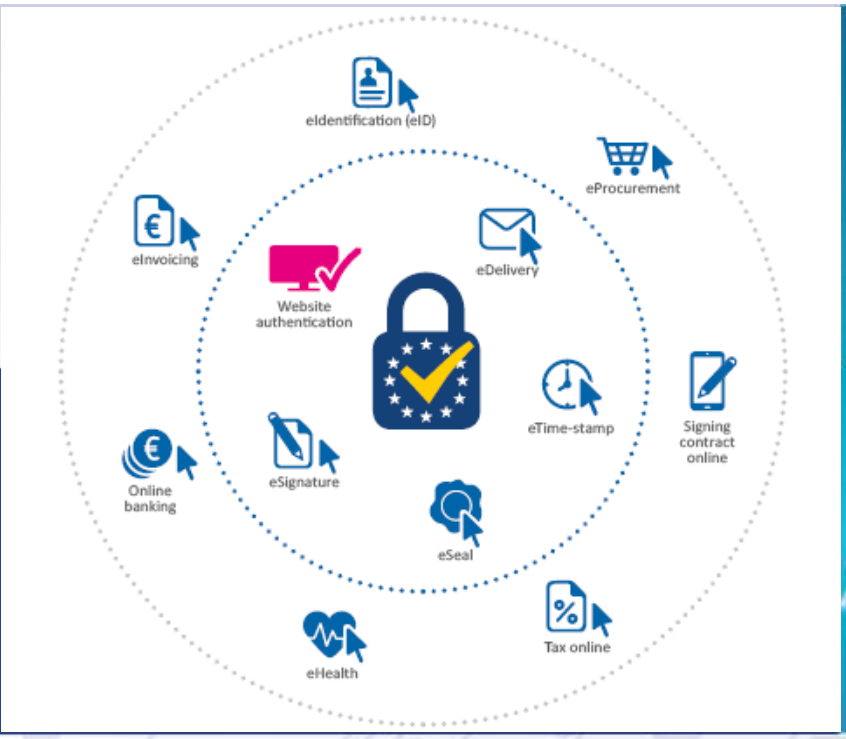


Security guidelines on the appropriate use of qualified website authentication certificates

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 enquires about this paper, please use press@enisa.europa.eu.

ISBN 978-92-9204-216-5, DOI 10.2824/353108

Table of Contents

Executive Summary

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

The eIDAS Regulation represented a big step forward in building a digital single market as it provides one common legal framework for all parties relying or providing on those kind of services. Indeed, various sectors of the economy (e.g. finance, banking, transport, insurance, health, sharing economy, trading, etc.) where obligations exist for security, reliable identification, strong authentication, legal certainty of evidences, will clearly be positively affected by the eIDAS Regulation. This latter will indeed allow citizens, businesses and public administrations to meet such obligations for any (cross-border) electronic transaction as they will now be able to use the recognised eID means and (qualified) trust services.

This document addresses qualified certificates for website authentication and is one out of a series of five documents which aim to assist parties wishing 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 certificate for website authentication is and what properties/function it does and does not provide, the following concrete examples of use are given as examples:

- Accessing an online government service;
- Accessing an eCommerce / eBanking website;
- Supporting secure G2G/B2B/B2G-communications;
- Securing payment (or other sensitive) services.

Next to the above, 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. This is expressed in three levels for relying parties:

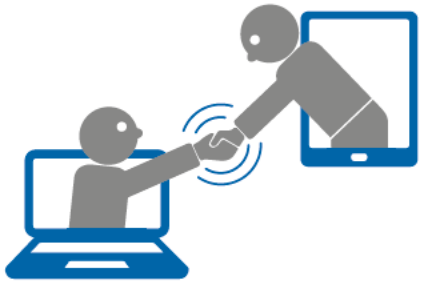
- Basic/Minimum recommended level of implementation to be followed by entities or in processes dealing with normal levels of criticality of data and therefor can live with a lower maturity in implementing trust services (technology).
- (Standard) Recommended level of implementation to be followed by 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 recommended level of implementation 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)

1. Introduction

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

Regulation (EU) No 910/2014[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 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 the eIDAS Regulation

The opportunities reside 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

[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.

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 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 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

[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).

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].

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 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

[4] See glossary
[5] See glossary.

electronic seals, qualified electronic time stamps services, and qualified electronic registered delivery services.[6]

For marketing purposes, once qualified, a QTSP/QTS may use the EU Trust Mark for qualified trust services when promoting its QTS. 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.[7] Basically, this secondary legislation sets the form, colour and size of the EU trust mark, sets the obligation to clearly indicate the qualified services that the EU trust mark pertains to, and allows association with other graphical or textual elements provided that certain conditions are met. [8]

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 website authentication certificates

Certificates for website authentication, widely known as SSL/TLS certificates, play a critical role in the security of online transactions and have been long employed in internet by websites (it is estimated that

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

currently 57.1% use them, according to Web Technology Surveys[9]). This number has grown sharply in the last years driven by business needs rather than any regulatory framework, and the market has evolved to be highly concentrated in a small number of players, mostly from outside Europe. Today, it is possible to surf the internet and access different websites which are using the https protocol but do not give you any, or very little, information on the owner of the website except some specific certificates. With the qualified website authentication certificates, that information is provided and it also provides the legal assurance of it. These certificates benefit from full legal recognition thanks to the eIDAS Regulation.

