eIdentification (eID)
eProcurement
eInvoicing
eDelivery
Website authentication
eTime-stamp
Signing contract online
Online banking
eSignature
eSeal
eHealth
Tax online

Security guidelines on the appropriate use of qualified electronic signatures

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 978-92-9204-212-7, DOI 10.2824/399794

Contents

Executive Summary 6

1. Introduction 7

1.1 General context/the eIDAS Regulation on eID and trust services 7

1.2 Opportunities brought by eIDAS Regulation 7

1.3 Specific role of the qualified trust services 8

1.4 Initiation and supervision of qualified trust services 8

1.5 A focus on qualified electronic signatures 10

1.6 Scope of the present document and relationship with other recommendations 11

2. Qualified electronic signature – what is it? 13

2.1 Legal definition of (qualified) electronic signatures 13

2.2 Public Key Cryptography as technical foundations for (Q)ES 14

2.3 Certification services as trust foundation for (Q)ES 16

2.4 The electronic signature process 17

2.5 Qualified electronic signatures 18

3. Qualified electronic signature – what key properties does it provide? 20

3.1 Legal properties 20

3.2 Security properties 20

3.3 Functional Properties 20

3.4 Other Properties 21

4. Qualified electronic signature – what properties can it not provide? 22

4.1 Legal properties not provided by QES 22

4.2 Security properties not provided by QES 22

4.3 Functional properties not offered by QES 22

4.4 Other properties not offered by QES 22

5. Qualified electronic signature – what are the potential use cases? 24

5.1 Overview and context of the given examples 24

5.2 Signing a document/message to confirm origin 24

5.3 Signing of a document/declaration 25

5.4 Signing a (commercial) proposal 25

5.5 Signing of an official document/attestation 26

5.6 Signing of a legal consent / an eMandate / … 26

5.7 Signing of a contract 26

6. Qualified electronic signature – what are the usage best practices? 27

6.1 Security Guidelines & Levels 27

6.2 BASIC27

6.3 RECOMMENDED 28

6.4 ENHANCED 29

7. Qualified electronic signatures – example of tools & practical usage aspects 32

7.1 Implementing qualified electronic signatures (user perspective) 32

7.2 Relevant standards regarding qualified electronic signatures (expert perspective) 34

Annex A - Glossary 36

A.1 eIDAS – What is it? 36

A.2 Electronic seal 36

A.3 Hash value (of a file) 36

A.4 Intellectual property 36

A.5 Trusted list 36

A.6 QTSP/QTS requirements and obligations 37

A.7 CEF eSignature building blocks 38

A.8 Trust services defined by the eIDAS Regulation 38

A.9 Qualified trust services defined by the eIDAS Regulation 39

A.10 Other terms 40

A.11 Acronyms 42

Annex B - Possible mapping basic/recommended/enhanced vs business criticality and/or data protection 44

B.1 Understanding an organization's environment and corresponding criticality-levels 44

Annex C - References and bibliography 46

C.1 References 46

C.2 Bibliography 46

C.3 Relevant implementing acts 46

Annex D - Frequently asked questions 47

D.1 What about the (international) recognition of electronic signatures (within Europe)? 47

D.2 What about the (international) recognition of electronic signatures (outside Europe)? 47

D.3 eIDAS Regulation – Questions and answers on rules applicable to trust services as of 1 July 2016 48

D.4 How can I find a qualified trust service provider issuing qualified certificates for electronic signatures? 48

D.5 How can I find a qualified trust service provider providing qualified preservation services for qualified electronic signatures? 48

D.6 How can I find a qualified trust service provider providing qualified validation services for qualified electronic signatures? 49

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 signature shall have the equivalent legal effect of a handwritten signature and, when based on a qualified certificate issued in one Member State, shall be recognised as a qualified electronic signature in all other Member States.

This document addresses qualified electronic signatures 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 or 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 eSignature is and what properties/function it does and does not provide, concrete examples of use are given for inspiration to the readers. Next to them, 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 signature
- In a signature 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 signature.
- Before algorithms, keys, and other cryptographic data used at the time a signature was built become weak and the cryptographic functions become vulnerable, or the certificates supporting previous time stamp tokens expire or are revoked, the signed data, the signature as well as any additional information should be protected by applying time stamp tokens.
- QES 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.

