



Security guidelines on the appropriate use of qualified electronic time stamps

Guidance for users

VERSION 2.0
FINAL
DECEMBER 2016



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 enquiries 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

© European Union Agency for Network and Information Security (ENISA), 2016

Reproduction is authorised provided the source is acknowledged.

ISBN 978-92-9204-215-8, DOI 10.2824/4115

Table of 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 time stamps	10
1.6 Scope of the present document and relationship with other recommendations	11
2. Qualified electronic time stamp – what is it?	13
2.1 Official time	13
2.2 Electronic time stamp	13
2.3 Qualified electronic time stamp	14
3. Qualified electronic time stamp – what key properties does it provide?	16
3.1 Legal properties	16
3.2 Security properties	16
3.3 Functional properties	16
4. Qualified electronic time stamp – what properties can it not provide?	17
4.1 No prevention of document alteration	17
4.2 Confidentiality	17
4.3 No proof of sending/receipt	17
4.4 No proof of origin on the time stamped data	17
4.5 No signing or content commitment on time stamped data	17
5. Qualified electronic time stamp – what are the potential use cases?	19
5.1 Overview and context of the given examples	19
5.2 Establishing the time of signing (and deposition) of a document/declaration	20
5.3 Establishing the time of issuance of official documents/attestations	20
5.4 Establishing the time of conclusion of a contract	21
5.5 Enforcing legal/procedural/contractual time limits	21

5.6	Long term validity of electronic records	22
5.7	Long term preservation of electronic records	22
5.8	Notarizing the exact chronology of events	23
6.	Qualified electronic time stamp – what are the usage best practices?	25
6.1	Security guidelines & levels	25
6.2	BASIC25	
6.3	RECOMMENDED	26
6.4	ENHANCED	27
7.	Qualified electronic time stamp – example of tools & practical usage aspects	28
7.1	Implementing time stamping in off-the-shelf applications (user perspective)	28
7.2	Implementing time stamping from APIs and other tool kits (expert perspective)	28
Annex A:	Glossary	31
A.1	eIDAS – What is it?	31
A.2	Electronic seal	31
A.3	Hash value (of a file)	31
A.4	Intellectual property	31
A.5	Trusted list	31
A.6	QTSP/QTS requirements and obligations	32
A.7	CEF eSignature building block	33
A.8	Trust services defined by the eIDAS Regulation	33
A.9	Qualified trust services defined by the eIDAS Regulation	34
A.10	Other terms	35
A.11	Acronyms	36
Annex B:	Possible mapping basic/recommended/enhanced vs business criticality and/or data protection	38
B.1	Understanding an organization’s environment and corresponding criticality-levels	38
B.2	Determining applicable criticality-levels and derive resulting minimum applicable recommendations	38
Annex C:	References and bibliography	40
C.1	References	40
C.2	Bibliography	40

C.3 Relevant implementing acts	40
Annex D: Frequently asked questions	41
D.1 eIDAS Regulation – Questions and answers on rules applicable to trust services as of 1 July 2016	41
D.2 How can I find a qualified trust service provider issuing qualified time stamps?	41

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 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.

This document addresses qualified electronic time stamps 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 electronic time stamp 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:

- Relying parties should look for the EU trust mark for qualified (time stamping) trust services when selecting providers and should read the applicable terms and conditions, the policies and practices used by the QTSP providing qualified time stamps.
- Relying parties Look out for the accuracy of the qualified time stamp which must be of 1 second or even better.
- All scenarios where a QTSP providing qualified time stamps stores hashes of files or the files themselves require strong guarantees with regards to the long term permanency and solvency of the QTSP.
- Applicable terms and conditions, the policies and practices used by the QTSP to provide its qualified time stamps should be available from the “TSP information URI”.
- For obtaining a proof of sending/receipt, use qualified electronic delivery services that includes qualified time stamps embedded in such a proof.
- For obtaining a proof of origin on the time stamped data, use qualified electronic signature as a natural person (or qualified electronic seal as a legal person) as such signature (seal) may be combined with the use of qualified time stamp.

1. Introduction

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

Regulation (EU) No 910/2014¹ (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 authentication³.

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

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



Since 1 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

The opportunities reside in leveraging eID and electronic trust services as key enablers for making 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

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.

³ See Glossary or Art.3.16 of the eIDAS Regulation for the definition of trust services.

customer experience, improve the security of electronic transactions and stimulate the provisioning of new and innovative services.

To this end, a large number of sectors (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 will indeed allow citizens, businesses and public administrations to conveniently meet such obligations for any cross-border electronic transaction using the 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 account⁴. 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.



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

⁴ 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).

