processes dealing with data of sensitive/high level of criticality and therefor need to be able to rely on a (very) high maturity of implementation of trust services (technology).

6.2 BASIC

When looking for trust services, selecting qualified services ensures benefiting from a high level of security and legal certainty of trust services. Qualified electronic seals enjoy, all over the EU, the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

As a basic recommendation, both the creator of the seal and the relying party should look for the EU trust mark for qualified trust services when selecting providers. In addition, the relying party shall follow the applicable CA's terms and conditions[10] and/or other contractual documentation.

Such documentation may be accessible via the certificate itself: e.g. a PKI Disclosure Statement (PDS), that is an instrument of disclosure and notice by a TSP, can be found from a link present in the creator of the

[10] Essentially Certification Practice Statement (CPS) and Certificate Policies (CP)

seal's certificate in all certificates issued by CAs conforming to the ETSI standards designed to support the eIDAS Regulation (see [2]). In general, the CA will ask the relying party to validate the revocation status of the certificate against its validation status information services (also accessible from links provided within the certificates). It is important to note that most applications available on the market perform such validation automatically. In particular, to comply with best practices and with the eIDAS requirement for the validation of qualified electronic seals (article 32) that request the confirmation that the certificate was valid at the time of sealing.

As a fundamental recommendation, the creator of the seal shall never share its seal activation data (e.g. PIN number).

6.3 RECOMMENDED

Augmenting seals is the process by which certain material (e.g. time stamps, validation data and even archival-related material) is incorporated to the seals for making them more resilient to change or for enlarging their longevity. Indeed, when the seal needs to be validated after its creation it is necessary to check, e.g., that the certificate was not revoked at the time of the seal. If a revocation occurred between the time of the seal and the time of validation, the verifier needs to be sure that the seal was created BEFORE that time of revocation. The augmentation can be done either by the creator of the seal, or by the relying party or by a TSP that validates or preserve the seal on behalf of the creator of the seal or the relying party. E.g. if someone asks a company to seal a credit note, it is likely to be the case that the first person has some interest in the preservation of the seal (which is not necessarily the case of the creator of the seal). On the contrary, if the seal is not verified immediately by the relying party, the creator of the seal may have some interest in completing the seal, e.g., with a trusted time stamp in order to provide a trusted evidence of the sealing time. By this way it will be difficult for the relying party to reject the seal in case of a subsequent problem with regard to the seal (e.g. expiration of the sealing certificate).

It is recommended that the first level of augmentation consists in time-stamping the seal.

Typically, the date of sealing will be indicated in the sealed document, at least if this plays a role in its legal value or legal meaning but this may not be sufficient. For electronic documents, time stamping is a possibility to avoid risks of tampering. An **electronic time stamp** is a data in electronic form which binds other electronic data to a particular time establishing evidence that this data existed at that time. Time stamping the seal provides the proof that it was created before the date indicated in the electronic time stamp. This allows the verifier to position the date of the creation with regard to the date of a possible revocation. This is not a condition sine qua non, but implementing it will remove a risk, support validation, and enhance legal certainty.

In a seal with Long-Term Validation Data, the set of validation material or references to it is sufficient to ascertain the validation status of all end-entity certificates (sealer certificate, time stamps certificates, attribute certificates, etc.) contained in the seal.

There can be more elements than necessary and can also be fewer elements than necessary if it is expected that recipients have an alternative mean of obtaining relevant proofs of existence on these elements.

Before algorithms, keys, and other cryptographic data used at the time a seal was built become weak and the cryptographic functions become vulnerable, or the certificates supporting previous time stamp

tokens expire or are revoked, the sealed data, the seal as well as any additional information should be protected by applying time stamp tokens.

Such additional time stamp tokens are called archive validation data. The time stamping process should be repeated in time before the protection provided by a previous time stamp token becomes weak and should make use of stronger algorithms or longer key lengths than those that have been used in the original seals or time stamp tokens. These evidences added to the seal are often called Long-Term Validation Data.

6.4 ENHANCED

It is recommended that QESeal is further supported by ancillary qualified trust services.

Either for the simple validating of the QESeal, but also for its augmentation according to the term of preservation, it is possible to request the support of qualified services:

- **qualified timestamps** (as defined in Article 42 of the eIDAS Regulation)
- **qualified validation of QESeal** (as defined in Article 40 of the eIDAS Regulation)
- **qualified preservation of QESeal** (as defined in Article 40 of the eIDAS Regulation).

The way to verify that the provider is duly qualified is to check its presence in the trusted list of the Member State where it operates. The presence of the EU trust mark for qualified trust services on the CPS web site or folders is also a good indicator.

There is no obligation to call such QTS for the validation or the preservation of seal, but as any other Qualified Service, their use provide the users with a pretty good legal protection (i.e. in case of litigation the burden of the proof lies on the QTPS).

Note: Importance of evidences and proofs in case of disputes

In case of a dispute over an electronic seal message, one needs to look at all available evidences in order to validate the seal and resolve the dispute.

The issues of the dispute may for example be that owner of the seal denies having performed the seal at all, or that the sealer acknowledges having performed the seal, but for a different message, etc. Most of the technical **evidence can be found in the sealed message and in documents** that it refers to, such as the certificate, the certification practices statement published by the CA (CPS) and the possibly used seal policy, as described below. However, it should be noted that the seal may also require evidence of the context in which the seal was created. For example, regardless of all technical evidence, the creator of the seal may still have been deceived or forced by violence to seal, or the creator of the seal may not have understood the document (e.g. it needs to be established that the document was written in a language understandable to the sealer).