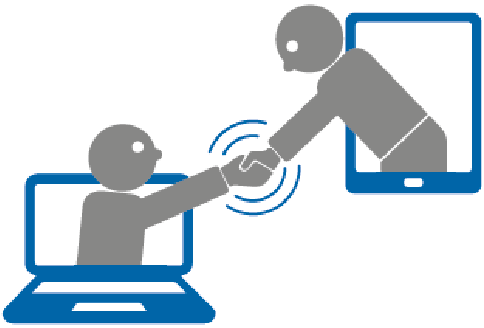
1. Introduction

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 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 brought by eIDAS Regulation

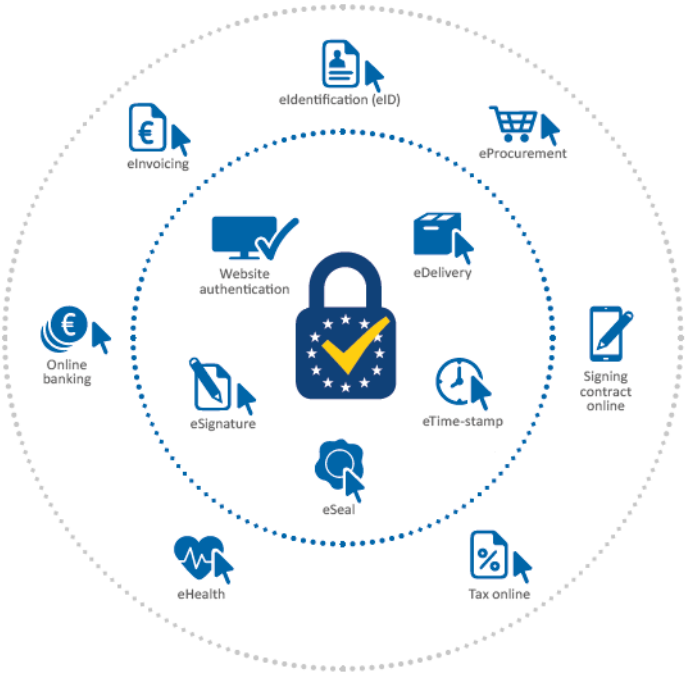
An array of opportunities resides in leveraging eID and electronic trust services as key enablers for making national and cross-border electronic transactions more secure, more convenient, trustworthy and benefiting from legal certainty.

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 ones 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 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]

[7]

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

For marketing purposes, once qualified, a QTSP/QTS may use the EU Trust Mark for qualified trust services when promoting its QTS. That 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 must be displayed on the QTSP's website) and rules of Commission Implementing Regulation (EU) 2015/806.[8] 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.

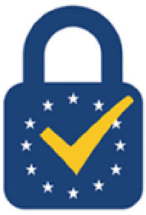


Figure 1: EU trust mark for qualified trust services

The use of the EU trust mark[9], which is voluntary, aims to foster transparency of the market and help consumers distinguishing 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 signatures

Today, it is possible to electronically sign data and to **achieve the same effects as when using a hand-written signature**. Such electronic signatures that benefit from a full legal recognition thanks to the eIDAS Regulation are called **qualified electronic signatures.**

[8] 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.
[9] 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.

Figure 2: Types of electronic signatures

The eIDAS Regulation addresses various services that can be used to support different types of electronic transactions and electronic signatures in particular.

Beside the legal framework, the technical framework is nowadays very mature. Citizens routinely sign data electronically e.g. when they use a credit card or debit card to make a payment.

The use of qualified electronic signatures 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, online games, e-services, online contracts, etc.

1.6 Scope of the present document and relationship with other recommendations

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

The target audience of the document are end users and relying parties of qualified electronic signature services. This could comprise individuals, businesses and public administrations. For example, it could be a public administration that wishes to use qualified electronic signatures for their electronic interactions with 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 signature:

- 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 seals, qualified electronic time stamps, qualified website authentication certificates and qualified electronic registered delivery.[10]

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:

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

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 signature – what is it?

2.1 Legal definition of (qualified) electronic signatures

The eIDAS Regulation defines an **electronic signature** as "*data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign*".

A signature is "**generated**" by a **signatory,** possibly "**augmented**" (i.e. completed with related proofs or evidences – see section 6), "**validated**" by the receiver of the signed 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 signatures. In particular, TSPs, qualified or not, can be called for the qualified **signature creation, validation** and/or **preservation**.

Looking at the definition above, as such, an electronic signature can be created using many technologies, ranging from the extremely weak (such as pasting a scanned signature image in a document) to the very strong (such as signing using an electronic identity card protected by a fingerprint).