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**⁵. 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**⁶. From there, the supervision scheme covers the full life cycle of each QTS and each QTSP, from its genesis until its 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.⁷

⁵ See glossary

⁶ See glossary.

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.⁹



Figure 1: EU trust mark for qualified trust services

The use of the EU trust mark, 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 time stamps

An internationally recognized time-scale is a necessity in today’s society. The Coordinated Universal Time (UTC) currently fulfils this function and is legally recognised in many countries. Electronic time stamps are a valuable tool in the context of electronic transactions where the date plays a significant role in the verification and authentication process of various events, data, documents, agreements or certificates. It is a kind of time attestation in electronic form which binds whatever kind of electronic data to a particular time establishing evidence that the latter data existed at that time.



Figure 1: Types of timestamps

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.

Qualified electronic time stamps provided by qualified trust service providers ensure benefiting from a high level of security and legal certainty of trust services. Qualified electronic time stamps 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.

1.6 Scope of the present document and relationship with other recommendations

This document proposes **security guidelines on the appropriate use of qualified electronic time stamps**. It aims to support relying parties and end users of qualified electronic time stamping services to securely use these services.

The target audience of the document are end users and relying parties of qualified electronic time stamping services. This could comprise individuals, businesses and public administrations. For example, it could be a public administration that wishes to use a (qualified) electronic seal and a qualified electronic time stamp for its 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 being maintained.

The present document is organised to provide information and guidance with regards to the following aspects of qualified electronic time stamp:

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

Four other linked documents propose security guidelines on the appropriate use respectively of qualified electronic signatures, qualified electronic seals, qualified electronic registered delivery and qualified website authentication certificates.¹⁰

Although each of these qualified trust services share some technical backgrounds or tools and thus provide some common functionalities, such as 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 time stamp – what is it?

2.1 Official time

Since the end of the 19th century, an internationally recognised time-scale as a basis of time measurement, has become a true necessity in civil society. The Universal Coordinated Time (UTC), the time-scale provided by the BIPM (Bureau International des Poids et Mesures - International Bureau for Weights and Measures), currently fulfils this function and is widely used as the basis of legal time around the world.

Note: Standard time divides the world into 24 “time zones”, each one covering, in theory at least, 15 degrees. All clocks within one of those time zones should be set to the same time. Greenwich Mean Time (GMT), a time measurement based on Earth rotation, was initially used to determine the standard time for each zone. For most practical purposes UTC, the modern successor of GMT, is equivalent to mean solar time at the prime meridian (0°). More specifically, UTC is a compromise between the highly stable atomic time (TAI - Temps Atomique International) and solar time derived from the irregular Earth rotation (related to the Greenwich mean sidereal time (GMST) by a conventional relationship) UTC forms the basis of a coordinated dissemination of standard frequencies and time signals. It corresponds exactly in rate with TAI but differs from it by an integer number of seconds. The full definition of UTC is contained in Recommendation ITU-R TF.460-6 [1].

2.2 Electronic time stamp

An **electronic time stamp** is a piece of data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.



Figure 3: Examples of “paper-based” time stamps

An electronic time stamp aims to achieve the same goal as a “paper based” time stamp, i.e. establishing that a document, sending, or act has been established before or at a specific date and time.

Obtaining a time stamp on an electronic document usually consists in sending a **hash value**¹¹ of a file to a time stamp service (e.g. server) from time stamp service provider, for example via Internet. The time

¹¹ See glossary.

stamp service adds the current date & time, signs it or seals it and sends back the signed/sealed time stamp to the requester.