Besides the legal framework, the technical framework is nowadays very mature thanks to the efforts of the CA/Browser forum which has developed requirements and guidelines for the issuance and management of these certificates and that the browsers have implemented in their own requirements.

The use of qualified website authentication certificates should help the development of online business and services in Europe and worldwide by securing online transactions and services in many sectors: e-business, e-administration, e-banking, e-services, etc.

This type of certificate provides real benefits to have a secure surfing of the internet in terms of security and legally, such as:

- **Protecting end users from online fraud**: Qualified website authentication certificates make website owners aware of the benefits that these certificates add to their sites for authentication. The website owners should also know that there are different levels of validations and checks, and thus different levels of security for those end users which use their websites. Adding a value to the end users letting them know the website they are visiting has the highest level of security will allow them to surf with confidence.
- **Protecting personal information during online transactions**: eIDAS Regulation sets clear requirements for website authentication certificates to be considered trustworthy together with minimal obligations for providers of such certificates with regard to the security of their operations and their liability. End users can be assured that there is a genuine and legitimate entity standing behind the website which contributes to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated.

1.6 Scope of this document and relationship with the other recommendations

This document proposes **security guidelines on the appropriate use of qualified website authentication certificates**. It aims to support relying parties and end users of qualified website authentication certificates to securely use these services.

The target audience of the document are end users and relying parties of qualified website authentication certificates. This could comprise individuals, businesses and public administrations. For example, it could be a public administration that wishes to use a qualified website authentication certificate 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 being maintained.

[9] http://w3techs.com/technologies/overview/ssl_certificate/all

This document provides information and guidance with regards to the following aspects of qualified website authentication certificate:

- 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 and practical usage aspects.

Four other linked documents propose security guidelines on the appropriate use respectively of qualified electronic signatures, qualified electronic seals, qualified electronic time stamps 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 illustrated below, each of them has its own objectives and core functionalities as summarised in Table 1 below:

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.

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

2. Qualified website authentication certificate – what is it?

2.1 Website Authentication Certificates in context

On the internet, sending sensitive information without secure protocols is like writing it on the back of a postcard and letting every postman or attacker on the way to its destination make a photocopy of it. The lack of implementation of a secure protocol implies that everything is being delivered in a way that anyone can see it.

This is where cryptography comes into play .The core principle is to take a plain text message and, through a series of transpositions and substitutions, convert it to cipher text. This process is called encryption and it aims at protecting data and data transmission, preventing the contents of a message from being revealed even if the message itself were to be intercepted while in transit.

Figure 1: Website Authentication Certificates

The protocol to support this on the internet is called SSL/TLS. It encrypts the message in a way that, while in transit, an attacker cannot read its content as he/she cannot decipher it. SSL (Secure Sockets Layer) and newer protocol TLS (Transport Layer Security) provide a secure and authenticated channel between clients and servers on the internet.To perform these tasks digital certificates are needed because to protect communication a client using a browser can authenticate against a web server by verifying the signature of the server´s certificate.

2.2 Digital certificates

In cryptography a digital certificate, also known as public key certificate, is an electronic document that associates a subject, presumably the owner, with a public key. This certificate has information about this key, the identity of the owner and a signature of the entity that has verified the content of this certificate. A certificate is typically issued by a third party trusted issuing authority.

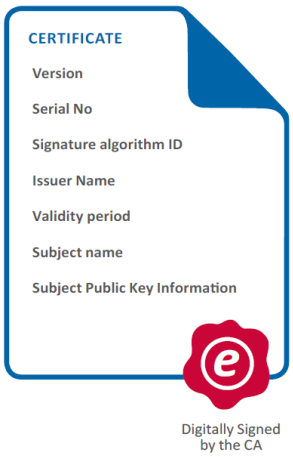


Figure 2: Example of a digital certificate

2.3 Website authentication certificates

Website authentication certificates can be used to authenticate websites, through a secure protocol, (SSL or TLS), and reflected in the website addresses by the prefix https instead of the normal http.

A generic definition of the website authentication certificates says that these are small data files that digitally bind a cryptographic key to a subject details. When installed on a web server, this allows secure connections from a web server to a browser. This type of certificate is commonly called SSL/TLS certificates.

The CA/Browser Forum (www.cabforum.org) has developed 2 documents (the baseline requirements and the Extended Validation guidelines) with policies for a guidance on the issuance and management of these SSL/TLS certificates.

Therefore, the main objective of these certificates is to enable encrypted communications with a Web site i.e. to facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a Web site. However, the main difference is how and what to validate to provide the end users with better information.

