EUROPEAN UNION AGENCY
FOR CYBERSECURITY

RECOMMENDATIONS FOR QTSPS BASED ON STANDARDS

Technical guidelines on trust services

MARCH 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. 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.

CONTRIBUTORS

Olivier Barette (Nowina), Erik Van Zuuren (TrustCore), Hans Graux (Time.Lex), Olivier Delos (SEALED).

EDITORS

Evgenia Nikolouzou (ENISA), Slawomir Gorniak (ENISA), Dorin Bugneac (ENISA), Ioannis Agrafiotis (ENISA)

ACKNOWLEDGEMENTS

Special thanks go to various stakeholders in Europe who provided their support to this report. ENISA would also like to thank the contributors to the first set of recommendations in this area, whose work was the basis of this work.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-438-1 - DOI: 10.2824/777927

TABLE OF CONTENTS

ABBREVIATIONS

CA	Certification Authority
CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
CEN	Centre Européen de Normalisation
CID	Commission Implementing Decision
EN	European Standard
ETSI	European Telecommunications Standards Institute
ETSI ESI	ETSI (Technical Committee) Electronic Signatures and Infrastructures
ETSI TS	ETSI Technical Specifications
eSig	electronic Signature
eSeal	electronic Seal
EU	European Union
GDPR	General Data Protection Regulation
ISMS	Information Security Management System
ISO	International Organization for Standardisation
MS	Member State
PIMS	Privacy Information Management System
PKI	Public Key Infrastructure
QERDS	Qualified Electronic Registered Delivery Service
QESeal	Qualified Electronic Seal
QESig	Qualified Electronic Signature
QTS	Qualified Trust Service
QTSP	Qualified Trust Service Provider
QTSP/QTS	Qualified Trust Service Provider and the Qualified Trust Service it provides
QTST	Qualified Time Stamp Token
QWAC	Qualified Website Authentication Certificate
SB	Supervisory Body
TL	Trusted List
TLSO	Trusted List Scheme Operator
TS	Trust Service
TSP	Trust Service Provider
TSP/TS	Trust Service Provider and the Trust Service it provides

EXECUTIVE SUMMARY

Regulation (EU) No 910/20141 (also known as the “eIDAS Regulation”), on electronic identification and trust services for electronic transactions in the internal market, provides a regulatory environment for electronic identification of natural and legal persons and for 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 those 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.

To further enhance 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 (QTS) and qualified trust service provider (QTSP) with a view to indicating requirements and obligations that ensure high-level security and a higher presumption of their legal effect.

This document provides recommendations to help qualified trust service providers and auditors understand the expected mapping between these requirements/obligations and reference numbers of standards, as well as practical recommendations for their usage.

The document is structured in two main sections:

- A section on “Requirements common to all QTSPs” that includes recommendations on the requirements common to all TSPs and on the additional requirements common to all QTSPs;
- A section on “Requirements for provision of specific QTS”, to be used in addition to the above, that includes specific recommendations for the provision of the qualified trust services defined in eIDAS.

1. INTRODUCTION

1.1 THE ROLE OF ENISA

The European Union Agency for Cybersecurity supports the European Commission and the Member States on the implementation of the eIDAS by providing security recommendations, mapping technical and regulatory requirements, promoting the deployment of qualified trust services and raising awareness among users on securing their e-transactions. Under the EU Cybersecurity Act, the Agency gained an extended mandate to explore the area of electronic identification (eIDs) included in the regulation.

ENISA also supports the national supervisory bodies in implementing their breach reporting by aggregating their annual summary reports on trust service provider security breaches. The Agency releases Annual Reports on Trust Services Security Incidents. Moreover, in a means to support an efficient, effective process of reporting, the Agency has released the Visual Tool - CIRAS to increase the transparency of cybersecurity incidents. The online tool is accessible to the public.

1.2 BACKGROUND ON TRUST SERVICES PROVISIONING

Trust services and their provisioning are defined in Regulation (EU) No 910/2014 (hereafter the eIDAS Regulation, or eIDAS [eIDAS, 2014]), on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

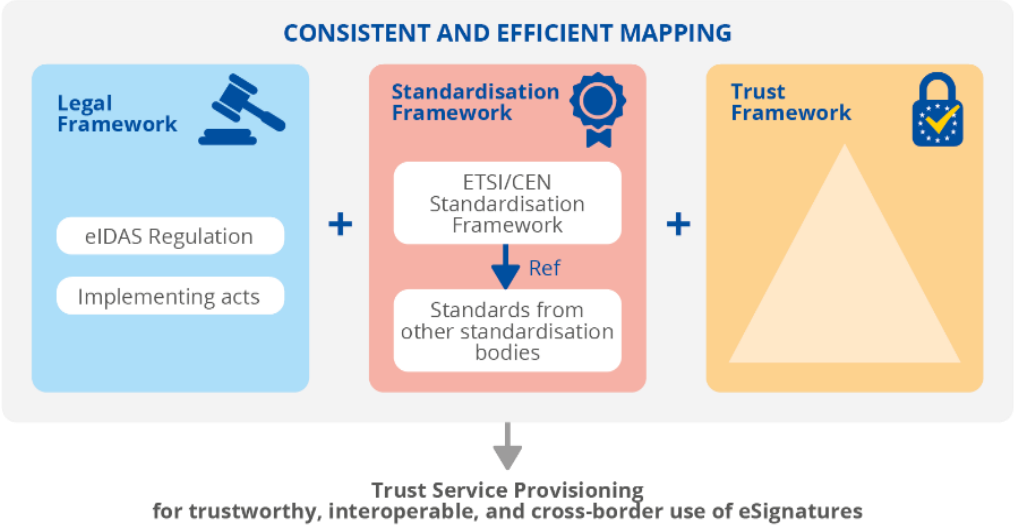
Regarding the repealed Directive 1999/93/EC, Recital (3) of eIDAS states that it *dealt with electronic signatures without delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy, and easy-to-use electronic transactions*. The eIDAS Regulation has been implemented in such a way to enhance and expand the *acquis* of that Directive to fill up this specific gap. In particular, as part of still ongoing work, this gap is and should remain filled up thanks to a consistent and efficient mapping between the three following frameworks:

- **Legal framework** for trust services established by eIDAS and implementing acts. It notably defines the requirements for provision of trust services and their legal effects, in a way to remove barriers to their cross-border usage.
- **Standardisation framework**[1] provided by ETSI and CEN standardisation bodies and relying on standards and “local” rules specified by other standardisation bodies such as ISO, IETF, OASIS, UPU, and ITU. This framework aims to meet the general requirements of the international community and eIDAS Regulation, to provide trust and confidence in electronic transactions.
- **Trust framework** established by eIDAS. This framework defines an *ex ante* and *ex post* supervision model to supervise the compliance of QTSP and the QTS they provide with the eIDAS requirements. The supervision model covers the full life cycle of each QTS and each QTSP, from its genesis until its termination.

These frameworks, illustrated in Figure 1, are further covered in the next sections.

[1] As covered in the remaining of the document, the eIDAS Regulation is technology-neutral. The legal effects it grants should be achievable by any technical means provided that the requirements of this Regulation are met.

Figure 1: Mapping between legal, standardisation, and trust frameworks



1.2.1 Legal Framework

The eIDAS Regulation establishes a general framework for the electronic identification of natural and legal persons and for the use of trust services in the internal market.

One objective of this Regulation is to enhance the trust of enterprises and consumers in the internal market and to promote the use of trust services and products. To that end, the Regulation introduces the notions of QTS and QTSP with a view to indicate their compliance with the eIDAS high-level security requirements and obligations.

In particular, the eIDAS Regulation defines 9 types of QTSs:

1. Provision of qualified certificates for electronic signatures;
2. Provision of qualified certificates for electronic seals;
3. Provision of qualified certificates for website authentication;
4. Qualified validation service for qualified electronic signatures ;
5. Qualified validation service for qualified electronic seal;
6. Qualified preservation service for qualified electronic signature;
7. Qualified preservation service for qualified electronic seal;
8. Qualified time stamping service;
9. Qualified electronic registered delivery service.

A natural or legal person providing one or more of these QTSs and that is granted the qualified status by the supervisory body (SB) is called a QTSP.

It is possible to use non-qualified and qualified 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 their validity in the same way they would do for their paper equivalent.

When the provided trust service is qualified, the outputs of such services (e.g. qualified certificate for electronic signature) can be used to achieve higher presumption of their legal effects, e.g. equivalent legal effect of a qualified electronic signature and a handwritten signature. For this purpose, the QTSP and the QTSs it provides (hereafter referred to as “QTSP/QTS”) shall comply with high-level security requirements. These requirements are covered in detail throughout the present document, along with recommendations for fulfilling them based on standards introduced below in Section 1.2.3.

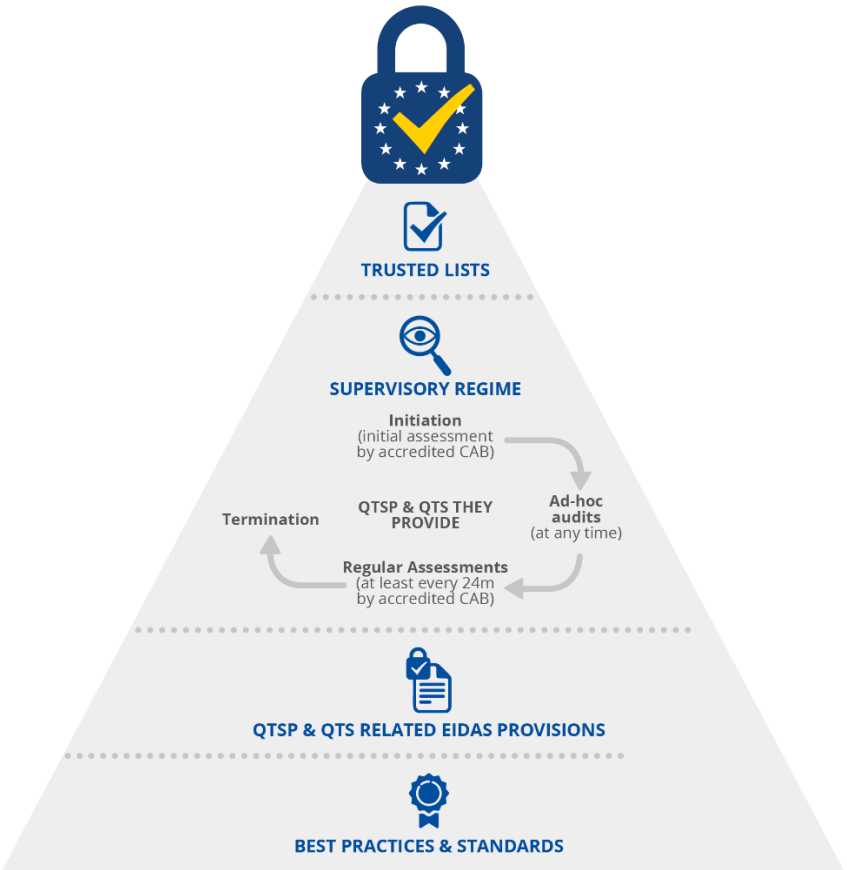
1.2.2 Trust Framework

In line with the objective to enhance the trust of enterprises and consumers in the internal market, eIDAS establishes an *ex ante* and *ex post* supervision model to supervise the compliance of QTSP, and the QTS they provide with the eIDAS requirements. This supervision model takes place:

- **At initiation, on regular basis, and at any time**[2] to ensure high-level security of QTSs: When a TSP without qualified status intends to start providing QTS or when a QTSP needs to confirm (as part of a regular assessment or an *ad hoc* audit) that the QTS it provides fulfils the eIDAS requirements and obligations, the QTSP is audited by an eIDAS-accredited conformity assessment body (CAB); The resulting conformity assessment report is then submitted to the SB which later decides to grant or, if applicable, to withdraw the qualified status of the TSP and the TS it provides;
- **At termination**[3] to ensure sustainability and durability of QTSs and to boost users' confidence in the continuity of QTS: SBs should verify the existence and the correct application of the provisions in the respective termination plans in cases where QTSPs cease their activities.

This supervision model is the foundation of the trust framework as defined by eIDAS. It is actually setting up a complete pyramid of trust for the QTSPs and the QTS(s) they provide, as illustrated in the figure below:

Figure 2: eIDAS QTSP pyramid of trust



[2] Initiation and supervision are further detailed in [ENISA Guidelines on Initiation of Qualified Trust Services] and [ENISA Guidelines on Supervision of Qualified Trust Services].
[3] Termination is further detailed in [ENISA Guidelines on Termination of Trust Services Provision].

At the top of the QTSP pyramid of trust is the trusted list. A trusted list is a signed XML file including information relating to the QTSPs which are established in and supervised by an EU Member State, together with information related to the QTSs provided by them, in accordance with the relevant provisions laid down in the eIDAS Regulation. Those lists have constitutive value and are the primary source of information to validate that a qualified status has been granted by the SB 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.

Finally, to clearly identify themselves from non-QTSP, and thus contributing to transparency in the market, QTSPs can promote their QTSs by using the EU trust mark; The usage of this trust mark furthermore enables users to fully benefit and consciously rely on electronic services, and thereby boosts their confidence in and convenience of online services.

The obligations of the QTSP regarding this trust framework (Article 20, 21, and 24.2) and the usage of the EU trust mark (Article 23) are further covered in the related sections of the present document.

1.2.3 Standardisation Framework

1.2.3.1 Context

The requirements established by the eIDAS Regulation are technology-neutral: It should be possible to achieve the necessary security requirements through different technologies.