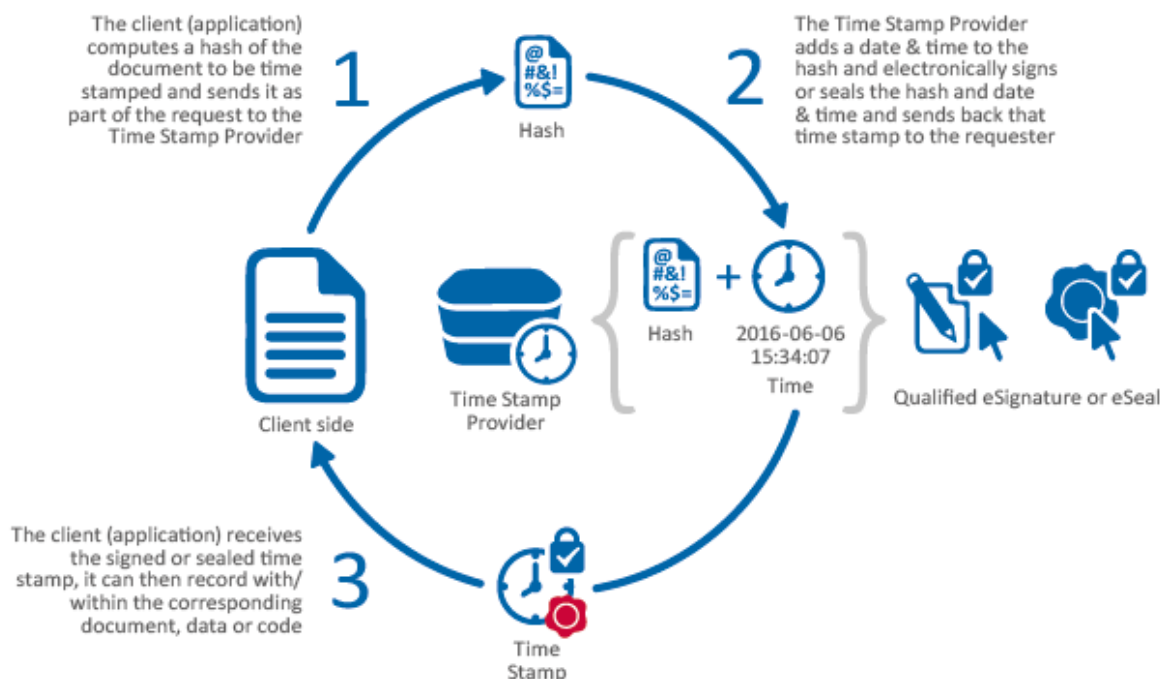


Figure 2: High level overview of the time stamp process flow

The time stamp, i.e. the signed/sealed combination of the hash of the document and date & time, proves that the hashed document and its content existed at that date & time. The time stamp service provider ensures that the clock used for time stamping is correctly synchronised with UTC.

Variants include sending the file (document) directly to the time stamp service provider, not just the hash of it. The service provider does not only time stamp the file but also archives the file and sends the requester an acknowledgement of receipt.

Note: As a standard best practice, a time stamp includes a reference to a time stamping policy, i.e. a document disclosing information on the rules and practices followed by the time stamp service provider when creating such a time stamp. This is particularly relevant to the requester and/or the verifier of a time stamp, when referring to the general terms & conditions and policies/practices documents of the provider to determine the level of quality, security an accuracy of the service and of the time stamp (e.g. an accuracy of 1 second, or worse or better).

2.3 Qualified electronic time stamp

The service consisting in the creation and provision of time stamps is a trust service, i.e. electronic service that enhances trust and confidence in electronic transactions.

The eIDAS Regulation introduces the notions of qualified trust services and qualified trust service provider with a view to indicating requirements and obligations that ensure high-level security of whatever qualified trust services and products are used or provided.

When looking for trust services, selecting qualified ones ensures benefiting from a high level of security and legal certainty of trust services. Qualified electronic time stamps 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.

A qualified time stamp, as specified by the eIDAS Regulation, must be based on an accurate time source linked to Coordinated Universal Time (i.e. the clock used for time stamping is correctly synchronised with UTC) and bind the date and time to the time stamped data in such a manner as to reasonably preclude the possibility of the data being changed undetectably (i.e. data integrity is maintained). It must also be signed using an advanced electronic signature or sealed with an advanced **electronic seal**¹² of the qualified trust service provider, or by some equivalent method. That advanced electronic signature or seal, when based on PKI-based cryptography will actually ensure proof of integrity of the time stamped data in situation illustrated in Figure 2.

Note: A trust service provider (TSP) providing time-stamping services to the public, is called a time stamping authority (TSA). The TSA has overall responsibility for the provision of its time stamping services, covering the operation of one or more time stamping units (TSUs) which are the technical server that create and sign the time stamps on behalf of the TSA. Each and every time stamp should identify the responsible TSA through its signature.

¹² See Glossary.

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

3.1 Legal properties

Legal presumption of the accuracy of the date and time of the stamped data & integrity of that data

From a legal point of view, the accuracy of the date and time in a qualified time stamp and the integrity of the corresponding time stamped data are legally presumed and recognised as such all over the EU.

3.2 Security properties

Accuracy of the date and time

The accuracy of the date and the time indicated in a qualified time stamp is ensured.

Data integrity

The integrity of the data to which the date and time are bound in a qualified time stamp is ensured via the **hash value** and the signature/seal on the time stamp. In other words, it is guaranteed that any alteration to the time stamped data can be detected.

The integrity of the qualified time stamp itself is ensured via the electronic signature or seal of the qualified time stamp provider.