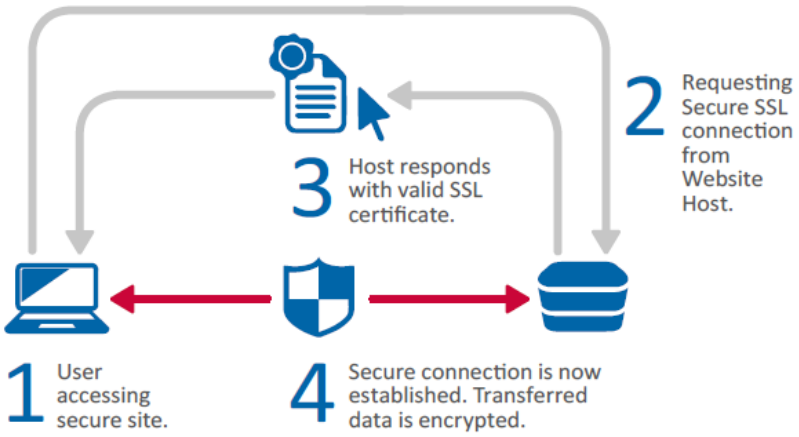


Figure 3: How Website authentication certificates work

According to the CA/Browser Forum, issuing this type of certificates requires certain validations to be carried out

beforehand and based on those validations, there can be different types of website authentication certificates issued (SSL/TLS certificates)

What are the different types of SSL Certificates?

Domain Validation (DV)

A Domain Validated SSL certificate is issued after proof that the owner has the right to use their domain is established. Many CAs perform additional fraud checks to minimize issuance of a certificate to a domain which may be similar to a high value domain. The certificate only contains the domain name. While the browser displays a padlock, examining the certificate alone will not show the legal person name as it was not a validated piece of information.

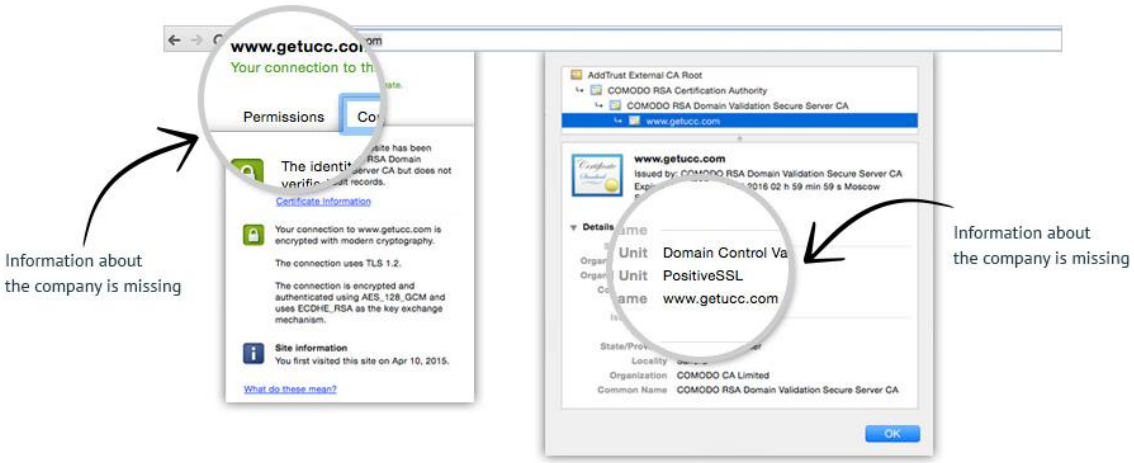


Figure 4: Example of a DV certificate[11]

This is an example of a DV certificate. By clicking on the padlock icon and later on the “view certificate” it´s possible to know the issuer and in the subject which indicates basically the domain name.

Organizational Validation (OV)

For OV certificates, CAs must validate the legal person name, domain name and other information through the use of public databases. CAs may also use additional methods to insure the information inserted into the certificate is accurate. The issued certificate will contain the legal person name and the domain name for which the certificate was issued for. Because of these additional checks, this is the minimum certificate

[11] www.leaderssl.com

recommended for ecommerce transactions as it provides the consumer with additional information about the business.

The main objective is to clearly identify the legal person or the natural person in case of an IV (Identity Validation) which is represented in the certificate information

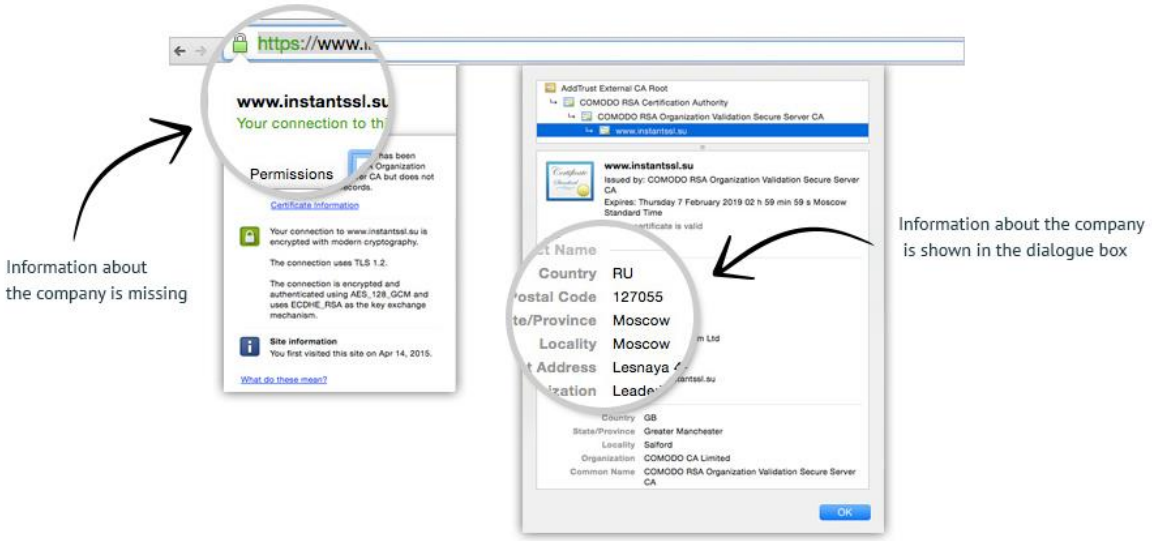


Figure 5: Example of an OV certificate[12]

This is an example of an OV certificate. Clicking on the padlock icon and later on the “view certificate” it´s possible to know the issuer and in the subject you can find additional information, such as the company to whom the certificate has been issued, location, etc.