Evidence present in the seal

Digital seals generally bear with them a series of pieces of evidence, provided they are correctly formatted (the reader may read CEN 419 040 for more detailed info). E.g. an unambiguous reference to the sealer’s certificate (the certificate itself or a reference to it), a time stamp and a certificate status information that proves that the certificate was valid at the claimed time of seal-creation, etc. The seal may also contain:

- A commitment type, indicating the purpose of the seal
- A location indicator, specifying the claimed location of the seal process,
- A reference to the Sealing Policy under which the seal is to be validated (see below)

The qualified certificate contains the following additional pieces of evidence:

- a reference to the Certificate Policy and/or Certificate Practice Statement followed by the CA when issuing the certificate (amongst other describing the security procedures for the CA, for example relating to the protection of the sealing key of the CA, the registration of the creator of the seal, etc.);
- different information to enquire about the validity status of the certificate (links toward Online Certification Status Protocol (OCSP), blacklist of certificates (CRLs)), the period of validity of the certificate, a link toward the CA certificate, a claim that the private key is located in a qualified electronic seal creation device).

Optionally, the certificate may also contain:

- limitations on the scope of use of the certificate, if applicable;
- limits on the value of transactions for which the certificate can be used, if applicable.

Evidence through a Sealing Policy

A sealing policy is a set of rules for the creation and validation of an electronic seal, under which the seal can be determined to be valid (see [3] and bibliography (b)as these considerations are not in the scope of the eIDAS Regulation). A given legal/contractual context may recognise a particular seal policy as meeting its requirements. An example of seal policy is the “evidence agreement” through which Parties agree to accept the validity of seal type X to seal transactions. This is typically included in terms and conditions of online banking application.

A seal policy may be issued, for example, by a party relying on the electronic seals and selected by the sealer for use with that relying party. Alternatively, a seal policy may be established through an electronic trading association for use amongst its members. Both the sealer and verifier use the same seal policy.

A seal policy may be implicit or explicit. The seal policy may be provided as part of the sealed document, out of band, or by other means. The seal policy may be explicitly identified or may be implied by the semantics of the data being sealed and/or other external data, like a contract being referenced which itself refers to a seal policy, as well as by the sealing context. An explicit seal policy for open usage has a globally unique reference, which is bound to an electronic seal by the sealer as part of the seal calculation.

The seal policy may include the following:

- rules for certification path construction/verification (including indication of trusted root certificates to be used)
- rules for use of revocation status information (e.g. CRLs or OCSP responses);
- rules for use of timing information, time-marking and/or time stamping;
- seal validation data to be provided by the sealer;
- seal validation data to be collected by the verifier.

- the period during which seals can be performed under that policy,
- a list of recognised commitment types;
- rules for the use of sealer roles;
- any constraints on seal algorithms and key lengths;
- other seal policy rules required to meet the objectives of the seal.
- rules for multiple seals or seals and signatures:
  - for documents sealed by multiple sealers/signatories, it may be necessary to establish the order of sealing/signing, and if all sealers/ signatories were present at the same place.
  - the seal policy should provide guidance on the actions to take (both at creation and verification sides), if one or more of the seal(s)/signature(s) are not valid, etc.

Additional evidence that may be required:

- Place of sealing. In some contractual situations this is of importance, and may have to be proven.
- Legal system to be applicable for the sealed document.

7. Qualified electronic seals – example of tools & practical usage aspects

7.1 Implementing qualified electronic seals (user perspective)

Seal creation tools

As mentioned previously, for creating a QESeal, the creator of the seal needs (access to):

- a qualified seal certificate,
- a qualified seal creation device (QSealCD) protecting the private key and enabling the seal creation process (e.g. cryptographic computation),
- a seal creation application managing the seal creation process (e.g. preparing the data to be sealed, allowing the creator of the seal to use the QSCD, to enter the PIN, to select the certificate and other seal creation parameters when applicable).

The creator of the seal does not need to have all these elements in hand. A (Q)TSP may manage (some of) them on his/her behalf. The strict minimum is that the creator of the seal must be able to control the activation of the private key.

Qualified certificate

Very probably, the first stakeholder that the creator of the seal will meet in the framework of electronic seal will be the CSP.

Arguments for choice: a certificate service provider that also manages the signature key on behalf of the seal owner (see below) may be interesting when the seal is to be used by more than one authorised persons representing the sealing organisation.

Qualified seal creation device

With regard to the QSCD, the creator of the seal may opt for a device that can be used within his/her own environment, or remotely managed by a TSP. When the QSCD is managed by a TSP, the device and the TSP must be qualified. The way to verify that the provider is duly qualified is to check its presence in the trusted list of the member state where it is established. The way to verify that the device is duly qualified is to check its presence in the **EC list of certified devices**.

Arguments for choice: in the first case, the control by the creator of the seal is higher, in the second case, the mobility is enhanced. If the device is to be shared by more than one physical person (i.e. when more than one person have the ability to seal in the name of the organisation to which the seal belongs), having a remote device might be an easier solution.

Seal creation application

There is no regulatory requirement on seal creation application. There are a variety of ways to implement the seal creation.

On the one hand, the seal can be entirely performed within the creator of the seal's environment; the creator of the seal holds his/her seal creation device and seals with an application residing on his computer. Quite a commonly used creation device is the smart card.

Example: a typical use case is the representative of a SME that seals a pdf invoice on his/her computer.

The creator of the seal may seal using his/her qualified seal creation device (e.g. eID) to create a QESeal on a data (e.g. a PDF, a form) prepared by a server.