3.3 Functional properties

Date and time attestation

From a functional point of view, a qualified electronic time stamp is a kind of time attestation in electronic form which binds whatever kind of electronic data to a particular time establishing evidence that the latter data existed at that time.

Identification of the qualified time stamp provider

Furthermore, as a qualified time stamp needs to be signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method, the qualified time stamp itself:

- Allows the identification of the qualified trust service provider to which it is uniquely linked, and
- Is also protected for integrity as the time stamp is signed/sealed in such a way that any subsequent change in the time stamp itself is detectable.

The identification of the qualified trust service provider having issued the qualified time stamp is provided by the certificate supporting the validation of the advanced electronic signature or seal of the qualified time stamp provider. The QTSP name, its postal and electronic address can in fine be found in the national trusted list when validating the qualified status of the time stamp and of its provider.

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

4.1 No prevention of document alteration

While a qualified time stamp guarantees that any alteration to the time stamped data can be detected, it provides no guarantee that such alteration will not happen. In other words, it does not prevent any alteration on the content of the time stamped document, but it allows detecting any alteration once it is time stamped.

4.2 Confidentiality

A qualified time stamp provides no guarantee that the time stamped data will remain confidential when sent over to recipients.

There is however no need to disclose the data to be time stamped towards the time stamp provider as the time stamp request is only including a **hash value** of that data.

4.3 No proof of sending/receipt

The qualified time stamp provides no guarantee that the time stamped document has been effectively sent to a certain recipient or has been received by a certain recipient. Those guarantees must be explicitly provided in addition to the security and legal properties provided by the qualified time stamp.

Note: For obtaining a proof of sending/receipt, a user should subscribe to qualified electronic delivery services that includes qualified time stamps embedded in such a proof.

4.4 No proof of origin on the time stamped data

The qualified time stamp provides no guarantee that the time stamped document originates from a certain party (no proof of origin of the document).

Note: For obtaining a proof of origin on the time stamped data, a user should create a qualified electronic signature as a natural person (or qualified electronic seal as a legal person) as such signature (seal) may be combined with the use of qualified time stamp. Alternatively, a qualified electronic delivery services that includes qualified time stamps embedded in such a proof may be used to obtain proof of origin on the time stamped data.

4.5 No signing or content commitment on time stamped data

The qualified time stamp provides no guarantee that the document owner or time stamp requester is clearly identified.

The time stamp is not a signature from the document owner and does not bear itself any commitment on the content of the time stamped document (no electronic signature of the document).

Note: For obtaining a proof of commitment on time stamped data, qualified time stamps may be combined with qualified electronic signatures not only to time stamp the data but to sign it as well.

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

5.1 Overview and context of the given examples

In general and to put (qualified) electronic time stamps in context, they are most often seen coming in addition to electronic signatures. Indeed, when advanced/qualified electronic signatures are implemented, the sole creation of the signature by the signer of a file, document or data does not make it possible to tell when the signature was created.

Moreover, and often forgotten, without such a time indication, it is not possible to verify that the signer’s public key certificate was valid (not revoked & not suspended) at the time of signing and that the signature had an advanced quality at the time of signing. Worse, longer term validation of an electronic signature might be impossible (for which reason and as explained elsewhere in these series of documents, standards have been issued on how to establish electronic signatures which provide for longer term validation assurance).

In this context (and although the properties of qualified electronic time stamps have been described above), we’d like to highlight the properties which are key for the use case examples mentioned below:

- Qualified time stamps can enjoy 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.
- This exact moment in time can be validated beyond reasonable doubt by all parties having access to the data and the related timestamp.
- If correctly set up this assurance of the exact moment in time associated to the time stamped document or data can cover a very long period of time¹³.

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 qualified time stamps.

	C2C	C2B C2G	B2B	B2G B2A	G2G A2A
Establishing the time of signing (and deposition) of a document/declaration	•	••	••	••	
Establishing the time of issuance of official documents/attestations	•	••	••	•	••
Establishing the time of conclusion of a contract	•	•	•	•	

¹³ The study of long term aspects, and in particular the erosion of the evidentiary values of digital signatures have lead standardisation organisation, like ETSI, to publish European standards on digital signature formats specifying all the elements required to prove the validity of a signature long after the normal life time of the essential elements of an electronic signature. All those elements form a so-called validation data set that needs to be preserved/archived in its entirety.