Some articles of the eIDAS Regulation, and in particular those laying down requirements for the QTSP/QTS, allow for referencing standards or specifications via implementing acts. Compliance to these standards or specifications would provide a legal presumption of compliance with the corresponding legal requirements. In other words, this would declare one “recognised” way of implementing the requirements, but not the only way.

So far, no such optional implementing act has been adopted. It is clearly expected from the industry to self-regulate as much as possible within the legal and trust framework provided by the Regulation. A list of the possible implementing acts and the description of their scope may be found in other ENISA Guidelines, in particular [ENISA Analysis of standards related to TSPs].

1.2.3.2 ETSI/CEN Standardisation Framework

In late 2009, the European Commission issued Standardisation Mandate 460[4] aiming at supporting Directive 1999/93/EC. This Mandate requested CEN, CENELEC and ETSI to update the existing electronic signature standardisation deliverables in view of establishing a fully rationalised framework, which would solve the issues raised in actual use of electronic signatures in the EU. After 2015, the activities under the Mandate were extended via the yearly-updated EC Rolling Plan for ICT Standardisation[5] to cope with the extension of scope brought by the then-upcoming eIDAS Regulation.

The end result of these standardisation efforts (as part of a still ongoing work) is a coherent set of standards for electronic signatures and related trust services, aimed to meet the general requirements of the international community to provide trust and confidence in electronic transactions, and in particular EU legislation regulatory requirements from the eIDAS

[4] http://www.etsi.org/images/files/ECMandates/m460.pdf
[5] https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/electronic-identification-and-trust-services-including-e-signatures

Regulation[6]. For this reason, the present document focuses on this ETSI/CEN framework and is based on the above-mentioned set of standards.

It is worth noting that this ETSI/CEN framework is standardising requirements for a **PKI-based** implementation of QTSP/QTS and so is not technology agnostic: All documents of the framework intend to cover digital signatures supported by PKI and public key certificates. A digital signature is defined in ETSI ESI standards as *"data appended to, or being a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery"*. When appropriately supported by relevant trust services, digital signatures can support the implementation of trust services outputs (e.g. electronic signatures, electronic seals, timestamps etc.) as they are defined in the eIDAS Regulation. Because of this PKI-based orientation, these standards provide less guidance (or possibly no guidance at all) for "alternative", "innovative" or "creative" implementations (e.g. blockchain-based timestamps) of the eIDAS requirements. In the latter cases, the TSP may have to transpose the standardised practices and controls.

It is also worth noting that ETSI standards are not meant to be EU-only standards but international standards that may be used in EU specific purposes and benefit to other non-EU purposes aiming to reach the same level of best practices.

Structure of the framework

ETSI technical report [TR 119 000] describes the general structure for ETSI/CEN digital signature standardisation, outlining existing and potential standards for such signatures, referred to as the ETSI/CEN framework for standardisation of signatures.

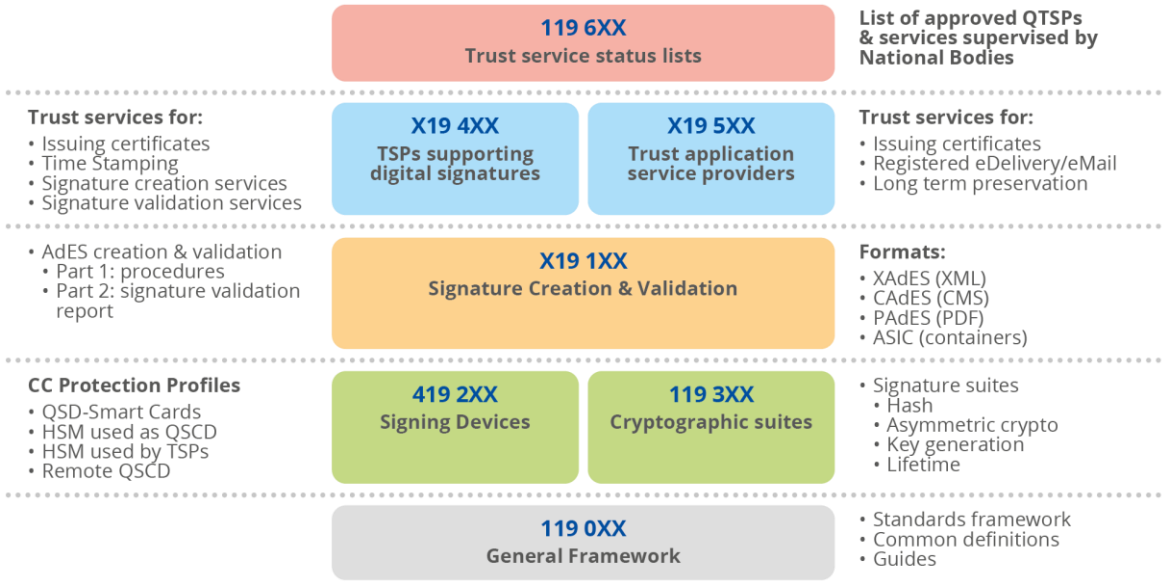
As stated in [TS 119 100], *to identify a single and consistent series of digital signatures standards and with the aim to keep the same number for each document whatever maturity level it reaches through its lifetime*, a consistent numbering has been defined as **DD L19 xxx-z** where:

- DD indicates the deliverable type in the standardisation process (SR, TS, TR and EN);
- L=4 identifies CEN deliverables and L=0-3 identified ETSI deliverables;
- 19 indicates the series of standardisation documents related to electronic signatures;
- xxx indicates the serial number and -z identifies multi-parts as some documents may be multi-part documents.

Regarding the above-mentioned serial number, this framework identifies six areas (identified with **X**xx) of standardisation with a list of existing and potential future standards in each area, as illustrated in Figure 3.

[6] https://portal.etsi.org/TB-SiteMap/ESI/ESI-ToR

Figure 3: Overview of ETSI/CEN standardisation framework



These areas are:

1. **Introductory deliverables:** gathering the overview document [ETSI TR 119 000] as well as common definitions, studies, and other introductory deliverables related to the framework for standardisation of signatures.
2. **Signature creation and validation**: focusing on standards related to the creation, augmentation, and validation of digital signatures, covering:
    a. the policy and security requirements for signature creation applications and signature validation applications;
    b. the expression of rules and procedures to be followed at creation, verification and for preservation of digital signatures for long term;
    c. signature format, packaging of signatures and signed documents; and
    d. protection profiles, according to Common Criteria for signature creation/verification applications.
3. **Signature creation and other related devices**: focusing on standards related to qualified signature/seal creation devices as defined in eIDAS, on signature creation devices used by trust service providers as well as other types of devices supporting digital signatures and related services such as authentication. In practice, the deliverables of this area have been produced by CEN, particularly the protection profiles referred to in the present document.
4. **Cryptographic suites**: covering standardisation aspects related to the use of signature cryptographic suites, i.e. the suite of digital signature related algorithms including key generation algorithms, signing algorithms with parameters and padding method, verification algorithms, and hash functions.
5. **Trust service providers supporting digital signatures and related services**: covering QTSPs issuing qualified certificates, TSPs issuing public key certificates other than qualified certificates, including certificates for website authentication, time-stamping services providers, TSPs offering signature validation services, TSPs offering remote signature creation services (also called signing servers).
6. **Trust application service providers**: covering trust service providers offering value added services applying digital signatures and relying on the generation/validation of electronic signatures in normal operation. This includes namely registered mail and other e-delivery services, as well as data preservation (long term archiving) services.

7. **Trust service status (list) provider**: covering standards related to the provision of trusted lists as specified by [CID 2015/1505].

Up to five types of documents may be associated with each area:

- Guidance documents;
- Policy and Security Requirements;
- Technical Specifications;
- Conformance Assessment Guidance;
- Compliance and Interoperability Testing.

More information on the ETSI/CEN standardisation framework may be found in [ETSI TR 119 000].

Standards for QTSPs

The main[7] standards listed in the present document are from areas 4 and 5 of this framework (Trust service providers and Trust application service providers, respectively) as presented in the table below:

Source: ETSI TS 119 403-3.

Qualified trust service in Regulation (EU) No 910/2014	Standards
Provision of qualified certificates for electronic signatures	ETSI EN 319 411-2 (requiring compliance with ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 412-2, ETSI EN 319 412-5)
Provision of qualified certificates for electronic seals	ETSI EN 319 411-2 (requiring compliance with ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 412-3, ETSI EN 319 412-5)
Provision of qualified certificates for website authentication	ETSI EN 319 411-2 (requiring compliance with ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 412-4, ETSI EN 319 412-5)
Provision of qualified time stamps	ETSI EN 319 421 (requiring compliance with ETSI EN 319 401), ETSI EN 319 422
Qualified validation service for qualified electronic signatures	ETSI TS 119 441 (requiring compliance with ETSI EN 319 401), ETSI TS 119 442, ETSI EN 319 102-1, ETSI TS 119 102-2 ETSI TS 119 172-4
Qualified validation service for qualified electronic seals	ETSI TS 119 441 (requiring compliance with ETSI EN 319 401), ETSI TS 119 442, ETSI EN 319 102-1, ETSI TS 119 102-2 ETSI TS 119 172-4
Qualified preservation service for qualified electronic signatures	ETSI EN 319 401, ETSI TS 119 511, ETSI TS 119 512
Qualified preservation service for qualified electronic seals	ETSI EN 319 401, ETSI TS 119 511, ETSI TS 119 512
Qualified electronic registered delivery services	ETSI EN 319 401, ETSI EN 319 521, ETSI EN 319 522 ETSI EN 319 531, ETSI EN 319 532

[7] In the sense of providing guidance and standardizing requirements regarding the core operations of the QTSP/QTS

For each of these QTSs, the ETSI standards are structured as follows:

- ETSI EN 319 401 is setting the basic requirements for a TSP, independently of the TS it provides;
- ETSI EN 319 4x1 and ETSI EN 319 5x1 are setting additional requirements regarding the policy and security requirements for a QTSP to provide a specific QTS;
- ETSI EN 319 4x2 and ETSI EN 319 5x2 are setting technical specifications, such as formats, procedures, outputs, and protocols related to a QTS.

The two figures below illustrate this structure for the issuance of qualified certificates and qualified time stamps.

Source: ETSI European standardisation framework for trust services

Figure 4: ETSI standards regarding issuance of qualified certificates

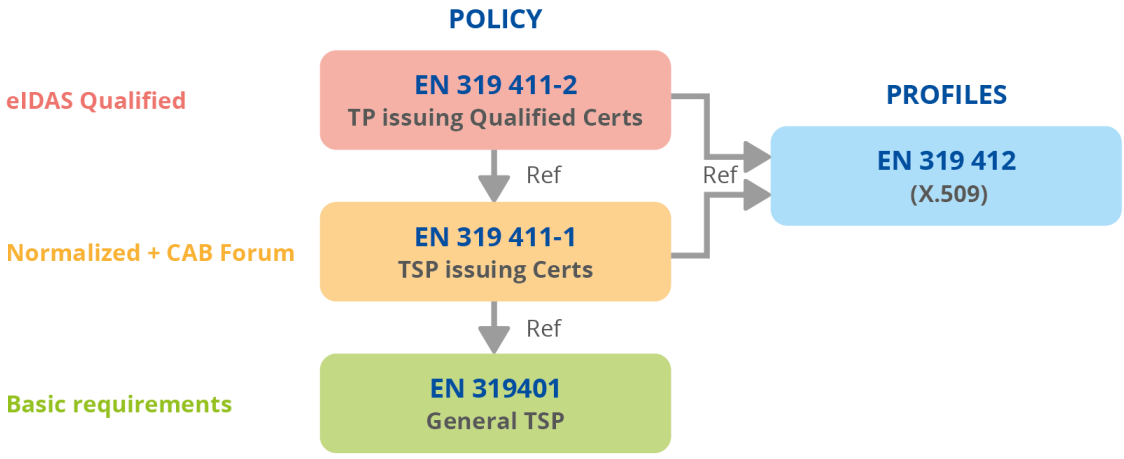
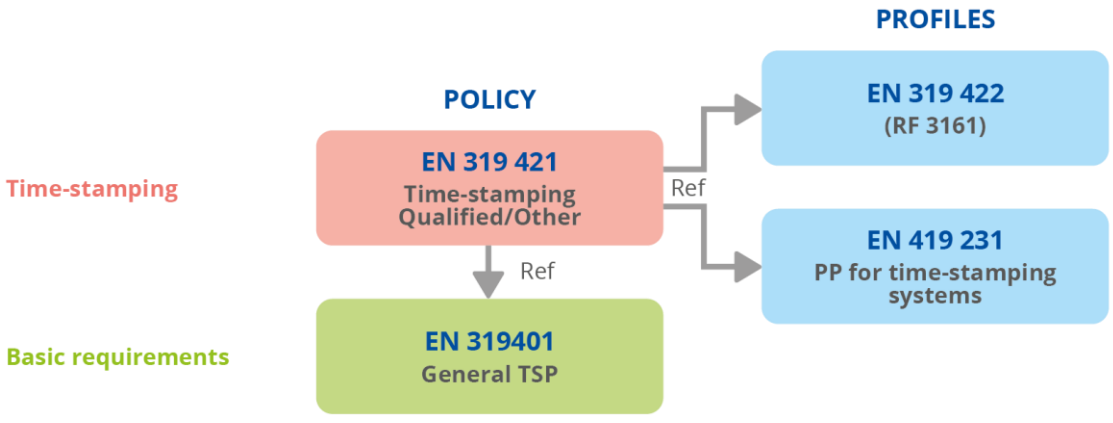


Figure 5: ETSI standards regarding issuance of qualified timestamps



The standards listed in the figures above provide guidance and set requirements regarding the operations of the QTSP/QTS. Other standards from ETSI may be referred in these documents, either as normative reference or as guidance for implementations.