Extended Validation (EV)

EV Certificates are only issued once an entity passes a strict authentication procedure. These checks are much more stringent than OV certificates.

The main objective is to identify the legal entity that controls a Web site i.e. to provide reasonable assurance to the user of an Internet browser that the Web site the user is accessing is managed by a specific legal entity identified in the EV Certificate by name, address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information.

The secondary purpose of an EV Certificate is to help establish the legitimacy of a business claiming to operate a Web site, and to provide a vehicle that can be used to assist in addressing problems related to phishing, malware, and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the business, EV Certificates may help to:

- Make it more difficult to mount phishing and other online identity fraud attacks using certificates;
- Assist organisations that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves to users; and

- Assist law enforcement organizations in their investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

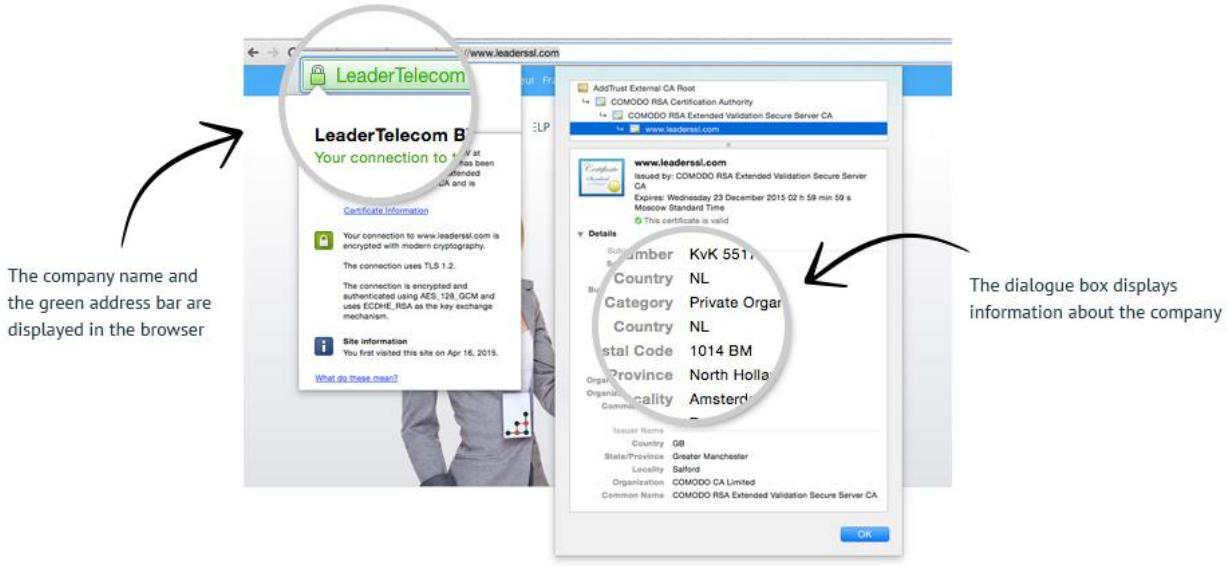


Figure 6: Example of an EV certificate[12]

This is an example of an EV certificate. Clicking on the padlock icon provides additional information on who verified it and when clicking on more information you´ll see the certificate subject and all the additional information contained.

One of the main and easy way to detect an EV certificate is the green colour in the browser bar, however every browser displays this differently.

In the next table, follows a comparison table with the validations that need to be performed and what additional features can be included or showed.

Type of certificate	Domain validated?	Subject Name Validated?	Address Validated?	Pad Lock Displayed by Browser?	Green address bar or other special treatment?	Relative price
DV	✓			✓		€
OV	✓	✓	✓	✓		€€
EV	✓	✓	✓	✓	✓	€€€

Table 2: Comparing the features of different types of certificates [ref CABF website]

2.4 Qualified website authentication certificates

The eIDAS Regulation, establishes a general legal framework for the use of trust services, including the provisioning of qualified website authentication certificates, making it possible, when meeting some provisions laid down in the Regulation, to use them to authenticate websites.

These qualified website authentication certificates offer legal assurance providing a presumption of accuracy of the information contained on the certificate

According to the next table it is seen that the EV and QWACs certificates seem basically the same.. From a technical point of view, they are very similar, the only difference is that the profile of the QWAC certificate includes some additional fields to be considered "qualified" according to the ETSI EN standards. From the legal point of view there are more differences because the QWACs are regulated by eIDAS.

Type of certificate	Domain validated?	Subject Name Validated?	Address Validated?	Pad Lock Displayed by Browser?	Green address bar or other special treatment?	Relative price
DV	✓			✓		€
OV	✓	✓	✓	✓		€€
EV	✓	✓	✓	✓	✓	€€€
QWAC	✓	✓	✓	✓	✓	€€€?