	C2C	C2B C2G	B2B	B2G B2A	G2G A2A
Enforcing legal/procedural/contractual time limits		•	•	••	
Long term validity of electronic records	••	••	••	••	••
Preservation of electronic records		••	••	••	••
Notarizing the exact chronology of events		•	••	••	

Table 2: QTStamp application areas

5.2 Establishing the time of signing (and deposition) of a document/declaration

When a document is signed by a person or business or administration and passed to another party, there is no way to be certain of the exact time at which the document was signed. Indeed an electronic signature will only provide authenticity, integrity and non-repudiation. Without a trustworthy time stamp the signer(s) can declare whatever time they chose to put on the document (before signing). In processes where this is to be avoided it is highly recommended to include a qualified electronic time stamp (in the sense as described in this document) as to establish at what time exactly this document was signed.



Figure 3: Example of establishing the time of signing

Examples of concrete application are:

- C2C/C2B: a person giving a relative or an accountant a mandate for a month (whereby the mandate must be signed “recently”).
- B2G: submitting declarations to government (which needs to be signed by mandated person at that moment in time).

5.3 Establishing the time of issuance of official documents/attestations

Certain government documents have to be signed by an official instead of by an administration (the latter would be an electronic seal for which we refer to the respective other document in this series). In that case and as official documents / attestation (e.g. VAT-certificate, confirmation of place of residency) need to bear a clear date of issuance, qualified time stamps can provide for the necessary certainty.


Examples of concrete application are:

- G2C / G2B: government generating attestations for individuals or companies.

- G2G / A2A: government (administrations) exchanging official information with each other whereby there should be no doubt about the date of issuance (e.g. police report to Ministry of Justice).

5.4 Establishing the time of conclusion of a contract

In some jurisdictions, the establishment of a fixed date and time (e.g. by official registration) is necessary in order to ensure the validity of a contract. Contracting parties are free to set the contract terms and conditions including the applicable date & time, being actual date and time or a different one. However, the moment of signing might be of great importance (e.g. because of applicable terms & conditions at the date of signing, because of damage claims in case of late delivery, or because of promotional conditions). Qualified time stamps allow to establish the exact moment of signing without the need for a contract registration.



Date	Title	Signatories	Status
09-03-13	contract_john_doe	● John Doe - In pending	● in progres
11-02-13	2013 Membership app	● Sarah Smith - Signed on 11 Feb. 2013 at 10:53	● signed
08-02-13	Insurance_contract_pdf	● John Smith - Signed on 08 Feb. 2013 at 20:12 ● Katy Jones - Signed on 08 Feb. 2013 at 20:47	● signed
03-09-12	Quote_Jack	● Luke Carter - Signed on 03 Sep. 2012 at 16:25 ● John Smith - Signed on 03 Sep. 2012 at 16:52	● signed

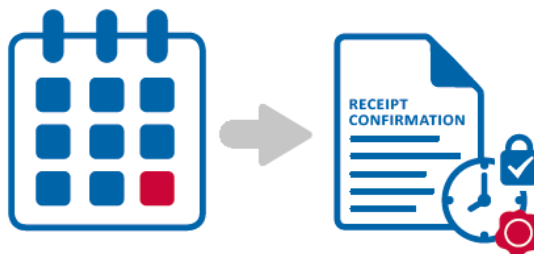
Figure 4: Example of establishing a fixed date and time

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.

5.5 Enforcing legal/procedural/contractual time limits

The application of time limits is particularly relevant in administrative and judicial procedures. E.g. public procurement rules require in substance that the devices for the electronic receipt of tenders or procedural requests must guarantee their exact time and date. E.g. in court procedures time limits play also a crucial role, in particular in those cases requiring strict formal rules where a specific time limit is determined, e.g. for filling a request, for submitting an opposition or an appeal. Magistrates, court clerks, bailiffs, lawyers, public notaries and civil servants could become heavy users of qualified time stamps in the near future.



Examples of concrete application are:

- B2G: provisioning of time-stamped receipts upon submission of a proposal.
- A2G: time stamping submitted documents when submitted to courts of justice.

5.6 Long term validity of electronic records

In some case the validity of signatures on certain documents needs to be verifiable over a long period of time because their legal effect will stay into force for a very long period of time (e.g. bank documents which need to be preserved for x years after expiry of the contract). Electronic timestamps can come there to the rescue as formats have been standardized which include the use of electronic timestamps to ensure the ability for longer term validation of the signature. In Figure 5 below the Document Security Store (DSS) extension is included in the document. The life-time of the protection can be further extended beyond the life-time of the last document time-stamp applied by adding further DSS information to validate the previous last document time-stamp along with a new document time-stamp.