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

In these definitions, the "unique data" is to be seen as a personal element that belongs to the signatory and that can be compared to the very personal behaviour of a signatory signing in the paper world (i.e. the graphics, speed, pressure that make that a signature can be unambiguously linked to a person). In the same way that signatory keeps these elements private in the paper word, the electronic signature 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).

Electronic signatures in general shall not be denied legal effect and admissibility as evidence in legal proceedings. Within the electronic signature family, the eIDAS Regulation defines subsets of electronic signatures that provide increasing legal predictability up to a level, the qualified electronic signature**,** which benefits from the legal equivalence to handwritten signatures:

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

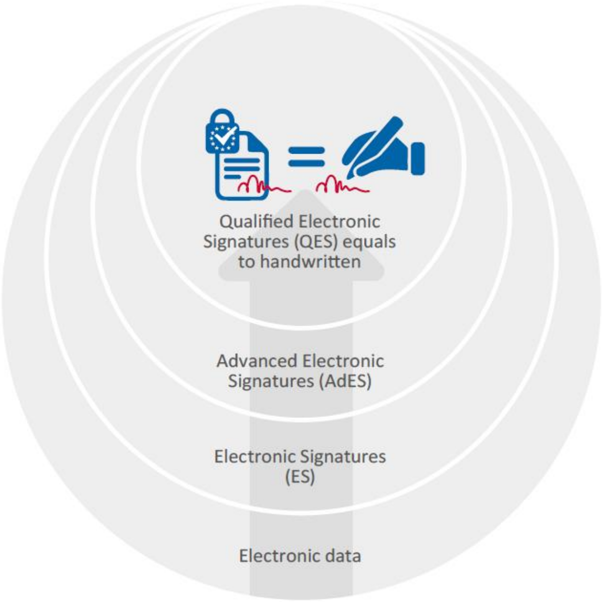

Qualified Electronic Signatures (QES) equals to handwritten
Advanced Electronic Signatures (AdES)
Electronic Signatures (ES)
Electronic data

Figure 3: Types of electronic signatures

A QES shall have the equivalent legal effect of a handwritten signature and shall be recognised as a qualified electronic signature in all Member States.

This equivalence is gained from the fact that qualified electronic signatures are supported by i) trustworthy process technology, similar to advanced electronic signatures, ii) qualified electronic signature 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)ES

In the current state of the art, QES are implemented by means of asymmetric cryptography. With this technology, each signatory owns a key pair made of a private and a public key (the technology is called the public key cryptography) and the so produced electronic signatures are called **digital signatures**.

The signature creation and verification process as follows:

1. The signatory uses the private key to sign a text:

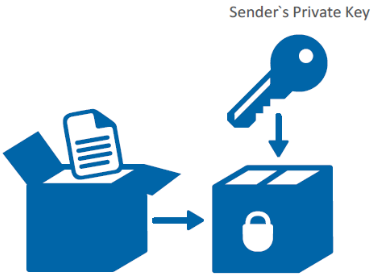


Figure 4: Digitally signing data with a private key to produce an electronic signature

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 'signature creation data' as defined in the eIDAS Regulation. In the paper world the "private key" concept can be compared to the unique behaviour of the signatory; what distinguishes a handwritten signature is the speed, the pressure, the graphic, that are in theory only reproducible by the signatory.

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

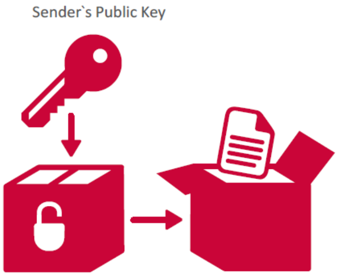


Figure 5: Verifying a signature with sender's public key.

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 signature that a verifier can compare with a received signature.

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

Another characteristic of digital signatures is that if the signed text has been modified after the signature, the verification of the signature will fail (because the signature computation mixed the private key and the data to be signed 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 signature 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 not a third person that would be able to imitate the signatory's signature):

- it is likely 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 signatory 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 signatory.
- The signatory shall protect the private key (in the same way as (s)he would not explain to third party how to imitate her signature).

2.3 Certification services as trust foundation for (Q)ES

The technical foundations presented above, alone, are not sufficient to ensure the full confidence in the system. Indeed, trust in signatures relies on the guarantee that a certain Public Key belongs to a particular signatory, 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 – signatory} in a public key **certificate**. In general, one finds the information on the identity of the signatory in the certificate, and sometimes one can also find other attributes relating to this person, such as his/her role within an organisation.