Examples of these standards include:

- Cryptographic suites: [TS 119 312];
- Signature formats: ETSI EN 319 1x2;
- Protection profiles regarding cryptographic modules, server signing, timestamping : CEN EN 419 221 series, [EN 419 241-2], [EN 419 231];
- Accessibility requirements: [EN 301 549].

Where appropriate, these standards are referred to in the sections below covering eIDAS requirements.

1.2.3.3 Standards from other standardisation bodies

Other standardisation bodies such as ISO, IETF, OASIS, UPU, ITU, and national accreditation or supervisory bodies are also defining "standards" or "local rules" that apply to Trust Services and Trust Service Providers.

These "standards" and "local rules" are usually indicated in the ETSI/CEN standards as the basis for the specific requirements or further guidance and implementation recommendations, with the aim of further clarifying or supplementing these base standards in order to maximise best practices, interoperability, and suitability to trust services.

References in ETSI standards to standards from other standardisation bodies include:

- Standard(s) regarding due diligence and risk management such as [ISO/IEC 27002] providing guidelines for information security practices and [ISO/IEC 27005] for guidance on information security risk management as part of an information security management system (ISMS) as defined by [ISO/IEC 27001];
- Standard(s) regarding management of personal data (e.g. [ISO/IEC 27701]);
- CA/Browser Forum (hereafter referred to as "CA/B Forum") requirements, designed by a voluntary group of certification authorities (CAs), vendors of Internet browser software, and suppliers of other applications that use X.509 digital certificates for SSL/TLS and code signing[8]. CA/B Forum work includes:
    - Baseline requirements for the issuance and management of publicly trusted certificates;
    - EV SSL certificate guidelines;
    - EV code signing certificate guidelines;
    - Network and certificate systems security requirements.

  A QTSP looking to be included in the browsers root stores may be interested in the recommendations provided in Section 3.1.1.4.
- Family of standards to the X.509 Public Key Infrastructure provided by IETF such as [RFC 5280];
- SOG-IS[9] Agreed Cryptographic Mechanisms to help ensure a high level of security in the recommended cryptographic suites, in particular when creating and validating digital signatures. ETSI standards such as [TS 119 312] on "Cryptographic Suites" notably delegate the assessment of the security of underlying cryptographic schemes to this document. Both documents are revised every two years and, in the case of new attacks or of the immediate need to remove an algorithm could arise, a revision of [TS 119 312] is published as soon as possible.

[8] Requirements for S/MIME certificates are expected to be published in the near future
[9] https://www.sogis.eu/. Agreed Cryptographic Mechanisms can be found via https://www.sogis.eu/uk/supporting_doc_en.html.

NOTE: Standards alternative to ETSI ones on PKI-based trust services exist but will not be covered in the present document, such as [ISO/IEC 27099] on PKI practices and policy and the ISO 14533 series on CAdES / XAdES / PAdES formats.

1.3 TARGET AUDIENCE

The audience of this document is TSPs, prospective QTSPs, and QTSPs looking for guidelines for fulfilling requirements originating from the articles of the eIDAS Regulation based on existing standards.

This document can also be used by auditors assessing (Q)TSPs, e.g. CABs, or Supervisory Bodies, looking for a mapping between the eIDAS requirements and reference numbers of standards, on which a (Q)TSP may rely.

1.4 PURPOSE AND STRUCTURE OF THIS DOCUMENT

This document provides recommendations to help stakeholders in understanding the expected mapping between the eIDAS requirements and reference numbers of standards, as well as practical recommendations for their usage. In the remainder of this document, unless stated otherwise, a reference of an "Article" indicates an article of the eIDAS Regulation.

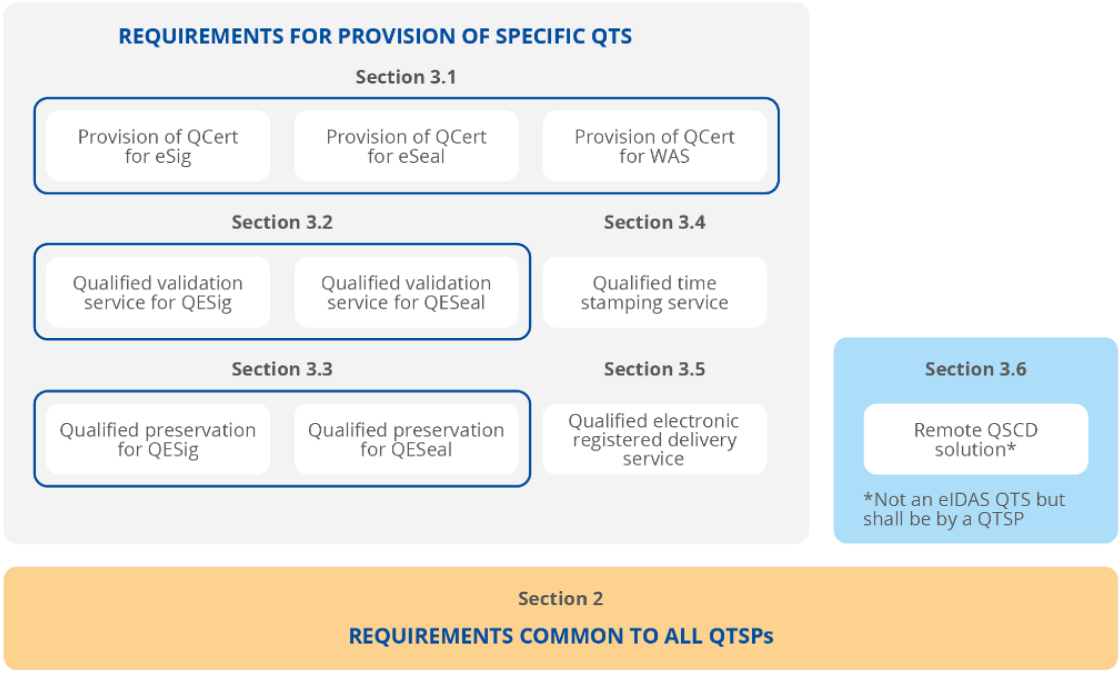
This document is an updated version of "Recommendations for QTSPs based on standards – Technical guidelines on trust services", published in December 2017, refreshed with standards that have been published and updated since. The document is also based on the ENISA deliverable from 2015 "Analysis of standards related to Trust Service Providers – Mapping of requirements of eIDAS to existing standards".

This document is structured as follows:

- **Section 2** "Requirements common to all QTSPs" that includes:
    1. Recommendations on the requirements common to all TSPs (both QTSPs and non-QTSPs), namely requirements on data processing and protection (Article 5), on liability and burden of proof (Article 13), on accessibility for persons with disabilities (Article 15), and on security (Article 19);
    2. Recommendations on the additional requirements common to all QTSPs, as required by Article 20, 21, 23, and Article 24.2 of eIDAS.
- **Section 3** "Requirements for provision of specific QTS", to be used in addition to the above common requirements, that includes specific recommendations for the provision of the qualified trust services defined in eIDAS:
    1. QTSP issuing qualified certificates for electronic signatures, electronic seals, and website authentication;
    2. QTSP providing qualified validation services for qualified electronic signatures (QESig) and/or qualified electronic seal (QESeal);
    3. QTSP providing qualified preservation service for QESig/QESeal;
    4. QTSP issuing qualified electronic time stamping service;
    5. QTSP providing qualified electronic registered delivery service;
    6. QTSP providing remote QSCD services (i.e. generating or managing electronic signature creation data on behalf of the signatory). This service is not a qualified trust service per se but, as it shall be provided by a QTSP, recommendations are proposed pursuant to the objective of the document to provide recommendations for QTSPs.

This document structure is illustrated in the following figure.

Figure 6: Recommendations for QTSP based on standards



1.5 DISCLAIMER

Due to the technological neutrality of the eIDAS requirements, it is worth noting that:

- Different approaches based on different technologies than the ones exposed in the present document can lead to eIDAS compliance;
- Compliance against these standards (or other standards) is not mandatory to achieve compliance against eIDAS requirements;
- Compliance against these standards does not automatically imply conformance to eIDAS requirements. Although these standards may be seen as best practices, there is no automatic presumption of compliance[10] to eIDAS after following the said standards.

[10] Some nationally-defined schemes (e.g. [ANSSI, 2017], [NSA-CS], [DKPv2]) specify conformity criteria based on the ETSI standards, along with a limited set of additional requirements, that provide presumption of compliance to the eIDAS requirements.

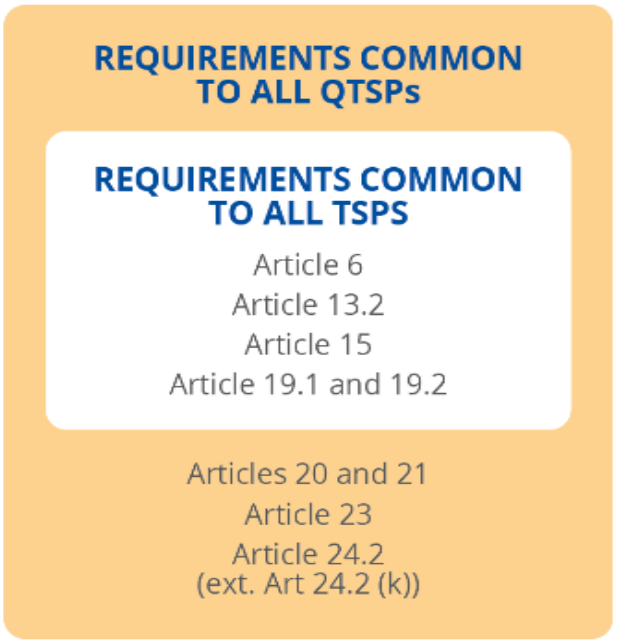
2. REQUIREMENTS COMMON TO ALL QTSPS

In order to ensure due diligence, inclusion, transparency, and accountability of the operations and services of QTSPs, all of them are subject to a common set of requirements:

- As a TSP:
  - Data processing and protection, as defined in Article 5;
  - Liability and burden of proof, as defined in Article 13.2;
  - Accessibility for persons with disabilities, as defined in Article 15;
  - Security, as defined in Article 19.1 and 19.2.
- As a QTSP:
  - Specific requirements regarding initiation and supervision, as defined in Articles 20 and 21;
  - Specific requirements on the usage of the EU trust mark, as defined in Article 23;
  - Specific requirements on the operations per se of a QTSP, as defined in Article 24.2 (excluding Article 24.2(k) specific to the issuance of qualified certificates).

This section details guidelines for QTSPs based on standards for the purpose of being compliant with the above-mentioned requirements.

Figure 7: Requirements common to all QTSPs



2.1 ARTICLE 5 (DATA PROTECTION)

Article 5 states that:

1. *Processing of personal data shall be carried out in accordance with Directive 95/46/EC.*
2. *Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.*

It is important to highlight that the Directive 95/46/EC is now replaced by the Regulation (EU) 2016/679 of 27 April 2016[11] on "the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC", known as the General Data Protection Regulation (GDPR).

The ETSI standardisation framework addresses this Article with the requirement REQ-7.13-05 of [EN 319 401]. However, the mentioned requirement does not contain detailed information on how to meet GDPR except that, regarding “the authentication for a service online, the processing of identification data shall be limited to only those data which are adequate, relevant and not excessive to grant access to that service online”.

Compliance to GDPR (and associated guidance) is a subject on its own and is thus outside of the scope of the present document. Further information on this topic may be found for instance in ENISA documents specific to the subject: https://www.enisa.europa.eu/topics/data-protection.

In terms of standards, [ISO/IEC 27701] is an extension of [ISO/IEC 27001] for Privacy Information, extending an ISMS (Information Security Management System) into a PIMS (Privacy Information Management System). [ISO/IEC 27701] may be seen as a framework for managing data privacy, and so may be seen as a tool to reach compliance to GDPR, demonstrating that the TSP is “in control” regarding data privacy. It is worth noting that being certified against [ISO/IEC 27701] is by no means a presumption of compliance to GDPR, and similarly that GDPR does not mandate the certification or the compliance to the [ISO/IEC 27701] standard.

Finally, it is worth mentioning that, in order to be useful in the context of demonstrating compliance with Article 5, the scope of [ISO/IEC 27701] certification (the same applies for [ISO/EC 27001] certification) should explicitly address the provision of the QTS(s) provided by the QTSP.

2.2 ARTICLE 13.2 (LIABILITY AND BURDEN OF PROOF)

Article 13.2 states that:

> *Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.*

The ETSI standardisation framework addresses this Article with the requirement REQ-6.2-01 of [EN 319 401] that requires TSPs to make clear terms and conditions available to all subscribers and relying parties, and in particular pay attention to REQ-6.2-02 items f) and g) of [EN 319 401]

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at https://eur-lex.europa.eu/eli/reg/2016/679/oj.

so that these terms and conditions state any possible limitation of liability together with the applicable legal system.

2.3 ARTICLE 15 (ACCESSIBILITY FOR PERSONS WITH DISABILITIES)

Article 15 states that:

> *Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.*

The ETSI standardisation framework addresses this Article with the requirements REQ-7.13-03 and REQ-7.13-04 of [EN 319 401]. In particular this standard recommends taking into account [EN 301 549], that specifies the functional accessibility requirements applicable to ICT products and services, together with a description of the test procedures and evaluation methodology for each accessibility requirement.