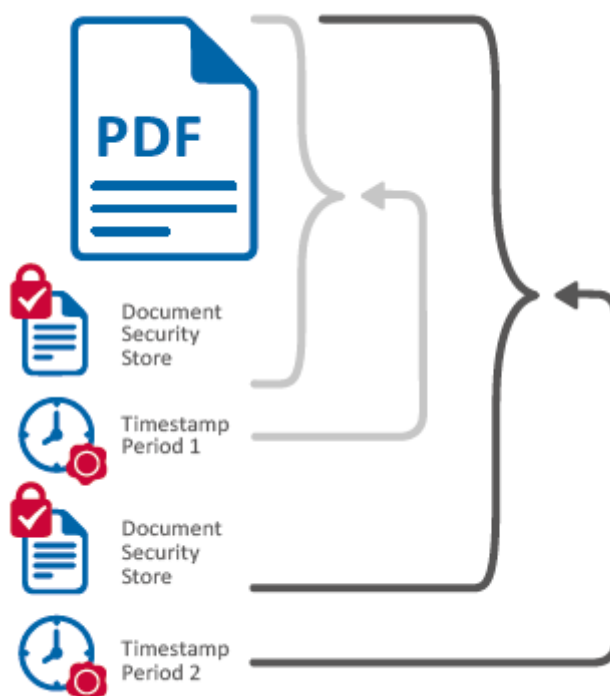


Figure 5: Example of long term validity of a document

Examples of concrete application are:

- C2B: signature on contracts between citizens and banks.
- C2G: signatures on digital building permits.

5.7 Long term preservation of electronic records

In extension to the above use case, there are many official/contractual documents which have to be preserved for a very long time. Also here qualified electronic time stamps can be used to timestamp documents on the moment of submission or be used to resign periodically as to establish the fact that the entity preserving the documents can attest that these were the original signed files. Note however that

qualified time stamps cannot be the only tool to satisfy a correct preservation of electronic records; for that, an appropriate strategy encompassing all aspects of their preservation must be implemented, monitored and maintained.



Figure 6: Example of long term preservation of records

Examples of concrete application are:

- C2B: Archiving consents/mandates given to a bank.
- C2G: Signatures on digital building permits.

5.8 Notarizing the exact chronology of events

In some circumstances, the exact chronological order will be essential in order to grant specific rights. For example, accountancy laws also attach a great importance to the unchangeable nature of bookings, hence in the exactness of the established chronological order. European eInvoicing rules also require electronic invoices to be dated and to be numbered in a chronological order, each invoice being part of an audit trail.



Figure 7: Example of notarizing chronology of events

Examples of concrete application are:

- C2A: many acts laid down at notaries need to be notarized with a clear date/time/sequence of events.

B2G: companies laying down patents or registering a trademark want to be very sure they were the first to register.

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

6.1 Security guidelines & levels

In this section, we propose recommendations according to three levels which represent the “strength/rigorousness” with which qualified time stamping 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 electronic time stamps provides legal reward compared to non-qualified ones as they enjoy 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.

As a basic recommendation, relying parties should look for the EU trust mark for qualified (time stamping) trust services when selecting providers. In addition, the relying party should read the applicable terms and conditions, the policies and practices used by the QTSP providing qualified time stamps.

As those documents may become long and heavy to read, best practice for a QTSP is to issue a Policy Disclosure Statement summarising the most important provisions related to the provision of its services.

Relying parties should look out for the accuracy of the qualified time stamp which must be of 1 second or even better.

All scenarios where a QTSP providing qualified time stamps stores hashes of files or the files themselves require strong guarantees with regards to the long term permanency and solvency of the QTSP.

6.3 RECOMMENDED

Relying parties should validate the use of the EU trust mark for qualified (time stamping) trust services when selecting providers by browsing the corresponding national trusted list.

The provider making use of the EU trust mark must be listed in that TL. As TL are organised per TSP, searches should be based on the name, trade name, VAT or official register number, when applicable. Once the TSP found as listed in the relevant TL, it must have been granted a qualified status for the provisioning of qualified time stamps: search for a qualified trust service type corresponding to the creation of qualified time stamps (i.e. for the URI <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>) for which the current status is to be “granted” (<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>).

When validating a claimed qualified time stamp:

- Validate the signature/seal of the time stamp,
- Identify the time stamp provider and its country of establishment from the signature/seal certificate,
- Identify, when applicable, the time stamping policy from the time stamp (e.g. a policy identifier that is specific to the provider and must be compared to its declaration of time stamp policies and/or practices, or a standard policy like ETSI best-practices-ts-policy 0.4.0.2023.1.1)
- Look out the national trusted list from the country of establishment of the time stamp provider to check its qualified status and qualified status of the time stamp (see B+ and qualified status must be “granted” at time stamp date & time).