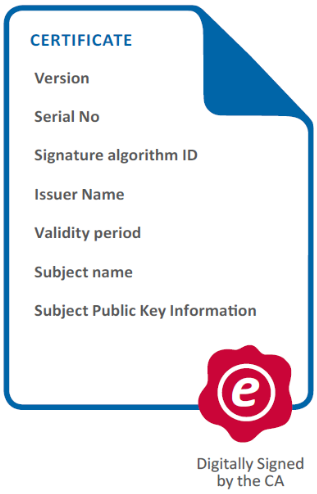


Figure 6: A digital certificate

The certificate is a signed statement by the CA; the CA's signature is trusted because the CA's key is published in a media trusted by the community (the official journal, e.g.). The procedures, techniques and mechanisms put in place to realise such certification services is commonly called **Public Key Infrastructure** (or PKI). The certificate officialises the link between a signatory and its key pair in the same way 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, signature creation devices for signatories of a good quality, trusted personnel, insurances, etc.

It also relies in 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 if the signatory has lost his/her signature creation device and fears that someone uses it to impersonate him/her.

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 signature process

The signature creation workflow

A signatory, to create a signature in a document, works in a certain environment (e.g. a laptop) to access signing functionalities made of:

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

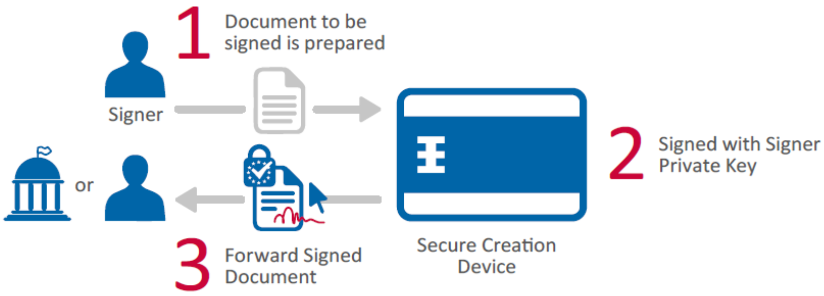

1
Document to be signed is prepared
Signer
2
Signed with Signer Private Key
Secure Creation Device
or
3
Forward Signed Document

Figure 7: Signature creation process

Concretely, how does it work?

1. The signatory prepares the document like any kind of document (e.g. a PDF file).

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

3. The signature creation device asks the authorisation to the signatory to sign the data, in general, though a windows that pops up on the screen. The signatory authenticates to the device (e.g. (s)he enters a PIN code, or a fingerprint).

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

At this stage, it is important to note that in general, the signatory's certificate is provided with the signature. This enables the identification of the signatory and the verification of the signature since the public key is immediately available from the certificate. If there are attributes relating to the signatory in the certificate, one can also validate these attribute(s) (e.g. the person may sign in quality of director of an organisation and this title is certified), but nothing prevents the signatory to (also) add a sentence in the signed document that says "I'm signing in quality of director". This is a self-claim similar to what is done in the paper world.

The augmentation for more resilience

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

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

2.5 Qualified electronic signatures

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

To achieve a QES, the eIDAS Regulation requires a qualified signature creation device (i.e. a signature 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 signatures: 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 signatures provides high assurance of the identity of the signatory**
- **QSCDs provide high assurance on the security of the signature**

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

There is no obligation to call such QTS for the validation or the preservation of (qualified) signature, 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).

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

3.1 Legal properties

Signing with the same legal value as with a handwritten signature

As presented above, QES benefit from a full legal recognition thanks to the eIDAS Regulation to achieve the same effects as when using a hand-written signature.

Such electronic signatures thanks to the obligations set by the eIDAS Regulation on both the TSP managing them (in particular the CAs) and on the underlying technologies: warrant data integrity, identify the signatory with a high level of certainty, and ensure the non-repudiation of signing.

At this stage, it is important to note that like handwritten signature, (qualified) electronic signatures are created by human beings (i.e. natural persons). Indeed, under the eIDAS Regulation, a legal person is not legally permitted to electronically sign. Rather, the eIDAS Regulation allows legal persons to electronically seal data. The concept of electronic seal for legal persons is very similar to the concept of electronic signature for natural persons and is the topic of dedicated security guidelines within the series.