Example: a typical use case is the seal of a form, prepared by an Administration on its servers, possibly completed online by the SME, and whose fingerprint is locally sealed by the representative of a SME on his/her computer.

On the other hand, the creator of the seal may rely on remote seal creation devices and facilities. It is possible to delegate a more or less important part of the seal creation process to a TSP. The strict minimum is that the creator of the seal must be able to control the activation of the private key. For this purpose, the creator of the seal must have the sole control on the authentication to her/his key. All the rest, even including the management of the private key (generation, storage), may be delegated to a TSP and implemented through a private key container. In this scenario interesting from a user friendliness perspective (the mobility is increased since the authentication towards the TSP may be limited to few components (e.g. a mobile phone)), it is possible to allow more than one person to create a seal.

However, the seal owner needs to trust the TSP for the sound protection of the private key when this one is managed by the TSP. Thanks to the eIDAS Regulation, with regards to QESeal, the seal creation device must be qualified (QSealCD) and the TSP managing the private key(s) must be qualified (QTSP) and will be supervised as part of the QSealCD certification.

Example: a typical use case is the seal of hospital attestations. There may be several geographical sites, each one with a director with a sealing power. The key is on a central server managed by TSP and the "empty" forms are also available from the TSP's site. Each director prepares the attestation by filling the form on line and then can create a seal. When the info is ready to be sealed, a SMS containing a challenge is sent to the director's phone and he just needs to copy the challenge via the apps to be authenticated; this allows the central server to activate and use the hospital private key to seal the form. The authentication is considered as a strong authentication since the mobile phone communications are secure and the mobile phone is supposed to be under the sole control of its owner. A variant of this example is the use of the mobile phone for the authentication only, while the data to be sealed preparation and the reception of the challenge occur via a web interface on the user laptop; this a bit more secure since two distinct channels are used to convey the information (the laptop and the internet, on the one hand, the mobile phone and the GPRS connection on the other hand).

Arguments for choice: When holding private keys, "in hands" the control by the creator of the seal is higher. When using remote seal creation facilities and devices, the mobility is enhanced and the sharing of the seal creation data is easier (with a device "in hand" the device needs to be passed from one person to another).

Augmentation and preservation tools

As stated previously, for any type of AdESeal, where the seal is not verified immediately by the relying party, the creator of the seal (or relying party) may have some interest in completing the seal with a trusted time stamp in order to provide a trusted evidence of the sealing time. By this way it will be difficult for the relying party to reject the seal in case of a subsequent problem with regard to the seal (e.g. expiration of the sealing certificate). Time stamping is not mandatory; it depends on the needs of the relying party to be protected against potential repudiation of the seal by the creator of the seal. Other events may also affect the possibility to (re)validate the seal; e.g. the revocation of another certificate linked to the creator of the seal certificate (e.g. the CA certificate), the end of availability of information on the certificate status by the CSP, etc. Hence, the seal should also be further enhanced with adequate proofs and evidence by the relying party to overcome such events.

Concretely, the creator of the seal (or relying party) may need to use an application that is able to:

- Request time stamps from a time stamp service provider and to integrate the time stamp within the seal. Generally, time stamping is a paying service that the creator of the seal needs to buy on-the-fly or needs to pay in advance.
- Collect the required validation evidences and correctly format the seal according to the terms of preservation.

The creator of the seal (or relying party) may use the services of a TSP to do so. When the seal creation application is provided in a remote way by a TSP, the service generally covers the augmentation and preservation aspects. The TSP may further enhance the offering with storage (archiving) services.

Validation tools

The validation application needs to execute the validation process of a qualified electronic seal as provisioned in Article 32 of the eIDAS Regulation. On top of the strictly cryptographic validation that the digital seal is technically valid, the application must enable the relying party to validate the fact that the seal is a QESeal: among other that the creator of the seal's certificate was issued by a QTSP, that the certificate was both qualified and valid at the time of sealing, the seal creation device is a QSCD, the creator of the seal's data are correctly presented to the relying party, etc. Validations tools should consequently be able to consume the EU MS national **trusted lists** to verify the qualified status of a QTSP/QTS.

For this purpose, the verifier may use an off-the shelf application, or can make use of the services from a TSP that will perform the validation for him. In that latter case, the use of QTSP providing qualified validation services of QESeal will bring more confidence and assurance to the verifier that the validation process is correctly executed as the QTSP and the qualified services it provides will be under supervision for meeting the eIDAS Regulation requirements.

7.2 Relevant standards regarding qualified electronic seals (expert perspective)

Seal formats

When an organisation (e.g. administration, SME) decides to develop its own seal creation application (whether to deploy it on its users environment or to offer it as a central service), the first recommendation is to use standard and recognised seal formats, namely those referred to by CID (EU) 2015/1506 pursuant to Article 27 of the eIDAS Regulation).

Such standards are defined in ETSI TS 103 171 v.2.1.1. (XAdES Baseline Profile), ETSI TS 103 173 v.2.2.1. (CAdES Baseline Profile), ETSI TS 103 172 v.2.2.2. (PAdES Baseline Profile) and ETSI TS 103 174 v2.2.1 (Associated Signature Container Baseline Profile). It is important to note that these norms specifies "digital signatures", the technology underlying electronic seals and electronic signatures, indifferently. The terminology "seal", which is a legal concept is barely used in these documents addressing "digital signature".