Applicable terms and conditions, the policies and practices used by the QTSP to provide its qualified time stamps should be available from the “TSP information URI”

TSP information URI is the URI associated to the TSP information in the trusted list from where the TSP has the obligation to provide access to its terms and conditions, policies and practices (to be found as part of the TSP information as listed in the relevant EU MS trusted list).

For obtaining a proof of sending/receipt, use qualified electronic delivery services that includes qualified time stamps embedded in such a proof.

For obtaining a proof of origin on the time stamped data, use qualified electronic signature as a natural person (or qualified electronic seal as a legal person) as such signature (seal) may be combined with the use of qualified time stamp.

Alternatively, a qualified electronic delivery services that includes qualified time stamps embedded in such a proof may be used to obtain proof of origin on the time stamped data.

For obtaining a proof of commitment on time stamped data, qualified time stamps may be combined with qualified electronic signatures.

6.4 ENHANCED

When validated time stamp reveals to be non-qualified, evaluate the applicable terms and conditions, the policies and practices used by the TSP to provide its time stamp.

In particular look up for claimed compliance to relevant standards (see clause above) and the effective audit program confirming such compliance.

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

7.1 Implementing time stamping in off-the-shelf applications (user perspective)

When making use of an off-the-shelf application allowing to create certificate-based digital signatures, one can usually configure it to include the date and time the document has been signed as part of the certificate-based signature. As seen in the present document, time stamp helps to establish when the document has been signed and reduces the chances of an invalid signature.

Time stamps are easier to verify when they are associated with a trusted time stamp authority certificate. One can obtain a qualified time stamp from a qualified trust service provider or time stamp authority. Sometimes, the (qualified) certificate authority that issued digital IDs may also provide (qualified) time stamps.

Usually, time stamps appear in the signature field and in the signature properties dialog box of the end-user application. If a time stamp server/service is configured, the time stamp appears in the field related to the date & time of the signature properties dialog box. If no time stamp server/service is configured, the signatures field displays the local time of the computer at the moment of signing.

If a (qualified) time stamp was not embedded when signing the document, it can later be added to the signature. A (qualified) time stamp applied after signing a document uses the time provided by the (qualified) time stamp server/service.

In order to configure a time stamp server/service in an off-the-shelf application, one needs the server name and the URL, which can be obtained from an administrator or from a security settings file downloaded from a trusted source, including (qualified) time stamp trust service providers. Before installing a security settings file, a check with the competent system administration or IT department is advised. Checking the application configuration manual for properly configuring the (qualified) time stamp server name, the URL and other optional settings if any is also a good start.

7.2 Implementing time stamping from APIs and other tool kits (expert perspective)

As a pre-requisite to the implementation of (qualified) time stamps in business electronic processes should start with a proper, complete and as detailed as possible analysis of the business processes (description and modelling of complex business electronic processes) within which one or more time stamps need to be implemented. This aims to ensure that all the details related to crucial aspects of the business electronic process are actually well captured and that the implementation of time stamps does not miss any of them. It also includes a risk assessment, as a way of getting the needed information from which policy and security requirements are identified, so that once they are satisfied, stakeholders are sure that the implementation is done in such a way that it actually counters the identified risks.

This is particularly true when (qualified) time stamps are to be implemented within or in conjunction with (qualified) electronic signatures. To this extent the ETSI technical report TR 119 100¹⁴ provides a business

¹⁴ ETSI TR 119 100: “Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for signature creation and validation”. Starting from a business analysis and risk analysis of the business' electronic processes, stakeholders are guided for making the best choice among the wide offer of standards in order to ensure the best

driven guided process for implementing generation and validation of digital signatures in business' electronic processes.

A wide range of market available products offer the ability to enterprise/business process architects, application architects, and application developers to benefit from APIs and toolkits for integrating time stamps in their applications or services.

CEF eSignature building block

With regards to off-the-shelf toolkits allowing 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 qualified electronic signatures, allowing use and integration of time stamping services provided by any time stamp service provider through standard interfaces.¹⁵

Time stamp service APIs and tool kits from time stamp service providers

Most often, implementers may obtain time stamp server/service APIs and tool kits from their (qualified) time stamp trust service providers.

Relevant standards regarding the creation and validation of time stamps

- ETSI EN 319 421: “Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps”.

This document specifies policy and security requirements relating to the operation and management practices of TSPs issuing time stamps and references ETSI EN 319 401 for generic requirements. Those policy requirements are applicable to TSPs issuing time stamps. Such time stamps can be used in support of digital signatures or for any application requiring to prove that a data existed before a particular time. The document can be used by independent bodies as the basis for confirming that a TSP can be trusted for issuing time stamps. An informative annex provides check lists that can be used by the TSP to prepare an assessment of its practices against the document and/or by the assessor when conducting the assessment for confirming that a TSP meets those requirements

- ETSI EN 319 422: “Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles”.