3.2 Security properties

Data integrity

As mentioned in the introduction, the use of public key cryptography to implement QES (and AdES in general) ensures data integrity (i.e. any change in the signed data after the signature process is detected).

Data origin authentication

The use of public key cryptography to implement QES (and AdES in general) warrants the proof of origin of the signed data since only the person in possession of the private key can be at the point of origin of data signed with the corresponding public key. For QES, 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 signing

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

Secure identification of the signatory

The qualified digital certificate ensures the identification of signatory with a very high level of assurance, thanks to the controls of the TSP on one hand, but also thanks to the requirements on the content of the signatory's certificate imposed by the eIDAS Regulation.

Creating huge amount of signatures and/or signatures on huge data

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

Also, a signature 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 signature to ensure the integrity and non-repudiation of the whole file. No need to sign each and every page like in the paper world, by virtue of the data integrity featured by the Public Key Cryptography technology underlying QES.

3.4 Other Properties

Signing with a signature that is understood and verifiable worldwide

Basic signatures, like non-qualified AdES, 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 QES because the signatory may be required to prove the security of the technology being used if the validity of the signature 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 signature solutions. It may also be the case that the relying parties have no applications or tools to validate such signature, when not based on standards; in such a scenario, the signature may be legally valid and technologically robust, but of limited use.

For these **interoperability** reasons, **QES** 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 signature solution is sufficiently certain.

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

Signing "in quality of"

It is possible to certify elements that are bound to the signatory such as a title (e.g. Director), a link with its employer, etc. Because the QCA is trusted for verifying the information it certifies, the Relying Party can get a high level of confidence in such information conveyed with the signature through the signatory's certificate.

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

4.1 Legal properties not provided by QES

“Signature” by a legal person

As mentioned above (qualified) electronic signatures are performed by human beings (i.e. natural persons).

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

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

Exactly like in the paper world, it is not because a contract is signed that the terms of the contract are fair.

4.2 Security properties not provided by QES

Confidentiality

The signature protocol used alone does not provide confidentiality, although the Public Key Cryptography can be used to offer encryption. Indeed, if the signature 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 signature, 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 signature and confidentiality. First the signatory signs and then (s)he may encrypt the signed document to the attention of a recipient, provided (s)he has the encryption certificate of this person. If the signed 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 QES

Time stamping

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

4.4 Other properties not offered by QES

Management of delegation

The relying party verifying a signature will not necessarily be ensured that the signatory is authorised to sign (e.g. to commit in the name of a certain organisation). Again this problem is not unique to electronic signatures; it exists in paper signatures as well (and arguably more so, since electronic signatures can more easily convey highly trustworthy identity information).

Electronic signatures do permit the implementation of solutions to this problem by incorporating authorisation management solutions. It is also possible to certify, in the certificate, elements that are bound to the signatory such as a title (e.g. Director), a link with its employer, etc. However, this is not provided by default. And it is not because the title Director is certified that the director is effectively empowered to sign any type of commitments in the name of the organisation (s)he represents.

Eternal integrity

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

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

5.1 Overview and context of the given examples

In general and to put qualified electronic signatures into context, they only provide signatures. As mentioned above, they do not establish the exact time on when the document was signed, they do not necessarily provide the commitment of a potential legal entity behind the signatory, and they do not confirm delivery of the signed message. Hence, qualified electronic signatures (QES) are most often seen coming in addition of other identification and/or trust services as part of a broader solution.

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

- QES to establish the originator of a signed document.
- QES to provide integrity of a signed document.
- QES to provide non-repudiation of having signed 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 QES.

	C2C	C2B C2G	B2B	B2G B2A	G2G A2A
Signing a document/message to confirm origin	●	●●	●●	●●	●●
Signing of a document/ declaration	●	●●	●●	●	●
Signing of a (commercial) proposal		●●	●●	●●	
Signing of an official document /attestation					●●
Signing of a legal consent / eMandate	●●	●●	●●	●●	
Signing of a contract	●	●●	●●	●●	