Table 3: Comparing the features of different types of certificates including QWAC

3. Qualified website authentication certificate – what key properties does it provide?

3.1 Legal properties

Attestation of the identity of a website and of its owner

QWACs benefit from EU wide recognition as a trustworthy authentication means for a website and links such an authenticated website to the natural or legal person to whom the certificate is issued.

Furthermore, since the provider of a QWAC needs to be a qualified trust service provider (QTSP), the burden of the proof of a correct execution of the provider's obligations laid down in the Regulation, (including those ensuring security, quality and trustworthiness) lies with that provider. Indeed, the intention or negligence of a QTSP shall be presumed unless it proves that the damage occurred without its intention or negligence.

Furthermore, the eIDAS reliable source for qualified certificates for website authentication is done through the national trusted lists and EU "List of the Lists". The trusted lists (TLs) have a constitutive value meaning that the qualified status of a certificate for website authentication can be only be confirmed by the inclusion in an EU TL of that qualified status as being granted to the QTSP and its certificate issuance service having issued such a certificate. The grant of a qualified status to a QTSPO and the qualified trust service it provides follows a strict EU harmonised procedure relying on a pre-authorisation and regular supervision and auditing process (see section 1.3).

When addressing the international level, and in particular providers established in non-EU countries, in order for them to have their certificates for website authentication recognised as QWACs or equivalent, they either need to set up a legal entity in one of the EU Member States and go through the pre-authorisation (initiation) procedure in order to be granted the qualified status by the competent supervisory body; or they may rely on an hypothetic agreement between their country of establishment and the European Union. The location of the technical infrastructure used by a QTSP issuing QWACs does not represent a legal impediment to the grant of the qualified status.

3.2 Security properties

Accuracy of the information contained in the certificate

Based on the CABF EV guidelines plus the legal requirements of the eIDAS regulation, the information on the subject of the certificate provides legal assurance as stated in section 2.3.

In order to prevent security cases like the one of Diginotar[12], the eIDAS regulation ensures:

[12] DigiNotar was a Dutch certificate authority owned by VASCO Data Security International. On September 3, 2011, after it had become clear that a security breach had resulted in the fraudulent issuing of certificates, the Dutch government took over operational management of DigiNotar's systems. That same month, the company was declared bankrupt.

- The transparency, the trustworthiness and the accountability for the qualified certificates for website authentication.
- A strengthened supervision system based on initial and regular audits supporting the verification by EU MS national supervisory bodies that the provisions laid down in the Regulation, including risk management obligations (both for Q and non-Q TSPs and services) are respected.
- Providers are liable for the services they provide.

Data integrity (of the certified information)

As mentioned above, the use of public key cryptography to issue QWACs ensures data integrity (as the certificate is signed in such a way that any subsequent change in the data is detectable).

Data origin authentication (of the certified information)

The use of public key cryptography to issue QWACs guarantees the proof of origin of the signed certificate data since only the QTSP having been in possession of the issuing CA private key can be at the origin of a data signed with the corresponding public key.

Furthermore, as a qualified website authentication certificate needs to be signed using an advanced electronic signature/seal of the qualified trust service provider, validating such a signature/seal allows the validation of the qualified trust service provider.

3.3 Functional properties

Identification of the subject

A qualified website authentication certificate ensures the identification of the subject 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 certificate imposed by the eIDAS regulation

Encryption of the communication (confidentiality)

The main objective of these certificates is to enable encrypted communication of information over the Internet between the user of an Internet browser and a web site hosted in a web server.

Identification of the qualified provider

As a qualified website authentication certificate needs to be signed using an advanced electronic signature/seal of the qualified trust service provider, validating such a signature/seal allows the validation of the qualified trust service provider.

3.4 Other properties

Recognized by browsers

When QWACs are recognised by Internet browser software, their validation provides a specific presentation (i.e. colouring the browser bar into green guaranteeing a specific treatment).

4. Qualified website authentication certificate – what properties can it not provide?

4.1 General User Experience

When surfing the internet, users should check the padlock "associated" to an https webpage, but does this mean that:

- The site is safe? *No*
- The site is secure? *No*
- The site is patched to an up-to-date version and has no vulnerabilities? *No*
- You know who the site is claimed to belong to? *Depends*
- The site is free of malware? *No*
- You can trust the site? *Up to you*

This type of certificate, SSL/TLS, only indicates that someone has control of the associated domain and that the data transmitted between you're the user's browser and this website is encrypted.

Taking into account that nowadays about 70% of the SSL certificates are DV certificates, this is problematic for protecting users from fraud. Even though nowadays, when everything is requested to be encrypted (they are required by the US government for all of its websites and by Google for assuring a better visibility when searching) consumers have a (gut) feeling of security and every time they see the HTTPS indicator or the padlock icon on a company website, they think that the website has passed all the validation methods, which is not true and could result in a lack of confidence.

4.2 Other features not provided

Time stamping

QWACs do not provide any proof on time accuracy because these type of certificates are not used nor intended for such use.

Signing or sealing

While QWACs can be issued either to natural persons or to legal persons, QWACs are not meant to be primarily used for signing by natural persons nor for sealing by legal person. In practice, those key usages are not included in QWACs.