These standards support different formats and forms of signatures, suitable for different terms of preservation (until very long term). Implementers are recommended, whenever possible, to use the most advanced forms allowing for best guarantees not only for long term, but also in case of many types of security breaches that might occur in the mid-term as well.

Newer versions of those standards are also available respectively as EN 319 122/132/142/162 series (see ETSI TR 119 000[11] for further guidance).

Specific implementations

When specific implementations are in place, e.g. for mass sealing, they shall ensure:

- that no data can be introduced in the flow of data to be sealed (network and application protection required);
- that the user is aware that more than one document is to be sealed that the data to be sealed are correctly "displayed".

EC funded DSS Open source libraries

With regards to off-the-shelf toolkits allowing more integrated solutions, the EC funded the development of the DSS toolkits, as part of the **CEF eSignature building block**, available from Join-up where a cookbook is also made available for use and integration of such toolkits for the creation and validation of QESeal.[12]

Policies and security requirements for applications for seal creation and seal validation

ETSI TS 119 101 provides general security and policy requirements for applications for seal creation, validation and augmentation. The document covers legal driven policy requirements, information security (management system) requirements, seal creation, seal validation and seal augmentation processes requirements, development and coding policy requirements and additional general requirements. Protection Profiles (PP) for seal creation applications and seal validation applications are out of scope and are defined in the CEN EN 419 111 standard "Protection Profiles for Seal Creation & Validation Applications".

An important tool for relying Parties is the **ETSI TS 119 172** [3] series on signature policies. This series of standards allows the definition and specifications of the rules to be applied during creation, augmentation and/or validation of seals, and how to fix the parameters for declaring a seal conformant to the specified rules.

[11] ETSI TR 119 000 V1.2.1 (2016-04): "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview".

[12] EC funded eSignature's DSS has been published on both JoinUp and the CEF Digital Portal, issues are handled via the DSS JIRA. All future releases and issue management will be available through the CEF Digital portal.

Annex A - Glossary

A.1 eIDAS – What is it?

eIDAS is the acronym used to refer to Regulation (EU) No 910/2014 on electronic identification (eID) and trust services for electronic transactions in the internal market. The eIDAS Regulation is about trust, seamless user experience and convenience in online cross-border transactions.

A.2 Hash value (of a file)

A hash value is a standardised and unique summary of a message, which is obtained by applying a specific cryptographic tool called a cryptographic hash function.

A hash function is any function that can be used to map digital data of arbitrary size to digital data of fixed size, with slight differences in input data producing very big differences in output data.

A cryptographic hash function is a hash function which has specific security properties:

- It is considered practically impossible to recreate the input message from its hash value;
- It is considered practically impossible to compute from a specific message a second message that has the same hash value (i.e. different messages lead to different hash values);
- It is considered practically impossible to find two different messages that would lead to the same hash value (no collisions)

With such properties, when applied to the same message repetitively the hash value is always the same, while if the message is slightly modified (even by one single bit) the hash value will always be different. That allows to verify the integrity of a message compared to the message on which the hash was previously computed; when the hash values are identical, then the messages are identical.

As cryptographic hash values represent large amounts of data as much smaller numeric values, they are often used with digital signatures. Signing a hash value is more efficient than signing the larger value.

A.3 Intellectual property

Intellectual property is the collective term for rights to intellectual creations such as books, music, trademarks, designs, inventions, software, texts and photographs. A single creation may be protected by multiple rights at the same time. The best-known intellectual property rights are trademark rights, copyrights and patent rights.

A.4 Trusted list

A trusted list is a list including information related to the qualified trust service providers which are established in and supervised by an EU Member State, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014. Those lists have constitutive value and are primary source of information to validate that a qualified status is or has been granted to a QTSP and to the QTS it provides.

Trusted lists are essential elements in building trust among electronic market operators by allowing users to determine the qualified status and the status history of trust service providers and their services.

Member States may include in the trusted lists information on non-qualified trust service providers, together with information related to the non-qualified trust services provided by them. It shall be clearly indicated that they are not qualified according to Regulation (EU) No 910/2014.

Member States may include in the trusted lists information on nationally defined trust services of other types than those defined under Article 3(16) of Regulation (EU) No 910/2014. It shall be clearly indicated that they are not qualified according to Regulation (EU) No 910/2014.

A.5 QTSP/QTS requirements and obligations

The eIDAS Regulation (EU) No 910/2014 foresees a set of requirements and obligations for qualified trust service providers (QTSP) and qualified trust services (QTS) they provide in order to ensure high-level security of the qualified trust services. Those obligations include in a nutshell:

- **Processing of personal data** shall be carried out in accordance with Directive 95/46/EC.
- Trust service provider (TSP) is liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation, while the **intention or negligence of a QTSP shall be presumed**, unless proven otherwise by QTS. When TSP informed customer in advance on limitations on the use of their services, and when such limitations are recognisable to third parties, TSP is not liable when limitations have been exceeded.
- Where feasible, services must be **accessible for person with disabilities**.
- **Implementing appropriate technical and organisational measures to manage the risks** posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. Measures shall be taken to prevent and minimize the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.
- Very strict rules regarding the obligation of **notifying security & personal data breaches**.
- **Additional requirements on QTSP operations and practices**:
    - Inform SB of any change in QTS provisioning and of intention to cease;
    - Up-to-date termination plan, agreed with the competent supervisory body (SB), to ensure continuity of service;
    - Requirements on employed staff and subcontractors, when used;
    - Sufficient financial resources and/or liability insurance, in accordance with national law;
    - Consumer information on terms and conditions, incl. on limitations on use;
    - Use of trustworthy systems and products ensuring the technical security and reliability of the supported processes;
    - Use of trustworthy systems to store (personal) data in a verifiable form;
    - Take appropriate measures against forgery and theft of data; and
    - Record and keep accessible activities related data, issued and received, even after cessation of activities.
- **Specific requirements** from the provisions laid down in the eIDAS Regulation with regards to the provision of a specific type of qualified trust service.