Table 2: QES application areas

5.2 Signing a document/message to confirm origin

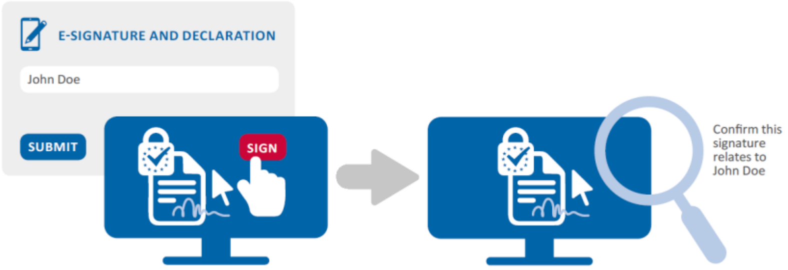
A first and often forgotten use case is (even if a QES might be considered excessive due to its qualified status) is simply to apply signatures on documents and messages to give proof of origin and integrity. Indeed, in the days of phishing it is for many people very difficult to see if a document or a message really originates from where it seems to come from. Applying qualified electronic signatures 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 signing, with QES, all their outgoing documents and messages and other hand validate incoming messages/documents.
- G2C: Governments should make it a standard to have outgoing documents/messages either using qualified electronic seals (cfr the eSeals Guideline document) or qualified electronic signatures.

5.3 Signing of a document/declaration

People or organisations can use QES to sign documents/declarations when submitting them e.g. to government as proof of their authenticity/origin and their endorsement of the content non-repudiation. 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 signed (with QES) and submit them in one single digital flow.


E-SIGNATURE AND DECLARATION
John Doe
SUBMIT
SIGN
Confirm this signature relates to John Doe

Examples of concrete application are:

- C2C/C2B: One person giving e.g. a relative or an accountant a mandate for a month.
- B2G: Submitting declarations to government (which needs to be signed by mandated person).

5.4 Signing a (commercial) proposal

A SME might choose to use qualified electronic signatures for the submission of bids in public procurement. This is an area which is traditionally mired by large amounts of paperwork that creates significant efforts and costs that could easily be diminished, while increasing the reliability of the process, through the application of qualified electronic signatures.

Examples of concrete application are:

- B2C: Companies using signing of proposals/offers towards their (potentials) clients (endorsing thereby the proposals).

- B2G: Companies participating in the eProcurement-process of government and being more and more obliged to submit their offer electronically.

5.5 Signing of an official document/attestation

Certain government documents have to be signed by an official instead of by an administration (the later would be an electronic seal for which we refer to the respective other document in this series). In the day and age of qualified electronic signatures, it is no longer needed to do all this on paper. Officials can (depending on the specific form factors obliged by law) generate official documents/attestations and sign them electronically.

Examples of concrete application are:

- G2C: Creation/signing of e-permits or an attestation of residence.
- G2B: Creation/signing of VAT-attestations, signing of custom documents, etc.

5.6 Signing of a legal consent / an eMandate / …

In many cases, one needs to know if a client agrees with the terms and conditions, or opts into certain services, or consents with certain processing of his/her data or gives a mandate to a third party to act on his/her/its behalf. Especially when entering into a relationship (not being in a closed system yet) or when e.g. mandate with might have effect on third parties need to be given the use of qualified electronic signatures is advisable or even mandatory.

Examples of concrete application are:

- B2C: Signing of the general terms and conditions when becoming a client of a bank
- B2B: Giving an accountant a mandate to act on one's behalf and to do financial transfers on one's behalf.

5.7 Signing of a contract

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

Examples of concrete application are:

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

6. Qualified electronic signature – 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 signature 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 time stamping 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 ones ensures benefiting from a high level of security and legal certainty of trust services. Qualified electronic signatures enjoy, all over the EU, the equivalent legal effect of a handwritten signature.

As a basic recommendation, both the signatory 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[11] and/or other contractual documentation.

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

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

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 signatures (article 32) that request the confirmation that the certificate was valid at the time of signing.

As a fundamental recommendation, a signatory shall never share its signature activation data (e.g. PIN number).

6.3 RECOMMENDED

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

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

Typically, the date of signing will be indicated in the signed 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 signature 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 signature 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 (signer certificate, time stamps certificates, attribute certificates, etc.) contained in the signature.

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 signature was built become weak and the cryptographic functions become vulnerable, or the certificates supporting previous time stamp tokens expire or are revoked, the signed data, the signature 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 signatures or time stamp tokens. These evidences added to the signature are often called Long-Term Validation Data.

6.4 ENHANCED

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

Either for the simple validating of the QES, 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 QES** (as defined in Article 33 of the eIDAS Regulation)
- **qualified preservation of QES** (as defined in Article 34 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 signature, but as any other Qualified Service, their use provides 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 signature message, one needs to look at all available evidences in order to validate the signature and resolve the dispute.