In practice, pragmatic ways of implementing Article 15 may include the setup of alternative ways to reach the same objectives (e.g. a dedicated support line that persons with disabilities may call if they experience difficulties with a webpage delivering the said product or service, so that they may be guided efficiently through the same procedure).

2.4 ARTICLES 19.1 AND 19.2 (SECURITY REQUIREMENTS)

Article 19.1 states that:

> *Qualified and non-qualified trust service providers shall take 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. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.*

Article 19.2 states that:

> *Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.*
>
> *Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.*
>
> *[Other requirements for the supervisory body]*

Article 19 requires that all TSPs:

1. Assess risks. This obligation is addressed in clause 5 of [EN 319 401], summarizing the five important steps for risk assessment, along with references to [ISO/IEC 27005] and information security policy specified in the clause 6.3;
2. Take appropriate security measures. [EN 319 401] and the other ETSI policy standards (related to provision of specific QTS) propose security measures that should be taken by the QTSP. For instance, appropriate security measures for all (Q)TSPs are defined

in clauses 7.2 to 7.12 of [EN 319 401] that are all subclauses from clause 7 on “TSP management and operation”, excluding clause 7.1 on “Internal organization” and clause 7.13 on “Compliance” that are not related to security per se;

3. Notify the supervisory body about significant security incidents and breaches of integrity. To that end, ENISA released an incident reporting framework for eIDAS Article 19 in [ENISA Article 19 Incident reporting].

The implementation of this article and details on the three above activities are specifically covered by the [ENISA Security Framework for QTSPs]. This document proposes a security framework for QTSPs, on top of the one proposed for TSPs in [ENISA Security Framework for TSPs], taking into account the type of provided QTSs, regarding policies, procedures, and processes in order to be compliant with the security requirements defined in eIDAS under aforementioned articles.

2.5 ARTICLES 20 AND 21 (SUPERVISION AND INITIATION)

Article 20 “Supervision of qualified trust service providers” and Article 21 “Initiation of a qualified trust service” may be seen as not related to the core operations of a QTSP. However, they lay down the foundation of a supervision scheme where the QTSP has an active participation, and as such define clear requirements towards this QTSP.

On this specific topic of initiation, supervision (and termination), ENISA published a series of deliverables whose objective is to propose guidelines aimed at facilitating the implementation of the provisions related to it. These deliverables state:

> *In order to ensure high-level security of qualified trust services, the eIDAS Regulation foresees an active supervision scheme of QTSP/QTS by the national competent SB that supervises, ex ante and ex post, fulfilment of the QTSP/QTS requirements and obligations.*
>
> *Before a TSP/TS is granted a qualified status (becoming a QTSP/QTS), it will be subject to a pre-authorisation process – the so-called initiation process in line with Article 21 of the eIDAS Regulation. QTSP may only begin to provide the QTS after the qualified status has been granted by the national SB and indicated in the national trusted list as referred to in Article 22 of the Regulation. From there, the supervision scheme covers the full life cycle of each QTS and each QTSP, from its genesis until its termination.*

The first deliverable of the above-mentioned series, [ENISA Guidelines on Initiation of Qualified Trust Services], proposes detailed guidelines pursuant to Article 21.

The guidelines continue with:

> *Once granted a qualified status, QTSPs and their QTSs have the obligation to pass, and submit to the competent supervisory body a conformity assessment report (CAR) issued by an accredited CAB confirming at least every 24 months, 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.*

The second deliverable of the above-mentioned series, [ENISA Guidelines on Supervision of Qualified Trust Services], proposes detailed guidelines pursuant to Article 20.

Finally, the guidelines state that:

> *To ensure sustainability and durability of QTS, and proper termination and user's confidence in the continuity of QTS, QTSPs have to maintain an up-to-date termination plan, as referred to in Article 24.2(i) of the Regulation.*

The third deliverable of the above-mentioned series, [ENISA Guidelines on Termination of Qualified Trust Services], proposes detailed guidelines pursuant to Article 24.2(i). Related recommendations can also be found in Section 2.7.9 of the present document.

With regards to conformity audits aiming to confirm that the assessed (Q)TSP/QTS fulfil the requirements of eIDAS, [ENISA conformity assessment of qualified trust service providers] provides an overview of the conformity assessment framework for (Q)TSPs in the context of this Regulation. This document can be used, for each phase of an eIDAS conformity assessment, as guidance to QTSPs for the purpose of preparing and undertaking the assessment in the best possible conditions.

2.6 ARTICLE 23 (EU TRUST MARK)

Article 23 states that:

1. *After the qualified status […] has been indicated in the trusted list […], qualified trust service providers may use the EU trust mark to indicate in a simple, recognisable, and clear manner the qualified trust services they provide.*
2. *When using the EU trust mark for the qualified trust services referred to in paragraph 1, qualified trust service providers shall ensure that a link to the relevant trusted list is made available on their website.*

The purpose of this trust mark is to identify the QTSP/QTS and clearly differentiate them from non-qualified trust services provided by non-QTSP. The objective behind the specification of this trust mark is to boost confidence and convenience of online services that are essential for users to fully benefit and consciously rely on electronic services.

Nevertheless, it is worth mentioning that the use of an EU trust mark by QTSPs is on a voluntary basis.

The usage of the trust mark does not lead to any requirement other than those provided in the eIDAS Regulation and CID 2015/806 laying down its specifications (such as size and design) pursuant to Article 23(3). In order to help QTSP properly using this trust mark, the Commission published[12] explanations, practical guidance, and logos.

Regarding clause 2 of Article 23, as alternatives to a link to the XML version of the trusted list, the QTSP may provide a link to the Trusted List Browser tool[13] provided by the European Commission. It enables any interested party to browse the EU trusted lists (and the information related to that QTSP) in a user-friendly manner. Additionally, unlike a trusted list location that is subject to change over time, a link to above-mentioned tool ensures to always redirect the interested party to a representation of the trusted list downloaded from the last location notified by the Member State to the Commission. To that end, the QTSP can either provide a link to:

1. A browsable version of the national trusted list, using https://webgate.ec.europa.eu/tl-browser/#/**tl**/CC where CC is the relevant applicable country code in two letters;

[12] https://ec.europa.eu/digital-single-market/en/eu-trust-mark
[13] https://webgate.ec.europa.eu/tl-browser/#/

2. A browsable version of the QTSP information, including the qualified trust services it provides, using https://webgate.ec.europa.eu/tl-browser/#/**trustmark**/CC/VATCC-NUMBER where both CC should be replaced by the country code in two letters, and NUMBER is the VAT Number provided in the trusted list as one of the trade names of that QTSP[14].

Both links (1) & (2) satisfy Article 23(2) and as such can be used in conjunction with the EU trust mark for an improved user experience.

2.7 ARTICLE 24.2 (REQUIREMENTS FOR QTSP)

Article 24.2 of eIDAS Regulation specifies 10 clauses for QTSPs providing QTSs. The following subsections 24.2(a) to 24.2(j) refer to each of these clauses and propose guidelines based on standards for compliance with them.

Article 24.2(k) is specific to QTSPs issuing qualified certificates and is covered in Section 3.1.3.

2.7.1 Article 24.2(a) (Notification of changes)

Article 24.2(a) states that *[a QTSP providing QTSs shall:]*

> *inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities*

This article specifies that the QTSP shall inform the SB of:

- Changes in provided QTS;
- Its intent to terminate providing a QTS.

Implementation of this article is tightly related to the change management process. One of the main goals of such a process is to introduce changes in a systematic, secure, and effective manner.

The present document recommends that the reporting mechanism should provide event driven triggers (according to threshold criteria: "when to notify") and communication channels ("how to notify") to report changes to a SB according to Member State regulations. It is a good practice to create a communication plan associated with the change management process which covers communication with a supervisory body.

ETSI standards do not impose any specific requirements or rules related to communication. However, it is recommended that such rules should be defined and information about them be included in the Trust Service Practice Statement (or the other practice statements such as the Certification Practice Statement for the issuance of qualified certificates).

For changes made in the above-mentioned practice statements, [EN 319 401] specifies:

- *The TSP shall notify notice of changes it intends to make in its practice statement* (REQ-6.1-09); and
- *The TSP shall, following approval […], make the revised TSP's practice statement immediately available […]* (REQ-6.1-10).

For other changes (those not reflected in a practice statement), the present document suggests to keep the same communication rules as above, with the exception that, when the QTSP

[14] E.g. https://webgate.ec.europa.eu/tl-browser/#/trustmark/BE/VATBE-0408425626 to point to Zetes S.A./N.V. in the trusted list of Belgium.

intends to terminate its activities, it should be communicated to the SB earlier (than in the actual termination process).

Further guidance on notification of changes under Article 24.2(a) may be found in the [ENISA Guidelines on Supervision of Qualified Trust Services]. Best practices regarding the change management process can be found in chapter 12.1.2 of [ISO/IEC 27002] standard.

Regarding the specificities of termination activities, the second part of Article 24.2(a) (information of the intention to cease activities), is covered by clause 7.12 of [EN 319 401] which is required to be applied before the TSP terminates its services. Guidelines on these termination activities are covered in further detail below in the section on Article 24(i) (termination plan).

2.7.2 Article 24.2(b) (Human resources)

Article 24.2(b) states that *[a QTSP providing QTSs shall:]*

> *employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards;*

QTSP should build an appropriate organization structure. Staff with good knowledge, segregation of duties and sufficient funds for maintaining this staff is a part of building QTSPs reliability. QTSP should develop and maintain appropriate human resources processes and procedures, education programs and keep records of such activities.

These measures should ensure:

- Reliability and competence of candidates for employment;
- Continuous personal education for staff and management;
- Trainings sessions;
- Security procedures trainings;
- Sufficient human resources of the TSP to fulfil requirements of segregation of duty, business requirements and implement countermeasures resulting from risk analysis;
- Appropriate discipline;
- Proper record keeping of these activities.

General requirements (applicable to any TSP) aiming to help TSPs comply with this clause are set by clause 7.2 of [EN 319 401]. For detailed provisions, this standard refers to [ISO/IEC 27002]. In particular, best practices regarding human resources security, security roles and responsibility and segregation of duties are described in clauses 6.1.1, 6.1.2, and 7 of [ISO/IEC 27002].

Depending on the type of service, the corresponding QTS-specific ETSI standards refine and extend these requirements and recommendations. Where applicable, a reference to these additional requirements and recommendations may be found in the following table.

Type of QTS	Standard	Reference
QTSP issuing qualified certificates	[EN 319 411-1]	Clause 6.4.4
QTSP providing qualified validation service for QESig/QESeal	[TS 119 441]	OVR-7.13-04
QTSP providing qualified preservation service for QESig/QESeal	-	-
QTSP issuing qualified electronic time stamps	-	-
QTSP providing qualified electronic registered delivery services	[EN 319 521]	Clause 7.2.2

2.7.3 Article 24.2(c) (Liability and financial resources)

Article 24.2(c) states that *[a QTSP providing QTSs shall:]*

> *with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law;*

There is no ETSI standard defining how to meet this requirement; this is an identified gap in standardisation. This matter is only referred to in [EN 319 401] via REQ-7.1.1-04, with no more guidance than in the Regulation, but replacing “national law” by “applicable law”.

The gap can be addressed by extension to the requirement of the above-mentioned REQ, to recommend that the assessment of “maintain sufficient financial resources and/or obtain appropriate liability insurance” should be a risk-based approach, i.e. based on a risk assessment, which takes into account commercial and financial issues, following local (national) rules and legislation (if any) and good practices, as part of the risk management. Further guidance on risk management is provided in the [ENISA Security Framework for QTSPs].

The most common approach towards the treatment of a risk of liabilities for damage is risk sharing, and the most common countermeasure is insurance against the risks. A QTSP should check the legislation related to the protection of consumers (subscribers) and trusting entities interests, in the Member State in which it operates or would like to start its activities.

If a regulator expects a TSP to declare an amount of liabilities, it is the most cost effective to establish a risk management process. The analysis of threats and potential losses per service allows a TSP to calculate an amount of money to allocate to assure compensation for potential damages or define insurance requirements and conditions.

2.7.4 Article 24.2(d) (Terms and conditions)

Article 24.2(d) states that *[a QTSP providing QTSs shall:]*

> *before entering into a contractual relationship, inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;*

Use of trust services by subscribers and trusting entities requires notice or knowledge of the terms and conditions of these services. One of QTSP's obligations is to inform about terms and conditions for each trust service. Information presented in the documentation should be up to date, understandable, easily accessible, and conspicuously communicated to stakeholders. Clause 6.2 of [EN 319 401] defines general requirements for the content of the terms and conditions.

When relying parties need to acknowledge the terms and conditions, the good practice proposed in the present document is the setup of an acceptance method, such as a mandatory acceptance button together with the necessity to scroll down (i.e. "read") the whole content.

Depending on the type of service, the corresponding QTS-specific ETSI standards refine and extend these requirements and recommendations. Where applicable, a reference to these additional requirements and recommendations may be found in the table below:

Type of QTS	Standard	Reference
QTSP issuing qualified certificates	[EN 319 411-1]	Clause 6.9.4 DIS-6.1-04 to DIS-6.1-09 REG-6.3.4-02 to REG-6.3.4-03 OVR-6.3.4-04 to OVR-6.3.4-06
	[EN 319 411-2]	Clause 6.9.4
QTSP providing qualified validation service for QESig/QESeal	[TS 119 441]	Clause 6.2
QTSP providing qualified preservation service for QESig/QESeal	[TS 119 511]	Clause 6.2
QTSP issuing qualified electronic time stamps	[EN 319 421]	Clause 6.6
QTSP providing qualified electronic registered delivery services	[EN 319 521]	Clause 4.2

2.7.5 Article 24.2(e) (Trustworthy systems)

Article 24.2(e) states that *[a QTSP providing QTSs shall:]*

> *use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;*

There is no clear definition of "trustworthy systems" and "trustworthy products". First, "trustworthiness" can actually be defined differently depending on the type of the service. Second, such systems and products can also be certified or not certified and hardware-based or software-based.