Being meaningful, fair or true

When used to authenticate a website (using TSL/SSL protocols), QWACs are only used to authenticate[13] and encrypt the information exchanged between the website (server) and the client web browser but it gives no guarantee on the content displayed on the website or available from there.

[13] Such an authentication can be unidirectional (website towards the browser client) or mutual.

5. Qualified website authentication certificate – what are the potential use cases?

5.1 Overview and context of the given examples

In general, and to put QWACS in context, whilst they allow to verify the identity of the online service with great certainty, they form often the basis of a broader solution. Indeed, before starting to exchange information with an online service one needs to be able to be sure one is connected to the right service. After that the user connecting to that service often needs to identify/authenticate him/herself and documents being exchanged need to be signed for integrity/non-repudiation reasons, etc.

In this context (and although the properties of QWACS have been described above), we would like to highlight the properties which are key for the use case examples mentioned below:

- QWACS assert the identity of a certain online service.
- QWACS can be used in authenticating an online service

The properties mentioned allow several "types of use cases" which can be applied in many areas of application (which we will try to give examples of whilst discussing the use cases). 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 indication the huge added value of QWACS.

	C2C	C2B C2G	B2B	B2G B2A	G2G A2A
Accessing an online government service		●●		●●	●●
Accessing an eCommerce / eBanking website		●●	●●		
Supporting secure G2G/B2B/B2G-communications			●●	●●	●●
Securing payment (or other sensitive) services.			●●		

Table 4: QWACS application areas

5.2 Accessing an online government service

When accessing a government service, how can a citizen or employee/employer be sure he/she is connected to the right official government website and not connecting to a website trying to impersonate government services? For this, the user needs to have a way to identify and authenticate the online service he/she is connecting to. When used as a general guideline like "TLS always on", meaning that online services would use website certificates (qualified or e.g. extended validation) pervasively, this may provide a significant improvement in the assurance people would have when accessing government services. For

example, Spain regulates by law that all websites of all Spanish public administrations shall use a qualified website authentication certificate and all the information to the public shall be published there, as well all the online transactions citizens can perform. This provides people interacting with the Spanish authorities with the certainty that they know with whom they are interacting online.

Figure 7: Governmental website example

Examples of concrete applications include:

- C2G: Citizens accessing Tax-services, Social Security eHealth-services, etc.
- B2G : Business accessing all kind of reporting systems of the government, either via web interfaces or by direct interaction between their system and systems of the government.
- G2G: Government administrations which access services of other government administrations, like consultation of national registries, online input of certain reports/measurements into the systems of other administrations.

5.3 Accessing an eCommerce / eBanking website

When accessing an online commercial service, the same applies as in the previous use case: how can a user be sure he/she is connected to the right website and not connecting to a website trying to impersonate the banking-service he/she wants to connect to? For this, the user needs to have a way to identify and authenticate the online service he/she is connecting to. Here as well, when used as a general guideline like "TLS always on", meaning that online services would apply the use of website certificates (qualified or e.g. extended validation) pervasively, this may provide a significant improvement in the assurance people would have when accessing online services. In the context of payments or accesses to health related-information this should even be mandatory and people should be educated not to access services which cannot be identified and authenticated in a very strong way.

Figure 8: eBanking website example

Examples of concrete application are:

- C2B: A client accessing his bank account or performing any other kind of financial transaction
- B2B: A subcontracting accessing his client systems (or vice-versa) to manage client-data, to exchange invoices, etc.
- G2B: Officials accessing cloud services online which support their governmental task (e.g. outsourced market-intel-data, outsourced supervision-activity-related data).

5.4 Supporting secure G2G/B2B/B2G-communications

All too often QWACS are being interpreted as only being used in interactive access to "websites". One should note that QWACS can also be used in direct interaction between systems. Indeed, when in a business process two systems are linked together to exchange more-or-less sensitive data it is vital that both systems are able to identify and authenticate each other before starting to exchange any sensitive information.

Figure 9: Interaction between systems example

Examples of concrete application are:

- B2B: Suppliers constantly exchanging data with their clients (e.g. in context of just-in-time-delivery) or exchange of information in context of eProcurement/eInvoicing-processes.
- G2G: Systems exchanging social security information (e.g. pension data) across border in context of the mobility of the European workforce.

5.5 Securing payment (or other sensitive) services.

At the time of this writing, it is becoming clear that QWACS will also play an important role in context of exchange of payment information (PSD2) between payment service providers (PSPs). Indeed, when e.g. an account PSP is accessing an account holding PSP then it should be clear that no data can be exchanged in context of the protection of the data, as long as both parties have not strongly authenticated each other. It is obvious that over time QWACS will provide such assurance, not only in the payment industry but also in many other areas where sensitive data is being exchanged (e.g. eHealth, social security).