All those requirements must be met by the QTSP/QTS before issuing the very first qualified trust service output, i.e. before issuing the very first qualified time stamp in the case of QTSP providing qualified time stamping services.

Once granted a qualified status, the eIDAS Regulation also foresees an active supervision scheme of qualified trust service providers (QTSP) and qualified trust services (QTS) they provide by the national competent supervisory body (SB) to monitor fulfilment of the QTSP/QTS requirements and obligations throughout their lifetime.

A.6 CEF eSignature building blocks

The Connecting Europe Facility[13] (CEF) supports trans- European networks and infrastructures in the sectors of transport, telecommunications and energy. It provides public administrations and businesses of reusable building blocks. Building blocks supported so far include: eIdentification; eSignature; eInvoicing; eDelivery; and Automated Translation.

The eSignature building block helps public administrations and businesses to accelerate the creation and verification of electronic signatures. The deployment of this building block in a Member State facilitates the mutual recognition and cross-border interoperability of eSignatures, so that the legal value of electronic documents can be recognized in other countries than the country of origin of the signer. This means that public administrations and businesses can trust and use eSignatures that are valid and structured in EU interoperable formats[14,15].

The CEF eSignature solution[16] consists of open source advisory services (Libraries, including source code, artefacts, bundle for demonstration and cookbook) managed by the European Commission allowing the creation and verification of electronic signatures, including the use of time stamps.

For more information about these services, please refer to the Digital Signature Service available from https://joinup.ec.europa.eu/asset/sd-dss/home.

A.7 Trust services defined by the eIDAS Regulation

In its Art.3.16, the eIDAS Regulation defines a 'trust service' as an electronic service normally provided for remuneration which consists of:

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

(b) the creation, verification and validation of certificates for website authentication; or

(c) the preservation of electronic signatures, seals or certificates related to those services.

A.8 Qualified trust services defined by the eIDAS Regulation

Only those trust services listed in Art.3.16 of the eIDAS Regulation for which there are applicable requirements in the Regulation can benefit from the qualified status. eIDAS regulates the following nine qualified trust services:

1. **The provision of qualified certificates for electronic signatures**

[13] https://ec.europa.eu/digital-single-market/connecting-europe-facility.

[14] CID (EU) 2011/130 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC on services in the internal market.

[15] CID (EU) 2015/1506 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 on eID and trust services for electronic transactions in the internal market.

[16] https://joinup.ec.europa.eu/community/cef/og_page/catalogue-building-blocks#eSignature.

Certificates for electronic signature are electronic attestations which link electronic signature validation data to a natural person and confirm at least the name or the pseudonym of that person. Since 1 July 2016, an electronic signature can only be used by a natural person to sign, i.e. mainly to express consent on the signed data/document. This represents a significant difference from the eSignature Directive 1999/93/EC regime where an electronic signature, which could be used by legal persons, was defined as a means of authentication. Under the eIDAS Regulation, the entity who creates an electronic signature (the so called signatory) will be a natural person. Therefore, certificates for electronic signature cannot be issued to legal persons anymore. Instead legal persons can use certificates for electronic seals (see below).

A qualified electronic certificate for electronic signatures is an essential element for a signatory to create qualified electronic signatures that shall have the equivalent legal effect of a handwritten signature all over the EU.

2. The provision of qualified certificates for electronic seals

As explained above, since 1 July 2016, legal persons cannot create legally valid (qualified) electronic signatures anymore and cannot be issued (qualified) certificates for electronic signatures. Instead legal persons can use certificates for electronic seals, which are electronic attestations that link electronic seal validation data to a legal person and confirm the name of that person. The aim of an electronic seal is not to sign but to serve as an evidence that an electronic data/document was issued by a legal person, ensuring certainty of the data/document's origin and integrity.

A qualified electronic certificate for electronic seals is an essential element for a legal person to create qualified electronic seals that shall enjoy, all over the EU, the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

3. The provision of qualified certificates for website authentication

Certificates for website authentication are issued to ensure the users (in particular citizens and SMEs) that behind the website there is a legal or natural person identifiable by trustworthy information.

The Regulation sets clear requirements for qualified website authentication certificates to be considered trustworthy together with obligations for qualified trust service providers of such qualified certificates with regard to the security of their operations, their liability and their 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 qualified authenticated websites and technological neutrality of services and solutions.

4. Qualified preservation service for qualified electronic signatures

Such a qualified trust service aims to ensure the long-term preservation of information, in order to ensure the legal validity and trustworthiness of qualified electronic signatures over extended periods of time and guarantee that they can be validated irrespective of future technological changes.

5. Qualified preservation service for qualified electronic seals

Such a qualified trust service aims to ensure the long-term preservation of information, in order to ensure the legal validity and trustworthiness of qualified electronic seals over extended periods of time and guarantee that they can be validated irrespective of future technological changes.

6. **Qualified validation service for qualified electronic signatures**

   Validation of electronic signature is an ancillary service to electronic signatures whose process aims to confirm the validity of an electronic signature.
   Qualified validation services for qualified electronic signatures entail the verification by a qualified trust service provider that the requirements of the eIDAS Regulation are met by a qualified electronic signature in order to confirm its validity.