The issues of the dispute may for example be that the signer denies having performed the signature at all, or that the signer acknowledges having performed the signature, but for a different message, etc. Most of the technical **evidence can be found in the signed 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 signature policy, as described below. However, it should be noted that the signature may also require evidence of the context in which the signature was created. For example, regardless of all technical evidence, the signatory may still have been deceived or forced by violence to sign, or the signatory may not have understood the document (e.g. it needs to be established that the document was written in a language understandable to the signer).

Evidence present in the signature

Digital signatures 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 signer'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 signature-creation, etc. The signature may also contain:

- A commitment type, indicating the purpose of the signature.

- A location indicator, specifying the claimed location of the signatory,
- A role under which the signature is applied,
- A reference to the Signature Policy under which the signature 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 signing key of the CA, the registration of the signatory, 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 signature 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 Signature Policy

A signature policy is a set of rules for the creation and validation of an electronic signature, under which the signature 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 signature policy as meeting its requirements. An example of signature policy is the “evidence agreement” through which Parties agree to accept the validity of signature type X to sign transactions. This is typically included in terms and conditions of online banking application.

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

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

The signature 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;
- signature validation data to be provided by the signer;
- signature validation data to be collected by the verifier.
- the period during which signatures can be performed under that policy,

- a list of recognised commitment types;
- rules for the use of signer roles;
- any constraints on signature algorithms and key lengths;
- other signature policy rules required to meet the objectives of the signature.
- rules for multiple signatures:
  - for documents signed by multiple signers, it may be necessary to establish the order of signing, and if all signers were present at the same place for signing.
  - the signature policy should provide guidance on the actions to take (both at creation and verification sides), if one or more of the signature(s) are not valid, etc.

Additional evidence that may be required:

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

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

7.1 Implementing qualified electronic signatures (user perspective)

Signature creation tools

As mentioned previously, for creating a QES, the signatory needs (access to):

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

The signatory 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 signatory must be able to control the activation of the private key.

Qualified certificate

Very probably, the first stakeholder that the signatory will meet in the framework of electronic signature will be the CSP. There is even not necessarily a need to search for a CSP since in many European countries, citizens are provided with electronic identity cards that bear digital certificate(s), and very often the signature certificate is a qualified certificate.

When the signatory is required to acquire the certificate by himself, (s)he may be presented with several options with regard to the information to be certified: the certificate may contain in addition to the “civil identity” of the signatory, the name and identifier of an organisation with whom the citizen is associated (e.g. his/her employer) and/or the indication of a role or **mandate** within an organisation.

Arguments for choice: a certificate with attributes help to evidence a role, function or belonging to an organisation but needs to be re-issued if any one of these attributes changes.

Qualified signature creation device

With regard to the QSCD, the signatory may opt for a device in his/her hand, 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 signatory is higher, in the second case, the mobility is enhanced.

Signature creation application

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

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

Example: a typical use case is the citizen that signs a pdf attestation thanks to his/her national electronic identity card.

The signatory may sign using his/her qualified signature creation device (e.g. eID) to create a QES on a data (e.g. a PDF, a form) prepared by a server.

Example: a typical use case is the signature of the tax declaration, prepared by the government on its servers, possibly completed online by the citizen, and whose fingerprint is locally signed by the citizen, with his/her eID card.

On the other hand, the signatory may rely on remote signature creation devices and facilities. As illustrated below, it is possible to delegate a more or less important part of the signature creation process to a TSP. The strict minimum is that the signatory must be able to control the activation of the private key. For this purpose, the signatory 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. This may be really 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).

However, the signatory 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 QES, the signature creation device must be qualified (QSCD) and the TSP managing the private key(s) must be qualified (QTSP) and will be supervised as part of the QSCD certification.

Example: a typical use case is the signature of bank transfers. This scenario can be concretised by a banking apps on a smart phone through which the user connects to his/her bank. Via the apps the user enters the figures required for the bank transfer. When the info is ready to be signed, a SMS containing a challenge is sent to the phone and the user needs to copy the challenge via the apps to be authenticated; this allows the central server to activate and use the user's private key to sign the transfer. 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 signed 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 signatory is higher. When using remote signature creation facilities and devices, the mobility is enhanced.

Augmentation and preservation tools

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

Concretely, the signatory (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 signature. Generally, time stamping is a paying service that the signatory needs to buy on-the-fly or needs to pay in advance.
- Collect the required validation evidences and correctly format the signature according to the terms of preservation.