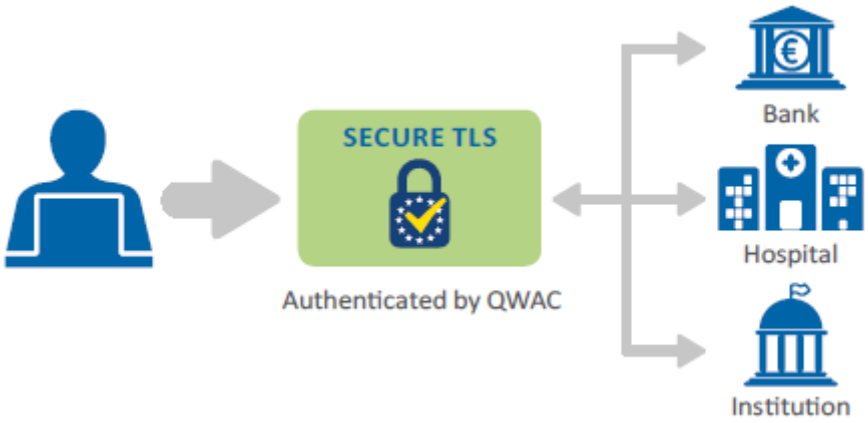


Figure 10: Critical/sensitive services example

Examples of concrete application are:

- B2B – PSP accessing an Account Holding PSP for acquiring account information.
- B2G – Reporting by social security institutions to government.
- A2A – hospitals exchanging payment information with other (supporting) medical institutions.

6. Qualified website authentication certificate – 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 website authentication certificate services should be applied in a specific context. This "strength/rigorousness" depends on the use case or type of application / environment in which website authentication certificate 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 dealing with normal level of criticality of data or having a low maturity in implementing this technology.
RECOMMENDED	for recommendations to be followed by entities dealing with important business data willing to take full advantage of this technology or having a fair maturity in implementing it.
ENHANCED	for recommendations to be followed by entities dealing with data of sensitive/high level of criticality or reaching a high maturity level in implementing this technology.

6.2 BASIC

Making use of qualified website authentication certificates provides legal reward compared to non-qualified ones as they enjoy the presumption of the accuracy of the information contained in the certificate.

Search for the EU trust mark for qualified (website authentication) trust services when selecting providers.

Look out for the green bar and padlock at the URI browser. Browsers may include all CA root certificates for those CAs issuing qualified website authentication certificates to grant the special status. This is after approval, in case of request from the TSP, as per its own root program requirements. If the CA root certificates are not included in the browser root programs, these won´t be shown in green colour.

Read the applicable terms and conditions, the policies and practices used by the QTSP to provide its qualified website authentication certificates i.e. a document disclosing information on the rules and practices followed by the TSP when creating and issuing such certificate.

As those documents may be lengthy , best practices is for QTSP to issue a Policy Disclosure Statement summarising the most important provisions related to the provision of its services. This is particularly relevant to the requester and/or the verifier of the certificate, when referring to the policies/practices documents of the provider to determine the level of quality, security an accuracy of the service. However, there is but limited guidance on the content of Policy Disclosure Statements (see [2]).

6.3 RECOMMENDED

A TSP is granted a qualified status for each type of qualified trust service covered by the eIDAS Regulation, and in practice for each technical instance of such a qualified trust service.

E.g. a QTSP qualified for the provisioning of qualified certificates is not per se granted a qualified status for the issuance of qualified website authentication certificates; it must first complete the full pre-authorisation process and have its granted qualified status for the provision of qualified website authentication certificates published explicitly in the national trusted list before issuing qualified website authentication certificates in addition to the provision of qualified certificates.

Check the correct use of the EU trust mark for qualified (website authentication) 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 website authentication certificates: search for a service type for which the current status is to be “granted” (http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted).

A trust service provider (TSP) providing website authentication certificates to the public, is called a publicly-trusted CA according to the CA/Browser Forum if the CA root certificate is included in any of the browser root program. A Qualified TSP providing qualified website authentication certificates will be called the same by the browsers root stores. There won´t be any difference for the browsers root programs.

Applicable terms and conditions, the policies and practices used by the QTSP to provide its qualified website authentication certificates should be available from the “TSP information URI” as part of the TSP information as listed in the relevant EU MS trusted list.

When validating a received a claimed qualified website authentication certificate:

- Identify the certificate provider and its country of establishment,
- Identify, when applicable, the policy for these certificates (e.g. a policy identifier that is specific to the provider and must be compared to its declaration of policies and/or practices, or a standard policy like ETSI or CA/Browser Forum)
- Look out the national trusted list from the country of establishment of the time stamp provider to check its qualified status and qualified status (see B+ and qualified status must be “granted” at time).

6.4 ENHANCED

When validated website authentication certificate reveals to be non-qualified, evaluate the applicable terms and conditions, the policies and practices used by the TSP to provide its QWACs. In particular look up for claimed compliance to relevant standards (see clause 6) and the effective audit program confirming such compliance.

7. Qualified website authentication certificate – example of tools & practical usage aspects

7.1 Implementing QWACs (user perspective)

From user's perspective there is no need for any implementation measures or activities. However he/she needs to be aware when navigating through the internet on web pages with the encryption enabled by simply looking for the padlock at the URI browser, at least as a basic procedure.

Once used for this type of navigation, the user can go further and look for the certificate used in the website allowing to clearly identify the owner of the certificate. In the case of a qualified website authentication certificate, like for an EV SSL certificate, the browser bar will turn into green allowing the user to clearly understand that this is a valuable type of certificate. From there, by looking into the certificate it can be checked that the certificate is qualified when further identifying the QC Statements as part of the certificate content display.

7.2 Relevant standards regarding QWACs (expert perspective)

ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements

This document specifies generally applicable policy and security requirements for Trust Service Providers (TSP) issuing public key certificates, including trusted web site certificates and references ETSI EN 319 401 for generic requirements. The policy and security requirements are defined in terms of requirements for the issuance, maintenance and life-cycle management of certificates.