7. **Qualified validation service for qualified electronic seals**

   Validation of electronic seal is an ancillary service to electronic seals whose process aims to confirm the validity of an electronic seal.
   Qualified validation services for qualified electronic seals entail the verification by a qualified trust service provider that the requirements of the eIDAS Regulation are met by a qualified electronic seal in order to confirm its validity.

8. **Qualified electronic time stamps services**

   Electronic time stamps are issued to ensure the correctness of the time linked to data/documents. Qualified electronic time stamp shall enjoy, all over the EU, the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.

9. **Qualified electronic registered delivery services**

   By relying on a qualified electronic registered delivery service, one will benefit, all over the EU, from the presumption of the integrity of the registered data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by that qualified trust service.

The Regulation sets clear requirements for all such qualified trust services to be considered trustworthy together with obligations for their qualified trust service providers with regard to the security of their operations, their liability and their supervision regime.

A.9 Other terms

Advanced electronic signature as per eIDAS Regulation: means an electronic seal which meets the requirements set out in Article 26.

Browser: short of web browser, is a software application used to locate and display web pages.

Certificate (for electronic seal): as per eIDAS Regulation: means an electronic attestation which links (electronic seal) validation data to a natural person and confirms at least the name or the pseudonym of that person.

Certification Authority (CA): authority trusted by one or more users to create and assign certificates.

Cryptography: the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, and authentication of origin.

Digital certificate: A certificate identifying a public key to its subscriber, corresponding to a private key held by the subscriber. It´s a unique code that typically is used to allow the authenticity and integrity of communication can be verified.

EC list of certified devices as per eIDAS Regulation: list of QSCD as defined in Article 31trs.

Electronic seal creation data as per eIDAS Regulation: *"a unique data which is used by the creator of the seal to create an electronic seal"*.

Electronic seal: "*data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the creator of the seal to seal*".

Electronic time stamp as per eIDAS Regulation: means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.

Encryption algorithm: a set of mathematically rules for encoding information, making unintelligible to those who do not have the algorithm decoding key.

Encryption: the use of algorithms to encode data in order to render a message, or other file, readable only for the intended recipient.

EU trust mark for qualified trust services: as per eIDAS Regulation article 23: the way to indicate in a simple, recognisable and clear manner the qualified trust services they provide

Correctness of origin (or non-repudiation of a seal): (a seal for which) the (creator of the seal) cannot deny to be at the origin of such seal.

Protocol: a set of instructions required to initiate and maintain communication between sender and receiver devices.

Public Key Infrastructure (PKI): A PKI is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of digital certificates issued by a certificate authority (CA).

Qualified electronic seal as per eIDAS Regulation: means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seals.

Qualified electronic time stamp as per eIDAS Regulation: means an electronic time stamp which meets the requirements laid down in Article 42.

Qualified seal creation device as per eIDAS Regulation: means an electronic seal creation device that meets the requirements laid down in Annex II of the Regulation.

Qualified trust service provider as per eIDAS Regulation: means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body.

Registration Authority (RA): entity that is responsible for identification and authentication of subjects of certificates mainly.

Revocation status: the indication on the validity status of a certificate. It can take different values, typically; 'valid', 'revoked' 'on hold' or 'indeterminate' (revoked is the state of a certificate that has lost its validity).

Creator of the seal as per eIDAS Regulation: means a natural person who creates an electronic seal.

Seal creation data as per eIDAS Regulation: means unique data which is used by the creator of the seal to create an electronic seal.

Seal creation device as per eIDAS Regulation: "*a configured software or hardware used to create an electronic seal*.

Seal preservation as per eIDAS Regulation: procedures and technologies capable of extending the trustworthiness of the (qualified) electronic seal beyond the technological validity period.

Seal validation as per eIDAS Regulation: means the process of verifying and confirming that an electronic seal or a seal is valid.

Supervisory body as per eIDAS Regulation: an organisation that carries out the supervisory activities under this Regulation.

Trust service provider (TSP) as per eIDAS Regulation: means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider.

Validation services as per eIDAS Regulation: a service that allows relying parties to receive the result of the validation process.

A.10 Acronyms

Acronyms	Description
A2A	Administration to Administration
AdESeal	Advanced electronic seal
B2A	Business to Administration
B2B	Business to Business
B2C	Business to Consumer
B2G	Business to Government
C2B	Consumer to Business
C2C	Consumer to Consumer
C2G	Consumer to Government
CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
CEN	Centre Européen de Normalisation
eID	electronic Identification

Acronyms	Description
EN	European standard
ETSI	European Telecommunications Standardisation Institute
EU	European Union
G2G	Government to Government
GMST	Greenwich Mean Sidereal Time
GMT	Greenwich Mean Time
HTTP	Hyper Text Transport Protocol
HTTPS	HTTP Secure
IETF	Internet Engineering Task Force
MS	Member State
PKI	Public Key Infrastructure
Q&A	Questions and Answers
QeDel	Qualified Electronic Delivery Service
QESeal	Qualified Electronic Seal
QSealCD	Qualified seal creation device
QTS	Qualified Trust Service
QTS	Qualified trust service
QTSP	Qualified Trust Service Provider
QTSP/QTS	Qualified Trust Service Provider and the Qualified Trust Service it provides
QWAC	Qualified Website Authentication Certificate
RFC	Request For Comments
SB	Supervisory Body
SCD	Seal creation device
SME	Small and Medium-sized Enterprise
TR	Technical Report
TS	Technical Specifications
TSA	Time Stamping Authority
TSP	Trust Service Provider
TSU	Time Stamping Unit
UTC	Universal Coordinated Time
WWW	World Wide Web