In addition, it is worth noting that this clause does not relate only to trustworthy systems and products that appear in dedicated QTSP-related processes (e.g. generation and storage of cryptographic keys), but are also related to storage of data and supporting processes such as

“supplier service delivery management” or “system acquisition, development, and maintenance management”.

Article 24.2(e) is explicitly covered by the set of requirements defined in clause 7.7 of [ETSI 319 401]. This article is also implicitly covered in this standard by:

- Clause 7.5 on cryptographic control, in case the QTSP makes use of cryptographic keys or devices;
- Clause 7.6 on physical and environmental security, and in particular for components whose security is critical to the provision of the trust service(s) and minimize risks related to physical security;
- Clause 7.4 on the limitation of QTSP's system access to authorized individuals (and in particular REQ-7.4-02, REQ-7.4-03, and REQ-7.4-10 in the context of Article 24.2(e));
- Clause 7.8 on the network and related systems security.

These clauses refer to [ISO/IEC 27002] and [CA/B Forum network security guide] for additional guidance.

Depending on the type of service, the corresponding QTS-specific ETSI standards refine and extend these requirements and recommendations. Where applicable, a reference to these additional requirements and recommendations may be found in the table below:

Type of QTS	Standard	Reference
QTSP issuing qualified certificates	[EN 319 411-1]	Clause 6.5
	[EN 319 411-2]	Clause 6.5
QTSP providing qualified validation service for QESig/QESeal	[TS 119 441]	Clause 7.5 Clause 7.6 Clause 7.7 Clause 7.8 Clause 8
QTSP providing qualified preservation service for QESig/QESeal	[TS 119 511]	Clause 7.5 Clause 7.8 PRP-8.1-01 and PRP-8.1-03
QTSP issuing qualified electronic time stamps	[EN 319 421]	Clause 7.6 Clause 7.8 Clause 7.10
QTSP providing qualified electronic registered delivery services	[EN 319 521]	Clause 7.5 Clause 7.6 Clause 7.8

In accordance with [EN 319 411-2], for QTSPs issuing qualified certificates, it is worth noting that the generation of TSP's key pair shall be carried out within a trustworthy system which:

a) is assured to EAL 4 or higher in accordance with [ISO/IEC 15408], or equivalent national or internationally recognized evaluation criteria for IT security provided this is a security target or protection profile which meets the requirements of the above-mentioned standards; or
b) meet the requirements identified in [ISO/IEC 19790] or [FIPS PUB 140-2] level 3.

The same applies for QTSP issuing qualified time stamps regarding the generation of the timestamping unit signing key (cf. [EN 319 421].

Regarding clause a) (on EAL 4 and [ISO/IEC 15408]), CEN EN 419 221 series of standards are dedicated to the specification of common criteria protection profiles for TSP's cryptographic modules, in accordance with [ISO/IEC 15408]. For QTSP issuing qualified time stamps and as further detailed in Section 3.4, CEN published [EN 419 231], i.e. protection profile for "trustworthy systems supporting time stamping".

Regarding QSCD, and according to Article 30 and 39 of eIDAS, when a qualified certificate relies on a QSCD[15], this QSCD shall be certified against the requirements laid down in Annex II of eIDAS; notified by the Member States to the European Commission; and published by the Commission[16]. With regards to the certification of local QSCDs, [CID 2016/650] lays down the list of standards to be used as part of their security assessment (i.e. the CEN EN 419 211 series)[17].

The particular case of remote QSCDs (when the electronic signature/seal creation data is managed on behalf of the signatory/creator of seal) is covered in Section 3.1 "Requirements for QTSP issuing qualified certificates" and Section 3.6 "Requirements for QTSP providing remote QSCD services ".

2.7.6 Article 24.2(f) (Data storage)

Article 24.2(f) states that *[a QTSP providing QTSs shall:]*

use trustworthy systems to store data provided to it, in a verifiable form so that:

i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,
ii) only authorised persons can make entries and changes to the stored data,
iii) *the data can be checked for authenticity;*

This article expands Article 24.2(e) by additional aspects concerning personal data handling. As a consequence, the references to standards in Section 2.7.5 also applies to the present section.

Personal data is part of the sensitive information a QTSP acquires during standard operations. Personal data protection is covered in Section 2.1 related to Article 5 on data processing and

[15] The private key related to a qualified certificate does not necessarily need to be stored on a QSCD. But being protected by a QSCD is requirement for a qualified electronic signature (as defined in eIDAS Article 3(12).
[16] The list of SSCD and QSCD is currently published in https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds
[17] "Alternative processes" as defined in Article 30.3(b) might still be used in the case where the standards listed in Article 30.3(a) are considered as not applicable. This is demonstrated (at the time of writing of the present document) by the alternative process notified by the Netherlands and described in https://www.tuv-nederland.nl/assets/files/general-files/2019/12/190724-trn-eidas-dutch-conformity-assessment-process---v5.0.pdf. This alternative process explicitly covers "Type 1 QSCDs" that cannot claim conformance to the CEN EN 419 211 series. Local (i.e. Type 1) QSCDs have been certified under this process and are currently published in the European Commission's SSCD and QSCD list above.

protection. Depending on the type of services provided, Section 2.7.10 on Article 24.2(j) provides additional guidelines in that respect.

Additionally, depending on the type of service, the corresponding QTS-specific ETSI standards refine and extend these requirements and recommendations. Where applicable, a reference to these additional requirements and recommendations may be found in the table below:

Type of QTS	Standard	Reference
QTSP issuing qualified certificates (in addition to the ones mentioned above)	[EN 319 411-1]	Clause 6.4.3 Clause 6.4.6
QTSP providing qualified validation service for QESig/QESeal	[TS 119 441]	Clause 7.13 Clause 7.5
QTSP providing qualified preservation service for QESig/QESeal	[TS 119 511]	Clause 7.5
QTSP issuing qualified electronic time stamps	-	-
QTSP providing qualified electronic registered delivery services	[EN 319 521]	Clause 5.1

2.7.7 Article 24.2(g) (Measures against forgery and theft of data)

Article 24.2(g) states that *[a QTSP providing QTSs shall:]*

take appropriate measures against forgery and theft of data;

Measures against forgery and theft of data shall warrant particular attention when the QTSP takes appropriate technical and organisational measures to manage the risks posed to the security of the trust services it provides as required by Article 19 (see Section 2.4).

It is recommended in the present document that such measures must be considered in nearly all the aspects of the QTSP management and operations, and in particular the ones listed in [EN 319 401] such as:

- Human resources (clause 7.2);
- Asset management (clause 7.3);
- Access control (clause 7.4);
- Cryptographic controls (clause 7.5);
- Physical and environmental security (clause 7.6);
- Operation security (clause 7.7);
- Network security (clause 7.8);
- Incident management (clauses 7.9);
- Collection of evidence (clause 7.10);
- Business continuity management (clause 7.11);
- In case of termination (clause 7.12).

Measures derived from the above clauses can be expanded with the catalogue of available ones in [ISO/IEC 27002], which is indeed referred to by the ETSI standards when applicable.

Depending on the type of service, the corresponding QTS-specific ETSI standards refine and extend the related measures. Where applicable, a reference to these additional measures may be found in the table below:

Type of QTS	Standard	Reference
QTSP issuing qualified certificates	[EN 319 411-1]	Clause 6.4 Clause 6.5
	[EN 319 411-2]	Clause 6.4 Clause 6.5
QTSP providing qualified validation service for QESig/QESeal	[TS 119 441]	Clause 7.6 Clause 7.7
QTSP providing qualified preservation service for QESig/QESeal	[TS 119 511]	Clause 7.6 Clause 7.7
QTSP issuing qualified electronic time stamps	[EN 319 421]	Clause 7.8
QTSP providing qualified electronic registered delivery services	[EN 319 521]	Clause 7.6 Clause 7.8

2.7.8 Article 24.2(h) (Records)

Article 24.2(h) states that *[a QTSP providing QTSs shall:]*

> *record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;*

This requirement should be read together with Article 17.4(i):

> *[…] the tasks of the supervisory body shall include in particular:*
>
> > *to verify the existence and correct application of provisions on termination plans in cases where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance with point (h) of Article 24(2);*

The preservation and accessibility for an appropriate period of time, including after the activities of the QTSP have ceased, of all relevant information concerning data issued and received by the QTSP are essential. It is in particular required for the purpose of providing evidence in legal proceedings (e.g. audit on data collection and treatment), GDPR legal compliance, and for the purpose of ensuring continuity of the service.

In that sense, it should still be possible to validate previous evidence created as part of the qualified trust service or by means of its outputs. This may not require, except for the issuance of qualified certificates, that the QTSP makes a copy of all such evidences from their creation but that the necessary elements for validating them would be made available. Nevertheless,

recording all data issued and received by the QTSP, regardless of the type of QTS provided, is recommended and may be proven to be useful to achieve the objectives of Article 24.2(h).

As an example, for QTSP issuing qualified certificate, [EN 319 411-1] (OVR-6.4.6-01) requires the QTSP to record and keep available certain records (such as logs of event related to certificates and relevant documentation) for a period of at least 7 years after any certificate based on these records ceases to be valid (i.e. from when it expires or is revoked). Regarding the period of retention, it is worth noting that "an appropriate period of time" may not necessarily translate into 7 years. Application domains or sectoral regulations may require the period to be considered as being much longer than that, and it is recommended in the present document to consider this evaluation as part of the compliance management.

The termination plan, further detailed in the next section on Article 24.2(i), needs to include procedures and means allowing the (Q)TSP to meet Article 24.2(h) of the eIDAS Regulation. In particular, the termination plan should cover, at least, expected and unexpected cessation of activities, the cessation of one, more or all the QTS from a QTSP, the potential take-over of ceased activities by a third party or as a last resort by the SB, and the assurance of the preservation and availability of the information referred to in Article 24.2.(h).

Additionally, it is recommended that the QTSP includes in its communication to subscribers (e.g. as part of the termination notification and as part of the CP/CPS, terms and conditions) information on the period of time during which the QTSP will ensure Article 24.2(h) referred data are recorded and kept available and of the importance of the use by concerned parties of appropriate procedures and technologies capable of extending such a period when applicable, with regards to the data/records they are concerned with.

Types of records applicable to Article 24.2(h) are mostly dependent on the type of service(s) provided by the QTSP. Relevant references may be found in the table below:

Type of QTS	Standard	Reference
QTSP issuing qualified certificates	[EN 319 411-1]	REG-6.2.2-18 REG-6.3.4-07, REG-6.3.4-08, and REG-6.3.4-17 REG-6.3.8-02 REG-6.4.5-04 Clause 6.4.6 Clause 6.4.9
QTSP providing qualified validation service for QESig/QESeal	[TS 119 441]	Clause 7.10 Clause 7.11
QTSP providing qualified preservation service for QESig/QESeal	[TS 119 511]	Clause 7.10
QTSP issuing qualified electronic time stamps	[EN 319 421]	Clause 7.12 Clause 7.13
QTSP providing qualified electronic registered delivery services	[EN 319 521]	Clause 7.10 Clause 7.11

2.7.9 Article 24.2(i) (Termination plan)

Article 24.2(i) states that *[a QTSP providing QTSs shall:]*

> *have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4);*

A termination plan is a key document regarding a QTSP/QTS. As stated in Recital (41), Article 17(4) and Article 24.2(i), this document shall be verified by the SB because of its particular importance regarding the sustainability and durability of qualified trust services and to boost users' confidence in the continuity of qualified trust services, such as in exceptional/unfortunate cases of QTSP unscheduled termination (e.g. bankruptcy).

The termination plan should contain at least information on affected entities, reliable party (parties) to which TSP obligations will be transferred, as well as a detailed procedure of notification and transfer including a timing aspect with all affected parties taken into consideration. Such document should be maintained as part of TSP documentation management and change management processes, to keep it up to date.

TSP termination and termination plan are covered in clause 7.12 of [EN 319 401], where some requirements or guidance may be found regarding the termination process. Clause 7.12 does not however cover the actual content of the termination plan.

Depending on the type of service, the corresponding QTS-specific ETSI standards refine and extend these requirements and recommendations. Where applicable, a reference to these additional requirements and recommendations may be found in the table below:

Type of QTS	Standard	Reference
QTSP issuing qualified certificates	[EN 319 411-1]	Clause 6.4.9
QTSP providing qualified validation service for QESig/QESeal	-	-
QTSP providing qualified preservation service for QESig/QESeal	[TS 119 511]	Clause 7.12
QTSP issuing qualified electronic time stamps	[EN 319 421]	Clause 7.14
QTSP providing qualified electronic registered delivery services	[EN 319 521]	Clause 7.12

The [ENISA Guidelines on Termination of Qualified Trust Services] provides further guidance on the termination obligations and activities, the exploration of a set of possible termination scenarios, and a proposed structure of termination plan.

2.7.10 Article 24.2(j) (Personal data)

Article 24.2(j) states that *[a QTSP providing QTSs shall:]*

ensure lawful processing of personal data in accordance with Directive 95/46/EC;

Regarding QTSPs, point (j) of Article 24.2 may be seen as a duplication of Article 5 of eIDAS[18]. Guidelines provided in Section 2.1 are then also applicable to the present Article.