The signatory (or relying party) may use the services of a TSP to do so. When the signature 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 signature as provisioned in Article 32 of the eIDAS Regulation. On top of the strictly cryptographic validation that the digital signature is technically valid, the application must enable the relying party to validate the fact that the signature is a QES: among others that the signatory's certificate was issued by a QTSP, that the certificate was both qualified and valid at the time of signing, the signature creation device is a QSCD, the signatory'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 QES 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 signatures (expert perspective)

Signature formats

When an organisation (e.g. administration, SME) decides to develop its own signature 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 signature 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). 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[12] for further guidance).

Specific implementations

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

- that no data can be introduced in the flow of data to be signed (network and application protection required);
- that the user is aware that more than one document is to be signed that the data to be signed 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 QES.[13]

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

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

An important tool for relying Parties is probably **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 signatures, and how to fix the parameters for declaring a signature conformant to the specified rules.

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

An electronic seal is a piece of data in electronic form, created by a legal person, which is attached to or logically associated with an electronic document (or data) to ensure its origin and integrity.

It is similar in the paper world to the dry seal of a company on a piece of paper to indicate that the document originates from the company and make it authentic and official.

A.3 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.4 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.5 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.6 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.7 CEF eSignature building blocks

The Connecting Europe Facility[14] (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[15,16].

The CEF eSignature solution[17] 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.8 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.

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

[15] 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.

[16] 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.

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

A.9 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**

   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.10 Other terms

Advanced electronic signature as per eIDAS Regulation: means an electronic signature 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 signature): as per eIDAS Regulation: means an electronic attestation which links (electronic signature) 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 signature creation data as per eIDAS Regulation: *"a unique data which is used by the signatory to create an electronic signature"*.

Electronic signature: "*data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign*".

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

Non-repudiation (of a signature): (a signature for which) the (signatory) cannot deny to be at the origin of such signature.

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 seal.

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

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

Qualified signature creation device as per eIDAS Regulation: means an electronic signature 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).

Signatory as per eIDAS Regulation: means a natural person who creates an electronic signature.

Signature creation data as per eIDAS Regulation: means unique data which is used by the signatory to create an electronic signature.

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

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

Signature validation as per eIDAS Regulation: means the process of verifying and confirming that an electronic signature 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.11 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

Acronyms	Description
CAR	Conformity Assessment Report
CEN	Centre Européen de Normalisation
eID	electronic Identification
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
PDS	PKI Disclosure Statement
PK	Public Key
PKI	Public Key Infrastructure
PKI	Public Key Infrastructure
Q&A	Questions and Answers
QeDel	Qualified Electronic Delivery Service
QESeal	Qualified Electronic Seal
QSCD	Qualified Signature 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

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 signatures (within Europe)?

A qualified electronic signature (QES) shall have the equivalent legal effect of a handwritten signature and shall be recognised as a qualified electronic signature in all Member States; since QES 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 signature is not qualified. There is quasi no risk of rejection with QES.

AdES also benefit from a legal recognition, but the burden of proving that the AdES is an AdES as per the EU Regulation N° 910/2014 is on the signatory. In case of litigation the confirmation or information will come from experts hired by the tribunal. There is a risk of rejection with AdES (depending on the quality of the AdES; 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 AdES 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 AdES because the signed document is not in a paper form.

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

From a legal perspective, the automatic mutual recognition of QES 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 AdES (non-QES), 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 AdES received from a third country is comparable to an AdES 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 signature.

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 signatures?

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

- For the use of the EU trust mark for qualified trust services associated to the provision of qualified certificates for electronic signatures 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/esignature/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 signatures (service type identifier: http://uri.etsi.org/TrstSvc/Svctype/CA/QC and additional service information extension http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures) 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 signatures 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 signatures?

You can find a QTSP providing qualified preservation services for qualified electronic signatures 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 signatures 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/esignature/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 signatures (service type identifier: http://uri.etsi.org/TrstSvc/Svctype/PSES/Q and additional service information extension http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures) 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 signatures 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 signatures?

You can find a QTSP providing qualified validation services for qualified electronic signatures 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 signatures 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/esignature/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 signatures (service type identifier: http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q and additional service information extension http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures) 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 signatures 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-07-16-161-EN-N

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

ISBN: 978-92-9204-212-7
DOI: 10.2824/399794