This document defines a profile for the time stamping protocol and the time stamp token defined in IETF RFC 3161 including optional ESSCertIDv2 update in IETF RFC 5816. It defines what a time stamping client supports and what a time-stamping server supports. Time stamp validation is out of scope and is defined in ETSI EN 319 102.

- ETSI TS 119 142-3: “Electronic Signatures and Infrastructures (ESI); PAdES Document Time-stamp digital signatures (PAdES-DTS)”.

implementation of digital signatures within the addressed application/business electronic processes. It also cover the use of time stamps within or in conjunction with electronic signatures.

¹⁵ 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.

This document specifies a format for PAdES digital signatures using a Document Time-Stamp as a digital signature intended to specifically prove the integrity and existence of a PDF document as defined in ISO 32000-1, rather than proving any form of authentication or proof of origin.

- IETF RFC 3161: “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”.

It describes the format of a request sent to a Time Stamping Authority (TSA) and of the response that is returned. It also establishes several security-relevant requirements for TSA operation, with regards to processing requests to generate responses.

- IETF RFC 5816: “ESSCertIDv2 Update for RFC 3161”.

This document updates RFC 3161. It allows the use of ESSCertIDv2, as defined in RFC 5035, to specify the hash of a signer certificate when the hash is calculated with a function other than the Secure Hash Algorithm (SHA-1).

- ANSI ASC X9.95: “Trusted Time Stamp Management and Security”.

This standard specifies the minimum security requirements for the effective use of time stamps in a financial services environment. It augments the RFC 3161 standard with data-level security requirements to ensure data integrity against a reliable time source that is provable to any third party

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. These 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 block

The Connecting Europe Facility¹⁶ (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^{17,18}.

The CEF eSignature solution¹⁹ 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.

¹⁶ <https://ec.europa.eu/digital-single-market/connecting-europe-facility>.

¹⁷ 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.

¹⁸ 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 the eIDAS Regulation.

¹⁹ 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

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

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.

Hyper Text Transport Protocol (HTTP): A communication protocol used to connect to servers on the WWW. It establishes basically a connection with a web server and transmit information (e.g. HTML pages) to the client browser.

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).

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

Web server: using the client/server model and the WWW HTTP, web server is a software program that serves web page files to users

World Wide Web (WWW): Also shortened to Web. The World Wide Web is an information space where documents and other web resources are identified by URLs, interlinked by hypertext links, and can be accessed via the Internet.

A.11 Acronyms

ABBREVIATION	DESCRIPTION
A2A	Administration to Administration
B2A	Business to Administration
B2B	Business to Business
B2C	Business to Consumer
B2G	Business to Government
CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
CEN	Centre Européen de Normalisation
C2B	Consumer to Business
C2C	Consumer to Consumer
C2G	Consumer to Government
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

ABBREVIATION	DESCRIPTION
IETF	Internet Engineering Task Force
MS	Member State
PKI	Public Key Infrastructure
Q&A	Questions and Answers
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
SME	Small and Medium-sized Enterprise
TR	Technical Report
TS	Technical Specifications
TSA	Time Stamping Authority
TSP	Trust Service Provider
TSU	Time Stamping Unit
UTC	Universal Coordinated Time
WWW	World Wide Web

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

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

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

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

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

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

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

- **“Standard”** would entail any usage of a trust service under normal circumstance like but not limited to use cases e.g. involving financial exchange of a rather limited amount, personal records

with limited potential impact, or access to data/services of a limited classification level (e.g. internal/restraint).

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

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

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

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

Annex C: References and bibliography

C.1 References

REF. ID	DESCRIPTION
[1]	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014, p. 73–114.
[2]	Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".

C.2 Bibliography

ID	DESCRIPTION
(a)	Jos Dumortier & Hannelore Dekeyser: "The Regulatory Framework for Trusted Time Services in Europe", S.Paulus, N. Pohlmann, H. Reimer (Editors): ISSE 2005 Securing Electronic Business Processes, Vieweg (2005), 107-119.

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). C/2015/3364. 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.

Annex D: Frequently asked questions

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

The European Commission compiled 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 compiled 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.2 How can I find a qualified trust service provider issuing qualified time stamps?

You can find a qualified trust service provider providing qualified time stamps by looking:

- For the use of the EU trust mark for qualified trust services associated to the provision of qualified time stamps 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 identifying the issuance of qualified time stamps (<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>) 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 time stamps 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-06-16-355-EN-N



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

ISBN: 978-92-9204-215-8
DOI: 10.2824/4115