Nevertheless, depending in the type of service, the corresponding QTS-specific ETSI standards refine and extend these requirements and recommendations. Where applicable, a reference to these additional requirements and recommendations may be found in the table below:

Type of QTS	Standard	Reference
QTSP issuing qualified certificates	[EN 319 411-1]	Clause 6.8.4
QTSP providing qualified validation service for QESig/QESeal	[TS 119 441]	Clause 7.13
QTSP providing qualified preservation service for QESig/QESeal	-	-
QTSP issuing qualified electronic time stamps	-	-
QTSP providing qualified electronic registered delivery services	-	-

[18] As confirmed for instance in [TS 119 403-3] CAR-4.2-16 a) i)

3. REQUIREMENTS FOR PROVISION OF SPECIFIC QTS

This section details recommendations based on standards for QTSPs providing specific types of QTS, to be used in addition to the above common recommendations, for the purpose of being compliant with the requirements that are relevant for the provision of this specific QTS.

3.1 REQUIREMENTS FOR QTSP ISSUING QUALIFIED CERTIFICATES

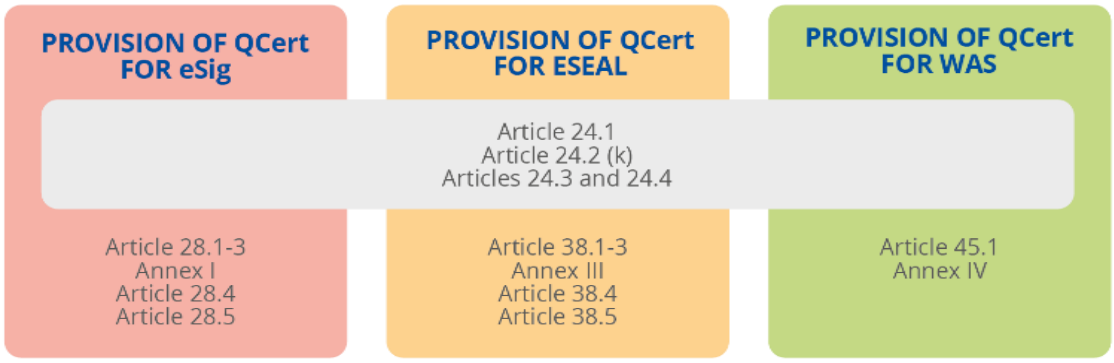
The eIDAS Regulation defines in Article 3 three types of certificates and three corresponding types of qualified certificates:

- Article 3(14): *Certificate for **electronic signature**: an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;*
- Article 3(15): ***Qualified** certificate for electronic signature: a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;*
- Article 3(29): *Certificate for **electronic seal**: an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;*
- Article 3(30): ***Qualified** certificate for electronic seal: a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III;*
- Article 3(38): *Certificate for **website authentication**: 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;*
- Article 3(39): ***Qualified** certificate for website authentication: a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV.*

Qualified certificates for electronic signatures / for electronic seals / for website authentication may only be provided by a QTSP that has been granted to provide the related qualified trust service(s).

In addition to common requirements for all QTPs, this chapter addresses specific requirements in relation to the provision of these qualified trust services. These requirements of eIDAS cover both the operations of issuance of such qualified certificates as a trust service, and the content of the qualified certificate itself. Articles defining these requirements are illustrated in the following figure.

Figure 8: Requirements for QTSP issuing qualified certificates for eSig / eSeal / WSA



The table below indicates whether a mapping with eIDAS Regulation and whether a conformity assessment checklist for this type of trust service are currently provided by ETSI standards:

	Available	Standard reference
Mapping with eIDAS Regulation	Yes	Annex A of [EN 319 411-2]
Conformity assessment checklist	Yes	Annex B of [EN 319 411-2]

3.1.1 Preliminary recommendations

3.1.1.1 ETSI qualified certificates policies

This section refers to [EN 319 411-2]. Requirements defined in this standard are dependent on the type of qualified certificate provided by the QTSP. In particular, based on the certificate policies defined in [EN 319 411-1] (i.e. NCP, NCP+, and EVCP), the standard defines five eIDAS qualified certificate policies:

1. **QCP-n**: policy for qualified certificates issued to **natural** persons offering the level of quality defined in eIDAS for qualified certificates (so to be used for certificates for electronic signatures);
2. **QCP-l**: policy for qualified certificates issued to **legal** persons offering the level of quality defined in eIDAS for qualified certificates (so to be used for certificates for electronic seals);
3. **QCP-n-qscd**: policy including QCP-n requirements and requiring the use of a QSCD;
4. **QCP-l-qscd**: policy including QCP-l requirements and requiring the use of a QSCD;
5. **QCP-w**: policy for qualified website certificates offering the level of quality defined in eIDAS used in support of website authentication.

3.1.1.2 Qualified certificates for PSD2

Regarding the specific case of qualified certificates for PSD2 (Directive (EU) 2015/2366), and in addition to the applicable requirements below, requirements on the certificate profile and on the TSP policies are listed in [ETSI TS 119 495].

3.1.1.3 Qualified certificates relying on a QSCD

Information on the eIDAS QSCD can be found at the end of Section 2.7.5, related to Article 24.2(e) on trustworthy systems and products.

It is important to note that the QTSP issuing qualified certificates with the private key located on a QSCD shall monitor the QSCD certification status until the end of the validity period of the

certificate (and shall take appropriate measures in case of modification of this status), as stated in SDP-6.5.1-07 of [EN 319 411-2]. Following Article 30 (on the certification of QSCD) and Article 31 (on the publication of list of certified QSCD), it is recommended that the QTSP monitors this QSCD certification status in the list of those certified QSCDs (and SSCDs) published by the EC[19]. Nevertheless, it should be noted that this list is not constitutive; A device may be a QSCD but not appear on the EC list. In practice, there may also be a delay between the certification/determination of a device as a QSCD and its inclusion in the EC list.

In the particular case of a remote QSCD, "monitoring the QSCD certification status" should be understood in the broad sense of whether the remote QSCD can still "be considered as a QSCD". Indeed, this status may be lost for different reasons:

- As for a local QSCD, because the remote QSCD lost[20] its certification (and is removed from the published list); or
- because the QTSP managing this remote QSCD on behalf of the signatory/creator of seal has lost its qualified status because its "last" QTS lost its qualified status[21].

3.1.1.4 Recognition of qualified certificates for website authentication as Extended Validation certificates by browsers

Inclusion in the CA root stores of the main browsers (but also software vendors such as Adobe or Oracle) may be seen as an interesting feature. As presented in the introduction, the CA/Browser Forum has adopted guidelines and requirements as a common basis for CAs for their eligibility in the CA root store programs.

The standards that are published by ETSI are developed by experts from different industries and requirements from the CA/B Forum are included in the latest standards (e.g. [EN 319 411-1]).

Audit for compliance against these ETSI standards (by a CAB qualified for audits against ETSI EN 319 411 standards series) is recognized by browsers for inclusion in the root stores. Alternatively, demonstration of compliance via the WebTrust Program for CAs is another recognized path.

It is worth noting that for both alternatives, the latest CA/Browser Forum guidelines and requirements (which might differ from the standards above due to separate document lifecycles) still typically apply together with specific requirements for each root store program[22], and the CA (here the QTSP issuing QWACs) must still apply separately for the inclusion in each root store program it is interested in.

As the present document focuses on QTSPs under eIDAS, further details underlying the recognition of QWACs as EVs are beyond its scope. More information on the topic may be found in:

- [ENISA Towards global acceptance of eIDAS audits], in particular regarding the relation between CA/B Forum guidelines, ETSI standards and WebTrust audit scheme.
- The ETSI report [TR 103 684], in particular regarding legal context, supervision and auditing, best practices, and trust representation of the WebTrust model.
- [ENISA Conformity assessment of qualified trust service providers] regarding multipurpose audits.

[19] https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds
[20] For instance, some QSCD certifications have an expiry date. But identified security vulnerabilities might also impact a certification status.
[21] A QTSP is qualified because it has at least one QTS.
[22] See for instance https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/

3.1.2 Article 24.1 (Identity verification)

Article 24.1 states that:

> *When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued.*
>
> *The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law:*
>
> *a) by the physical presence of the natural person or of an authorized representative of the legal person; or*
> *b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorized representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or*
> *c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or*
> d) *by using other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body*

It must be stressed that this process is an essential part of the registration procedure for issuing a qualified certificate, as this initial identity validation will determine the binding between the (physical or legal) person and all subsequent signatures or seals supported by this certificate.

In addition, as stated in the eIDAS article, identity verification must be carried out in accordance with the national law of the Member State in which the QTSP is established.

The process of identity verification has two key elements:

- How the verification is actually performed;
- If not performed with physical presence of the person, how the equivalence to this physical presence can be ensured.

Generally, identity verification means collecting identity data and related evidence or attestation from an appropriate and authorised source, checking its validity and authenticity, and binding this data to the applicant. The most common way is to use a nationally recognized identity document. Other means are for instance national registry information, bank or utility account information, credit bureau information, or breeder documents (unless local legislation states otherwise).

Guidelines on how to perform this identity verification may be found in clauses 6.2.2 and 6.2.3 of [EN 319 411-1] and clauses 6.2.2 of [EN 319 411-2]. However[23], the requirements might be seen as rather generic (no requirement on the verification procedure, definition of what "physical presence" may mean or its equivalence in the light of new practices such as video onboarding), considering the cruciality of this preliminary step.

[23] The identity verification process in the certificate issuance process has a lot in common with identity proofing process during (notified) issuance of electronic identification means. Therefore, another source of good practices (whenever applicable) is the Commission Implementing Regulation (EU) 2015/1502 for the high and substantial assurance levels of electronic identification means.

As a result, a Specialist Task Force, STF 588[24], has been setup at ETSI ESI. The scope of the STF is "to produce specification on identity proofing for trust services as defined by eIDAS, particularly for issuers of qualified and non-qualified certificates supporting electronic signatures, electronic seals or website certificates. It needs to be aligned with, and to further support the ETSI EN 319 411 parts 1 and 2 providing policy requirements for Trust Service Providers (TSP) issuing such certificates".

The expected results of STF 588 are twofold:

- A survey of technologies and regulatory requirements for identity proofing for trust service subjects: ETSI TR 119 460 "Electronic Signature and Infrastructures (ESI); Survey of technologies and regulatory requirements for identity proofing for trust service subjects" expected to be published in December 2020;
- Requirements for identity proofing: ETSI TS 119 461 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects" expected to be published end of July 2021.

NOTE: ETSI standards distinguish two types of identity verification:

- Initial identity validation (clause 6.2.2 of [EN 319 411-1] and [EN 319 411-2]), where the issuance of a certificate is meant for a person not registered by the QTSP;
- Re-keying process (clause 6.2.3 of [EN 319 411-1]), which means the process of issuance of a new certificate for the person who has already been registered by the QTSP and possess a qualified certificate from this QTSP.
  In case of a re-key request, the identity verification procedure can be simplified, where existing evidence can be re-used to validate the identity, provided the evidence remains valid given the time elapsed and it is allowed by the national legislation. In any case, such a procedure must meet all the requirements of initial identity validation.

3.1.3 Article 24.2(k) (Certificate database)

Article 24.2(k) states that *[a QTSP providing QTSs shall:]*

> *in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database.*

The QTSP shall maintain a certificate database. This database should be protected to ensure availability and integrity and should be maintained on an operational basis.

To be compliant with this article, it is recommended to follow clause 6.1 of [EN 319 411-1].

[24] https://portal.etsi.org/STF/STFs/STF-HomePages/STF588

3.1.4 Articles 24.3 and 24.4 (Certificate revocation)

Article 24.3 states that:

> *If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.*

Article 24.4 states that:

> *With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.*

These articles are related to operating and maintaining a certificate database and in particular to revocation management and revocation status services described (in particular) in:

- Clause 6.2.4 of [EN 319 411-1];
- Clause 6.3.9 of [EN 319 411-1];
- Clauses 6.3.10 of [EN 319 411-1] and [EN 319 411-2].

Generally, validity / revocation status information should be available 24 hours per day, 7 days per week. In case of failure, TSP should endeavour to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the Certification Practice Statement. As this availability is crucial, the QTSP should identify assets, vulnerabilities, and countermeasures to minimalize risk of loss of availability. Following Article 19, it is recommended to include these aspects in the global risk management process.

Two methods of providing validity and revocation status are the most popular: through a Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP). Clause 6.3.10 of [EN 319 411-1] provides further guidance on the selection of the method(s).

In case both methods are supported by a TSP, the information provided by all services shall, as required by eIDAS, be consistent over time. Different delays in updating the status information for all these methods should be taken into account.

For more information about availability of service assurance, one can refer to [ISO/IEC 20000-1] clause 6.

3.1.5 Articles 28.1-3, 38.1-3, and 45 (Content of certificates)

Article 28.1 to 28.3 states that:

1. *Qualified certificates for electronic signatures shall meet the requirements laid down in **Annex I**.*
2. *Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in **Annex I**.*
3. *Qualified certificates for electronic signatures may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures.*

Article 38.1 to 38.3 states that:

1. *Qualified certificates for electronic seals shall meet the requirements laid down in **Annex III**.*
2. *Qualified certificates for electronic seals shall not be subject to any mandatory requirements exceeding the requirements laid down in **Annex III**.*
3. *Qualified certificates for electronic seals may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic seals.*

Article 45.1 states that:

1. *Qualified certificates for website authentication shall meet the requirements laid down in **Annex IV**.*

These requirements address the content of the certificates. Annex I, III, and IV of the eIDAS Regulation contain detailed requirements for certificate content. A QTSP issuing qualified certificates should prepare a certificate profile for this purpose. The Regulation mandates only information listed in Annex I, III, and IV to be present, but other information can be added by a QTSP.