This document is applicable to:

- the general requirements of certification in support of cryptographic mechanisms, including digital signatures and seals;
- the general requirements of certification authorities issuing TLS/SSL certificates;
- the general requirements of the use of cryptography for authentication and encryption.

ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

This document specifies policy and security requirements for the issuance, maintenance and life-cycle management of EU qualified certificates as defined in Regulation (EU) N° 910/2014, the eIDAS regulation. These policy and security requirements support reference certificate policies for the issuance, maintenance and life-cycle management of EU qualified certificates issued to natural persons (including natural persons associated with a legal person or a website) and to legal persons (including legal persons associated with a website), respectively.

This document provides in annex B a check list of the policy requirements specific to TSP issuing EU qualified certificates as well as all the requirements incorporated by reference to ETSI EN 319 411-1 and ETSI EN 319 401, that can be used by the TSP to prepare an assessment of its practices against this

document and/or by the assessor when conducting the assessment for confirming that a TSP meets the requirements for issuing qualified certificates under the eIDAS regulation.

ETSI EN 319 412-4: Electronic Signatures and Infrastructures (ESI); Certificate profiles; Part 4: Certificate profile for web site certificates

This document specifies a certificate profile for web site certificates that are accessed by the TLS protocol. The profile defined in this document builds on the CA/Browser Forum Baseline requirements and extended validation guidelines.

This document focuses on requirements on certificate content. Requirements on decoding and processing rules are limited to aspects required to process certificate content defined in the document. Further processing requirements are only specified for cases where it adds information that is necessary for the sake of interoperability.

This profile can be used for legal and natural persons. For certificates issued to legal persons, the profile builds on the CA/Browser Forum EV Profile. For certificates issued to natural persons, the profile builds only on CA/Browser Forum baseline requirements.

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 has 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 SSL PKI ecosystem

In the eIDAS recital 67, it´s said that "Website authentication services provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website. Those services contribute to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated. The provision and the use of website authentication services are entirely voluntary. However, in order for website authentication to become a means to boosting trust, providing a better experience for the user and furthering growth in the internal market, this Regulation should lay down minimal security and liability obligations for the providers and their services. To that end, the results of existing industry-led initiatives, for example the Certification Authorities/Browsers Forum — CA/Browser Forum, have been taken into account."

The eIDAS Regulation, defines this type of certificates as: 'certificate for website authentication' means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued.

And when these certificates are considered as qualified, then the definition is: 'qualified certificate for website authentication' means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV of the eIDAS regulation.

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.

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 1st 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.

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.

Domain Name System (DNS): The distributed name and address mechanism used on the internet.

Domain name: the name used to identify an internet host.

Domain Validation (DV) Certificate: certificate which has no validated organizational identity information for the subject, only identifying the subject by its domain name.

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

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

Extended Validation (EV) Certificate: certificate that contains subject information specified in the CABF EV Guidelines and that has been validated in accordance with those Guidelines.

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.

Internet: a global computer network that links minor computer networks allowing them to share information via standardized communication protocols.

Organizational Validation (OV) Certificate: certificate that includes validated organizational identity information for the subject.

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.

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

Secure Sockets Layer (SSL): SSL is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. TLS is the successor to SSL.

Transport Layer Security (TLS): TLS is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

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
TSA	Time Stamping Authority
A2A	Administration to Administration
B2A	Business to Administration
B2B	Business to Business
B2C	Business to Consumer
B2G	Business to Government
C2B	Consumer to Business
C2C	Consumer to Consumer
C2G	Consumer to Government
CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
CEN	Centre Européen de Normalisation
eID	electronic Identification
EN	European standard
ETSI	European Telecommunications Standardisation Institute
EU	European Union
G2G	Government to Government
HTTP	Hyper Text Transport Protocol
HTTPS	HTTP Secure
IETF	Internet Engineering Task Force
MS	Member State
PKI	Public Key Infrastructure
Q&A	Questions and Answers
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
SSLGMST	Secure Sockets LayerGreenwich Mean Sidereal Time
TLSGMT	Greenwich Mean TimeTransport Layer Security
TR	Technical Report
TS	Technical Specifications
TSP	Trust Service Provider

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

C.2 Bibliography

ID	DESCRIPTION
(a)	CA/Browser Forum recommendations.
(b)	The ETSI standards developed for TSPs be able to issue QWACS take into account the CA/Browser Forum EV guidelines for the policies as indicated in the ETSI EN 319 411-2 which refers the ETSI EN 319 411-1 and the ETSI EN 319 412-4 for the profile of the certificate.
(c)	ENISA report on Qualified website authentication certificates; promoting consumer trust in the website authentication market.
(d)	Wikipedia.
(e)	CA Day presentations.

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 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.2 How can I find a qualified trust service provider issuing qualified website authentication certificates?

You can find a qualified trust service provider issuing qualified website authentication certificates by looking:

- For the use of the EU trust mark for qualified trust services associated to the provision of qualified website authentication certificates 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 website authentication (service type identifier: http://uri.etsi.org/TrstSvc/Svctype/CA/QC and additional service information extension http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication) 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 website authentication certificates 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-06-16-356-EN-N

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

ISBN: 978-92-9204-216-5
DOI: 10.2824/353108