Annex B - Possible mapping basic/recommended/enhanced vs business criticality and/or data protection

B.1 Understanding an organization's environment and corresponding criticality-levels

When trust services will be used by subscribers and relying parties, there will be many use cases / story-lines / etc. as explained in the use case examples mentioned in this document. However and depending on the concrete environment the use case is applied in, the "strength/rigorousness" with which the recommendations should be applied might be less or more severe. Dimensions that could have an impact on the "strength/rigorousness" of applying the recommendations, are the criticality of the processes and/or data being involved in the business process which is being supported by the respective qualified trust service. So, without intending to be complete as a risk assessment depends of the concrete environment/context in which the organization is operating, some dimensions which might be considered to determine the risk-profile of the process and/or data being protected (and therefor the minimum "strength/rigorousness" to apply) are:

- **Business critical data & processes**: organizations store or process information that can have a less or more significant impact on their own organization and/or their partners and/or their clients. Examples of potential risks are e.g. loss of integrity of a database, compromise of business-confidential data, incorrect contracting-data, etc.
- **Data & processes with potential financial impact**: organization (especially but not only financial industry related organizations) have several processes which might have direct financial impact for themselves, for their partners and/or their clients ranging from amounts e.g. below a thousand euros to amounts going into millions of euros. Examples of potential risks are e.g.: faulty validation of signatures on mandates or payment instructions, rogue / criminal impersonation of third party providers, hacking of personnel or corporate accounts, false invoices, etc.
- **Personal data (processing)**: Personal data is clearly a very complex and high risk matter. The scope of personal data is very broad, ranging from less delicate personal data, to directly identifiable information to sensitive personal data. The more sensitive the data the stronger and more rigorous one should apply the recommendations. Examples of potential risks are: fines of up to 4% of the global annual revenues of a company, embarrassment due to faulty access personal information, unauthorized access/manipulation to e.g. biometric data, responding to a request-for-info based on an incorrect signed request, health data getting exposed / delivered incorrectly, authenticity/integrity of critical health records being non-verifiable, etc.

Note: We stress that the above are just examples of possible areas to consider to assess the risk-profile of the process and/or data being protected. Depending on the reader's environment other dimensions might apply depending on regulation, corporate policies, contractual obligations, etc.

B.2 Determining applicable criticality-levels and derive resulting minimum applicable recommendations

Following the above, it is proposed that organizations do their own analyses and following map their processes / data-to-be-processed onto the following "criticality-levels":

- "**Standard**" would entail any usage of a trust service under normal circumstance like but not limited to use cases e.g. involving financial exchange of a rather limited amount, personal records with limited potential impact, or access to data/services of a limited classification level (e.g. internal/restraint).

- “**Advanced**” would entail any usage of a trust service in a context where more precautions / prudence is to be advised like cases which involve financial exchange of a rather important magnitude, personal records with rather important impact if going wrong, or access to data/services of a higher classification level like company-confidential.
- “**Sensitive**” would entail any usage of a trust service in a context where sensitive data is being involved, e.g. involving financial exchanges of a significant amount, personal record access of personal sensitive information, or access to data/services of a high classification level like company-/commercial-secret.

Based on the above “criticality-levels”, one can easily see how the levels (Basic, Recommended, Enhanced) can match to these levels:

- **Basic** would entail the recommendations to-be-considered at the moment one is involved in a (trans)action that involves data/services of a “standard” level of criticality.
- **Recommended** would entail the recommendations to-be-considered at the moment one is involved in a (trans)action that involves data/services of an “advanced” level of criticality.
- **Enhanced** would be the recommendations to-be-considered at the moment one is involved in a (trans)action that involves data/services of a “sensitive” level of criticality.

CRITICALITY	RECOMMENDATION	FINANCIAL - CORPORATE - PERSONAL DATA/PROCESSES
normal	Basic	Limited importance
advanced	Recommended	Higher importance
sensitive	Enhanced	Significant importance

Annex C - References and bibliography

C.1 References

REF. ID	DESCRIPTION
[1]	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014, p. 73–114.
[2]	EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[3]	ETSI TS 119 172-1: “Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents”.

C.2 Bibliography

ID	DESCRIPTION
(a)	CEN TR 419 030: “The framework for standardization of signatures: Best practices for SMEs”.
(b)	CEN TR 419 040: “The framework for standardization of signatures: Guidelines for citizens”.

C.3 Relevant implementing acts

ID	DESCRIPTION
(i)	Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services (Text with EEA relevance). OJ L 128, 23.5.2015, p. 13–15.
(ii)	Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance). OJ L 235, 9.9.2015, p. 26–36.
(iii)	Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance). OJ L 235, 9.9.2015, p. 37–41.
(iv)	Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance). OJ L 109, 26.4.2016, p. 40–42

Annex D - Frequently asked questions

D.1 What about the (international) recognition of electronic seals (within Europe)?

A qualified electronic seal (QESeal) shall be recognised as a qualified electronic seal in all Member States; since QESeal bear with them the proofs (or the links enabling the automatic validation through trusted sources) that they are qualified, they shall never be refused by anybody in any European Member States. In case of litigation it is up to the requesting party to proof that the seal is not qualified. There is quasi no risk of rejection with QESeal.