Regarding the profile of certificates, it is recommended to follow:

- [EN 319 411-1] clause 6.6.1;
- [EN 319 411-2] clause 6.6.1;

  NOTE: While following [EN 319 411-1] or [EN 319 411-2] it is a non-mandatory recommendation to be compliant with the eIDAS requirements, claiming for a TSP to be compliant with [EN 319 411-1] or [EN 319 411-2] requires compliance to (where applicable) [EN 319 412-2], [EN 319 412-3], [EN 319 412-4] and [EN 319 412-5], as stated in clause 6.6.1 of [EN 319 411-1] and clause 6.6.1 of [EN 319 411-2].

- [EN 319 412-1], providing an overview and common data structures on certificate profiles;
- [EN 319 412-2], providing certificate profile for certificates issued to **natural** persons (so to be used for certificates for electronic signatures);
- [EN 319 412-3], providing certificate profile for certificates issued to **legal** persons (so to be used for certificates for electronic seals);
- [EN 319 412-4], providing certificate profile for **web site** certificates (so to be used for certificates for website authentication);
- [EN 319 412-5], standardizing indications related to qualified certificates per se.

  NOTE: In Annex I a), III a) and IV a), eIDAS doesn't mandate the use the ETSI "id-etsi-qcs-QcCompliance (id-etsi-qcs 1)" statement, further specified by the "id-etsi-qcs-QcType (id-etsi-qcs 6)" defined in [EN 319 412-5] as "indication at least in a form suitable for automated processing" that the certificate has been issued as a qualified certificate and for which type. Still, the use of these standardised statements are highly recommended as the specifications of the EU MS trusted lists defined in CID (EU) 2015/1505 are using these statements as the "benchmark statements" for the machine processable indication referred above. The same applies for the ETSI "id-etsi-qcs-QcSSCD (id-etsi-qcs 4)" as "indication at least in a form suitable for automated processing" that the corresponding private key is located in an EU QSCD.

All the certificate profiles specified in the ETSI EN 319 412 series are based upon [Recommendation ITU-T X.509] and [RFC 5280]. It is important to note that point (b) of Annexes I, III, and IV of the eIDAS Regulation requires that qualified certificates shall include:

> *a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and:*
>
> - *for a legal person: the name and, where applicable, registration number as stated in the official records;*
> - *for a natural person: the person's name.*

The best practice to implement this requirement is by using the *organizationName* attribute ("O=" attribute) of the *Issuer* field of the qualified certificate. As per [RFC 5280] specifications, the "O=" attribute of the *Issuer* field of the qualified certificate shall be identical to the *Subject* field of the issuing CA certificate. In accordance with point (b) of the Annexes, this "O=" attribute must be identical – preferably case sensitively – to the name of the QTSP as stated in the official records and hence the name (or trade name if applicable) present in the trusted list[25]. Additionally, where applicable, the qualified certificate should also contain in the *organizationIdentifier* attribute the registration number as stated in the official records. Further guidance on the latter may be found in [EN 319 412-1].

Implementing additional attributes should be developed according to the same rules. During development of additional fields in certificate structure, the TSP may use the [EN 319 412-1] standard. As stated in the eIDAS article, introduction of additional (non-mandatory) attributes should not affect mandatory interoperability. Examples of additional (non-mandatory) attributes are: Organizational Unit, State or Province Name, Locality, Title.

The QTSP should also keep the certificate profile adequate to applicable regulations.

3.1.6 Articles 28.4 and 38.4 (Certificate revocation)

These articles only apply to certificates for electronic signatures and certificates for electronic seals, excluding certificates for website authentication.

Article 28.4 (the same applies to Article 38.4 where 'signature' is replaced by 'seal') states that:

> *If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.*

This article concerns qualified certificates for electronic signatures/seals that have been revoked **after initial activation**. It is therefore allowed and is a good/acceptable practice to create qualified certificate in a "on hold" status before its initial activation (e.g. once QTSP is convinced that it has been issued to the right person). At initial activation, this "on hold" status is reverted but after this, a potential revocation shall never be reverted, as required by Article 28.4.

TSP should conduct risk analysis to recognize all potential activities which can lead to reinstating a revoked certificate, for example restoring from backup. After the identification of potential threats appropriate countermeasures should be taken. A suggested solution is to

[25] The issuing CA certificate is usually provided by the TSP to the Trusted List Scheme Operator to be listed in the trusted list as the Service Digital Identity (SDI), defined in clause 5.5.3 of ETSI TS 119 612 v2.1.1, made mandatory by [CID 2015/1505] on technical specifications and formats relating to trusted lists.
Clause 5.5.3 defines specific requirements on the "O=" attribute of the SDI. Non-compliance with this clause can reflect a potential non-compliance with [CID 2015/1505] and therefore eIDAS Regulation.

choose an appropriate technology which prevents reinstating revoked certificates, or to enable the replay (e.g. based on logs) of all applicable revocations since the last backup.

Before a TSP issues a certificate, some obligations should be accepted by the subject and/or subscriber. One of them is not to create any electronic signature with the private key if the certificate has been revoked (cf. [EN 319 411-1] OVR-6.3.5-01 j)).

As required by REV-6.3.9-01 of [EN 319 411-1], the TSP shall revoke certificates in a timely manner based on authorized and validated certificate revocation requests mentioned in clause 6.2.4 of [EN 319 411-1] and [EN 319 411-2].

Recommendations to achieve compliance with these articles are proposed in REV-6.3.9-04 of [EN 319 411-1][26].

3.1.7 Articles 28.5 and 38.5 (Temporary suspension of certificates)

These articles only apply to certificates for electronic signatures and certificates for electronic seals, excluding certificates for website authentication[27].

Article 28.5 (the same applies to Article 38.5 where 'signature' is replaced by 'seal') states that:

> *Subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic signature:*
>
> *a) if a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension;*
> b) *the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.*

Certificate suspension is subject to national regulation, and so may vary between Member States[28]. The TSP should perform a compliance management process to ensure compliance to local regulation of the Member state in which it is established.

If suspension is allowed in a Member State, it is recommended to follow the provisions of:

- [EN 319 411-1] clauses 6.2.4, 6.3.9 and 6.3.10;
- [EN 319 411-2] clauses 6.2.4, 6.3.9 and 6.3.10.

In case of discrepancies between the standards and national law, national law prevails.

[26] It should be noted that, while these eIDAS articles exclude certificates for website authentication, the corresponding clauses of [EN 319 411-1] apply to them as well. As such, these may be seen as recommendations for certificates for website authentication.
[27] Similarly to the previous section, while the eIDAS articles exclude certificates for website authentication, the corresponding clauses of [EN 319 411-1] apply to them as well. As such, these may be seen as recommendations for certificates for website authentication.
[28] For instance, suspension of qualified certificate for electronic signatures, electronic seals and website authentication is forbidden in France, as stated in Section II.3.4. of https://www.ssi.gouv.fr/uploads/2016/06/eidas_delivrance-certificats-qualifies_v1.1_anssi.pdf (in French), but allowed in Luxembourg.

3.2 REQUIREMENTS FOR QTSP PROVIDING QUALIFIED VALIDATION SERVICES FOR QESIG/QESEAL

The eIDAS Regulation defines in Article 3(41) a validation as *the process of verifying and confirming that an electronic signature or a seal is valid*. Validation of the signature of an electronic transaction is an essential process for allowing any relying party to trust the corresponding signed data and/or document.

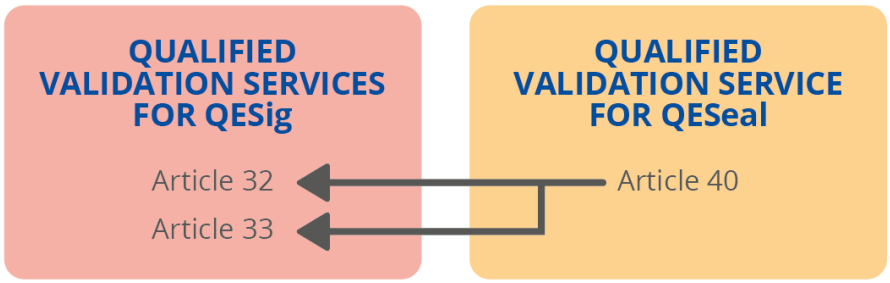
In a nutshell (detailed validation process is further covered below), for a qualified electronic signature, the validation service consists in verifying that it meets the requirements set out in **Article 26** (requirements on advanced electronic signatures), it is created by a QSigCD [29], and it is based on a qualified certificate for electronic signatures. For a qualified electronic seal, the validation service consists in verifying that it meets the requirements set out in **Article 36** (requirements on advanced electronic seals), is created by a QSealCD, and it is based on a qualified certificate for electronic seal.

A QTSP may be granted a qualified status to provide both of these services, or only one of them. Requirements on the validation of qualified electronic signatures are specified in Article 32 and 33 of eIDAS. Regarding the validation of qualified electronic seals, Article 40 of eIDAS states that these articles "*shall apply mutatis mutandis to the validation […] of qualified electronic seals*".

In particular, the qualified validation service for qualified electronic signatures and seals is specified by:

- Article 33 (resp. Article 40) for the requirements on qualified validation services of qualified electronic signatures/seals; which includes by reference;
- Article 32 (resp. Article 40) for the requirements on the validation of qualified electronic signatures/seals.

Figure 9: Requirements for QTSP providing qualified validation services for QESig / QESeal



The table below indicates whether a mapping with the eIDAS Regulation and whether a conformity assessment checklist for this type of trust service are currently provided by ETSI standards:

	Available	Standard reference
Mapping with eIDAS Regulation	Yes	Annex B and C of [TS 119 441]
Conformity assessment checklist	Yes	Annex E of [TS 119 441]

[29] QSCD stands for both QSigCD and QSealCD. In case of ambiguity or necessity, the explicit acronym QSigCD or QSealCD is used.

3.2.1 Article 32 (Validation of QESig/QESeal)

Article 32.1 states that:

> *The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that:*
>
> *a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;*
> *b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;*
> *c) the signature validation data corresponds to the data provided to the relying party;*
> *d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;*
> *e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;*
> *f) the electronic signature was created by a qualified electronic signature creation device;*
> *g) the integrity of the signed data has not been compromised;*
> *h) the requirements provided for in Article 26 were met at the time of signing.*

Article 32.2 states that:

> *The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.*

NOTE: Use of pseudonym (see Article 32.1(e)) is not applicable to electronic seals.

Several ETSI standards currently exists regarding the validation process:

- [TS 119 441] specifying policy requirements for TSP providing signature validation services;
- [TS 119 172-4] (currently in draft) on the signatures applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists. This standard Provides rules for the determination of the technical suitability of a digital signature to be considered QES by making reference to:
    - [EN 319 102-1] / [TS 119 102-1] specifying procedures for validation of digital signatures. This standard is to be used to validate whether the provided digital signature/seal is an advanced electronic signature/seal in the sense of eIDAS. This document refers to [TS 119 312] for guidance regarding the cryptographic algorithm's validity, based on the agreed cryptographic mechanisms from SOG-IS;
      When validating a signature, the QTSP must take care of the potential security related issues against either national rules or [TS 119 312].
    - [TS 119 615] (currently in draft) on the procedures for using and interpreting European Union Member States National Trusted Lists. This standard is to be used to validate the qualified status of the electronic signature/seal.
- These standards rely on the definition of an AdES (digital) signature as a digital signature that is either a CAdES signature (as specified in [EN 319 122-1] or older), or a PAdES signature (as specified is [EN 319 142-1] or older) or a XAdES signature (as specified is [EN 319 132-1] or older)[30];

[30] At the time of writing, a new format, JAdES signature, is being specified under [TS 119 182-1].

- These standards refer to [TS 119 101] defining policy and security requirements for applications for signature creation and signature validation.

In addition to the above standards and ETSI Conformance Checkers, the European Commission has made available different tools and documents that may be found helpful for implementing signatures/seals validation:

- DSS (Digital Signature Services)[31]: an open-source software library for digital signature creation, validation, and augmentation, designed to help digital solutions achieve compliance with the eIDAS Regulation, either by integrating it or cross-checking an implementation against it;
- DSS Demonstration WebApp[32] : a demonstration of integration of the DSS library in a web application;
- "Introduction to the Qualified electronic signature (QES) validation algorithm[33]": a document describing the validation algorithm used by DSS library, aligned with the above-listed standards;
- Test cases for assessing an implementation of electronic signatures and seals validation[34]: A web site hosting 100+ test cases[35] that can be used by a TSP or by any conformity assessment body or supervisory body to verify or demonstrate the conformity a validation service.

3.2.2 Article 33 (Qualified validation service for QESig/QESeal)

Article 33.1 states that:

> *A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who:*
>
> *a) provides validation in compliance with Article 32(1); and*
> b) *allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.*

Article 33 (resp. Article 40 for qualified electronic seals) defines requirements for QTSPs providing qualified validation service for qualified electronic signatures. It shall:

- be provided by a QTSP;
- provide validation in compliance with Article 32 for which guidelines are provided above;
- provide the validation result in an automated manner that needs:
  - to be reliable and efficient; and
  - to bear the advanced electronic signature or advanced electronic seal of the QTSP providing the qualified validation service.

Requirements on the validation result (or validation report) are provided in Annex B of [TS 119 441].