AdESeal also benefit from a legal recognition, but the burden of proving that the AdESeal is an AdESeal as per the EU Regulation N° 910/2014 is on the creator of the seal. In case of litigation the confirmation or information will come from experts hired by the tribunal. There is a risk of rejection with AdESeal (depending on the quality of the AdESeal; i.e. level of quality and of assurance on the CA and level of quality and assurance on the SCDev).

In all cases, the EU Regulation N° 910/2014 further supports the recognition of AdESeal through its Article 46 on electronic documents; "*an electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form*". It means that no one can refuse an AdESeal because the sealed document is not in a paper form.

D.2 What about the (international) recognition of electronic seals (outside Europe)?

From a legal perspective, the automatic mutual recognition of QESeal will come from international agreements between the Union and the foreign countries. Per Article 14 of the EU Regulation N° 910/2014, such agreements shall ensure that;

(a) the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in the third country or international organisations with which the agreement is concluded, and by the trust services they provide;

(b) *the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or international organisation with which the agreement is concluded*.

Even in the absence of such agreement, and this is anyway true for the AdESeal (non-QESeal), thanks to the international standards, the international recognition is possible. Many countries use schemes for assessing the security of their trust service provider; both the assessment process and the criteria used to assess the TSPs follow standards that, when not exactly the same as the ones used within Europe, are comparable to our standards. Yet probably not easy for the citizen, it is not that complex for an IT professional to assess whether an AdESeal received from a third country is comparable to an AdESeal issued in Europe. For international relationships, the citizen is encouraged to take advice from his/her CA, e.g. in order to verify interoperability of his/her seal.

D.3 eIDAS Regulation – Questions and answers on rules applicable to trust services as of 1 July 2016

The European Commission complied a Q&A document to help fully understanding the new legal framework in order to implement it or reap the benefits of electronic transactions.

The complied a Q&A document is available from https://ec.europa.eu/digital-single-market/en/news/questions-answers-trust-services-under-eidas.

The Commission launched the eIDAS Observatory - an online collaborative platform for exchanging views and positions, sharing ideas and good practices. It is a virtual community of stakeholders whose aim is to build a common understanding of the issues relating to the implementation and uptake of the eIDAS Regulation and to facilitate the use of cross-border electronic identification and trust services. You can join the eIDAS Observatory and take part in the discussions.

D.4 How can I find a qualified trust service provider issuing qualified certificates for electronic seals?

You can find a qualified trust service provider issuing qualified certificates for electronic seals by looking:

- For the use of the EU trust mark for qualified trust services associated to the provision of qualified certificates for electronic seals in the marketing material of envisaged providers;

- For EU MS national trusted list as they are available from the EC list of pointers to the EU MS trusted lists (https://ec.europa.eu/information_society/policy/eseal/trusted-list/tl-mp.xml) or by browsing the EU MS trusted lists from, e.g. http://tlbrowser.tsl.website. Trusted lists are organised per TSP, and then per trust service. Look up for a service type and its appropriate extension identifying the issuance of qualified certificates for electronic seals (service type identifier: http://uri.etsi.org/TrstSvc/Svctype/CA/QC and additional service information extension http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals) for which the current status is "granted" (http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted).

- For applicable terms and conditions, the policies and practices used by the QTSP to provide its qualified certificates for electronic seals should be available from the "TSP information URI" as part of the TSP information as listed in the relevant EU MS trusted list.

D.5 How can I find a qualified trust service provider providing qualified preservation services for qualified electronic seals?

You can find a QTSP providing qualified preservation services for qualified electronic seals by looking:

- For the use of the EU trust mark for qualified trust services associated to the provision of qualified preservation services for qualified electronic seals in the marketing material of envisaged providers;

- For EU MS national trusted list as they are available from the EC list of pointers to the EU MS trusted lists (https://ec.europa.eu/information_society/policy/eseal/trusted-list/tl-mp.xml) or by browsing the EU MS trusted lists from, e.g. http://tlbrowser.tsl.website. Trusted lists are organised per TSP, and then per trust service. Look up for a service type and its appropriate extension identifying the provision of qualified preservation services for qualified electronic seals (service type identifier: http://uri.etsi.org/TrstSvc/Svctype/PSES/Q and additional service information extension http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals) for which the current status is "granted" (http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted).

- For applicable terms and conditions, the policies and practices used by the QTSP to provide its qualified preservation services for qualified electronic seals should be available from the "TSP information URI" as part of the TSP information as listed in the relevant EU MS trusted list.

D.6 How can I find a qualified trust service provider providing qualified validation services for qualified electronic seals?

You can find a QTSP providing qualified validation services for qualified electronic seals by looking:

- For the use of the EU trust mark for qualified trust services associated to the provision of qualified validation services for qualified electronic seals in the marketing material of envisaged providers;

- For EU MS national trusted list as they are available from the EC list of pointers to the EU MS trusted lists (https://ec.europa.eu/information_society/policy/eseal/trusted-list/tl-mp.xml) or by browsing the EU MS trusted lists from, e.g. http://tlbrowser.tsl.website. Trusted lists are organised per TSP, and then per trust service. Look up for a service type and its appropriate extension identifying the provision of qualified validation services for qualified electronic seals (service type identifier: http://uri.etsi.org/TrstSvc/Svctype/QESealValidation/Q and additional service information extension http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals) for which the current status is "granted" (http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted).

- For applicable terms and conditions, the policies and practices used by the QTSP to provide its qualified validation services for qualified electronic seals should be available from the "TSP information URI" as part of the TSP information as listed in the relevant EU MS trusted list.

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilissis Sofias
Marousi 151 24, Athens, Greece

TP-07-16-162-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-213-4
DOI: 10.2824/352342