[31] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/DSS
[32] Hosted by the European Commission and currently available via https://ec.europa.eu/cefdigital/DSS/webapp-demo/
[33] Currently available via https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Qualified+electronic+signature+%28QES%29+validation+algorithm
[34] Hosted by the European Commission and currently available via https://webgate.ec.europa.eu/esig-validation-tests/testcases
[35] Algorithms in [TS 119 615] and [TS 119 172-4] have shown that there can be identified 100+ variations of cases based on combinations of the certificate content, trusted list content, pre/post-eIDAS time of signing, etc.

Additionally, [TS 119 102-2] specifies a recommended general structure and XML format for reporting the validation of digital signatures, in line with the requirements specified in [EN 319 102-1] / [TS 119 102-1].

3.3 REQUIREMENTS FOR QTSP PROVIDING QUALIFIED PRESERVATION SERVICE FOR QESIG/QESEAL

Preservation under eIDAS ensures the long-term preservation of the *trustworthiness* of electronic signatures and seals, in order (cf. Recital (61) of eIDAS) "*to ensure their legal validity over extended periods of time and guarantee that they can be validated irrespective of future technological changes*".

Requirements for qualified preservation service for qualified electronic signatures are laid down in Article 34 of eIDAS Regulation, which defines the purpose of such preservation to be "extending the trustworthiness of the qualified electronic signature beyond the technological validity period".

This type of service should not be confused with electronic archiving aimed at ensuring that a document is stored (or converted from a paper-based original version) in order to guarantee its integrity and benefit from legal features). Electronic archiving has not been identified as a trust service under eIDAS (as detailed in the definition under Article 3(16), which is a closed list of trust services). Consequently, the definition of requirements on electronic archiving remains the competence of Member States. More information on the differences and relationships between an archival service and a preservation service can be found in [TS 119 511], such as:

- The preservation of an electronic signature could be achieved through PKI-based signature augmentation, without storage by the TSP;
- The preservation of an electronic signature could be achieved through electronic archiving (i.e. with storage by the TSP) ensuring that the signature has not been modified since its submission to the TSP.

Requirements for a qualified preservation service for qualified electronic seals are laid down in Article 40 and states that Article 34 "*shall apply mutatis mutandis to the […] preservation of qualified electronic seals*".

Figure 10: Requirements for QTSP providing qualified preservation service for QESig / QESeal

The table below indicates whether a mapping with eIDAS Regulation and whether a conformity assessment checklist for this type of trust service are currently provided by ETSI standards:

	Available	Standard reference
Mapping with eIDAS Regulation	Yes	Annex B of [TS 119 511]
Conformity assessment checklist	No	N/A

3.3.1 Article 34 (Qualified preservation service for QESig/QESeal)

Article 34.1 states that:

> *A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.*

Standards that are proposed by ETSI to TSP providing preservation services are:

- [TS 119 511] "Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques";
- [TS 119 512] "Protocols for trust service providers providing long-term data preservation services".

More specifically, in order to achieve compliance with Article 34 (resp. Article 40), [TS 119 511] sets requirements on:

- Cryptographic monitoring in clause 7.14. In particular, [TS 119 312] may be considered when evaluating the cryptographic algorithm (NOTE: this standard may be superseded by national recommendations);
- Augmentation of preservation evidences in clause 7.15;
- Preservation evidences in clause 9.2;
- Preservation of digital signatures in clause 9.3;
- Verification of the qualified status of the signature or the seal in OVR-A-02.

In line with Article 24.2(e) on trustworthy systems, in order to ensure secure communication between the preservation client and the PSP (authentication of the client and confidentiality of the data), [TS 119 511] refers to [TS 119 512] for the preservation protocol (clause 8.1).

3.4 REQUIREMENTS FOR QTSP ISSUING QUALIFIED ELECTRONIC TIME STAMPS

The eIDAS Regulation defines in Article 3(33) an electronic time stamp as *data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time*.

A qualified electronic time stamp is defined in Article 3(34) as *an electronic time stamp which meets the requirements laid down in Article 42*. A qualified time stamp enjoys the legal presumption of the accuracy of the date and time it indicates and of the integrity of stamped data from the time of stamping (cf. Article 41(2)).

Figure 11: Requirements for QTSP issuing qualified electronic time stamps

The table below indicates whether a mapping with eIDAS Regulation and whether a conformity assessment checklist for this type of trust service are currently provided by ETSI standards:

	Available	Standard reference
Mapping with eIDAS Regulation	Partial	Annex E of [EN 319 421]
Conformity assessment checklist	Yes	Annex H of [EN 319 421]

3.4.1 Article 42 (Qualified electronic time stamp)

Article 42 states that:

> *A qualified electronic time stamp shall meet the following requirements:*
>
> *a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;*
> *b) it is based on an accurate time source linked to Coordinated Universal Time; and*
> c) *it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.*

Standards that are proposed by CEN and ETSI to TSP providing a time-stamping service are:

- [EN 319 421] "Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps" enforcing good security practices and correct time-management of a timestamping authority;
- [EN 319 422] "Time-stamping protocol and electronic time-stamp profiles" ensuring the binding of the date and time to data in the produced timestamps;
- [EN 419 231] "Protection profile for trustworthy systems supporting time stamping".

More specifically, in order to aim for compliance with Article 42, [EN 319 421] specifies that:

- Issued time stamps shall conform with the time stamp profile defined in [EN 319 422]. This intends to achieve compliance with the eIDAS definition of an electronic time stamp;
- Time stamps shall be issued securely. This is covered by clause d) and e) of [EN 319 421] clause 7.7.1. This intends to achieve compliance with clause a) and c) of Article 42;
- Time stamps shall include the correct time. This is covered by clause a), b), and c) of [EN 319 421] clause 7.7.1 and clause 7.7.2. This intends to achieve compliance with clause b) of Article 42.

Regarding the secure issuance of the time stamp, following [EN 319 421], it shall be signed using a key generated exclusively for this purpose. To that end, this key is stored in a time stamping unit (TSU) that is defined as a set of hardware and software which is managed as a unit and has a single time stamp signing key active at a time. [EN 319 421] specifies specific requirements for the generation, protection, rekeying, and expiration of this TSU's signing key in clause 7.6.

In particular, the TSU shall be trustworthy and comply with Article 24.2(e). For that purpose, CEN issued [EN 419 231] to provide a protection profile dedicated to trustworthy systems supporting time stamping.

3.5 REQUIREMENTS FOR QTSP PROVIDING QUALIFIED ELECTRONIC REGISTERED DELIVERY SERVICES

The eIDAS Regulation defines in Article 3(36) an electronic registered delivery service as a *service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations*.

In practice, the data referred to by that definition as being transmitted under such a service from a sender to a receiver can be of any type, including electronic documents (initially created in electronic form or dematerialised documents), structured or not. The transmission means can be of any kind as well including but not limited to email. When the registered delivery service is built on the formats, protocols and mechanisms used in ordinary e-mail messaging, the service is called “registered electronic mail service” by the standard literature.

A qualified electronic registered delivery service (QERDS) is an electronic registered delivery which meets the requirements laid down in Article 44 (cf. Article 3(37) of eIDAS). It should be noted that a QERDS may directly transfer data from the sender to addressee or use (possibly a network of) other QERDS services.

Figure 12: Requirements for QTSP providing qualified electronic registered delivery services

The table below indicates whether a mapping with eIDAS Regulation and whether a conformity assessment checklist for this type of trust service are currently provided by ETSI standards:

	Available	Standard reference
Mapping with eIDAS Regulation	No	N/A
Conformity assessment checklist	No	N/A

3.5.1 Article 44 (Qualified electronic registered delivery service)

Article 44.1 states that:

> *Qualified electronic registered delivery services shall meet the following requirements:*
>
> *a) they are provided by one or more qualified trust service provider(s);*
> *b) they ensure with a high level of confidence the identification of the sender;*
> *c) they ensure the identification of the addressee before the delivery of the data;*
> *d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;*
> *e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;*
> *f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.*
>
> *In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers.*

Regarding clause (a), the boundaries of qualified electronic registered delivery service are established by a network of qualified trust service providers. QTSP should manage these relationships and make sure that the entire "qualified electronic delivery network" it uses is based on the services from qualified trust service providers, present in an eIDAS trusted list for providing such kind of service.

Then, standards that are proposed by ETSI to TSP providing electronic registered delivery services are:

- [EN 319 521] "Policy and security requirements for Electronic Registered Delivery Service Providers";
- [EN 319 522] multi-part deliverable providing technical specifications for Electronic Registered Delivery Services;
- [TS 119 524] multi-part deliverable providing requirements for Testing Conformance and Interoperability of Electronic Registered Delivery Services;
- [EN 319 531] "Policy and security requirements for Registered Electronic Mail Service Providers";
- [EN 319 532] multi-part deliverable providing technical specifications for Registered Electronic Mail Services;
- [TS 119 534] multi-part deliverable providing requirements for Testing Conformance and Interoperability of Registered Electronic Mail Services.

In particular, [EN 319 531] mostly rely on [EN 319 521] which defines specific provisions for qualified electronic registered delivery services regarding the following aspects:

- User content integrity and confidentiality in clauses 5.1;
- User identification and authentication in clause 5.2;
- Time reference in clause 5.3;
- Events and evidence in clause 5.4.

3.6 REQUIREMENTS FOR QTSP PROVIDING REMOTE QSCD SERVICES

The eIDAS Regulation defines in Article 3(12) a qualified electronic signature as *an advanced electronic signature that is created by a qualified electronic signature creation device*

[(QSCD[36])], *and which is based on a qualified certificate for electronic signatures*. The same definition applies mutatis mutandis to a qualified electronic seal.

The Regulation also states through Recital(51) that it should be possible for the signatory (resp. creator of the seal) to entrust QSCDs to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory (resp. creator of the seal) has sole control (resp. control) over the use of his electronic signature/seal creation data, and the qualified electronic signature/seal requirements are met by the use of the device.

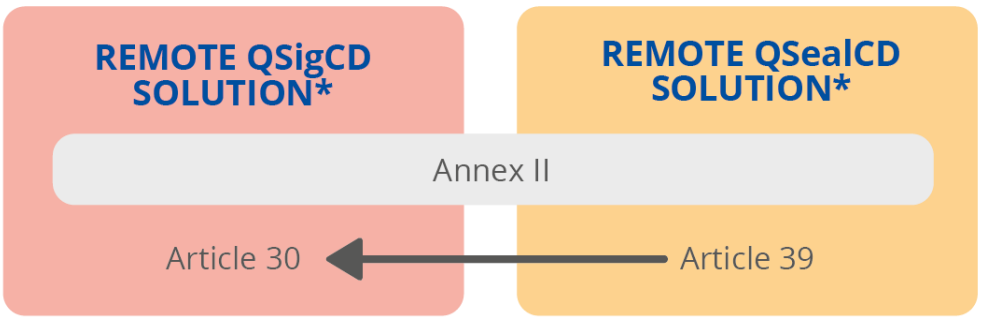
It is worth mentioning that a standard designed for signature and aiming thus to ascertain the sole control, might be too severe for seal. To this regard, [TR 419 210] can be used to assess what can or cannot be done when aiming to achieve a certain context of creation of the seal (local versus remote (applicable to TSP), shared authentication, shared key, etc.) while complying to these norms.

As stated in eIDAS Recital (52), *in order to ensure that such electronic signatures*[/seals] *receive the same legal recognition as electronic signature*[/seals] *created in an entirely user-managed environment, remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products*. For that purpose, remote QSCDs may only be provided by QTSPs.

It should also be noted that the management of a remote QSCD as a service is not a qualified trust service per se but, as it shall be provided by a QTSP, this section proposes guidelines for the provision of such a service (on top of the ones provided in Section 2) pursuant to the objective of the present document to provide recommendations for QTSPs.

Following the definition of a QSCD, such a device shall meet the requirements laid down in Annex II. Hence, its conformity to those requirements shall be certified according to Articles 30(1) and (3) for QSigCD or 39(2) for QSealCD.

Figure 13: Requirements for QTSP providing remote QSCD services



[36] QSCD stands for both QSigCD and QSealCD. In case of ambiguity or necessity, the explicit acronym QSigCD or QSealCD is used.

3.6.1 Annex II and Articles 30 and 39 (Requirements and certification)

Pursuant to Annex II, the standard that is proposed by ETSI to QTSP providing service components operating a remote QSCD is [TS 119 431-1] "Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev", and in particular the EU SSASC[37] policy (EUSCP) defined in this standard.

Pursuant to Article 30(3) and 39(2), the standards for the security assessment of information technology products that apply to the certification of qualified electronic signature creation devices or qualified electronic seal creation devices are laid down in [CID 2016/650].

However, at the time of drafting the [CID 2016/650], there were no available standards yet for signing devices operated by a trust service provider generating or managing signature creation data on behalf of the user to support the creation of qualified electronic signature / seals, and the security assessment of products were performed via "alternative processes" as defined under Article 30(3)b and as notified to the European Commission.

Since then, standards have been published by CEN to address the security assessment of such signing devices[38], namely:

- [EN 419 241-2] "Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing", which refers to [EN 419 241-1][39] "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements"; and
- [EN 419 221-5] "Protection Profiles for TSP Cryptographic Modules - Part 5 – Cryptographic Module for Trust Services".

ENISA produced the report [Assessment of standards related to eIDAS] providing a description, analysis, and assessment of the eligibility of the above-mentioned standards as being suitable references in an amended version of [CID 2016/650][40] and concluded the importance that, on top of those standards:

- The TSP managing the Trustworthy Systems Supporting Server Signing follows [TS 119 431-1] (or equivalent);
- The CA issuing the certificates follows [EN 319 411-1] (or equivalent);
- For qualified devices management and qualified certificates issuance, the verification that such requirements are followed, falls under supervision by the competent supervisory bodies.

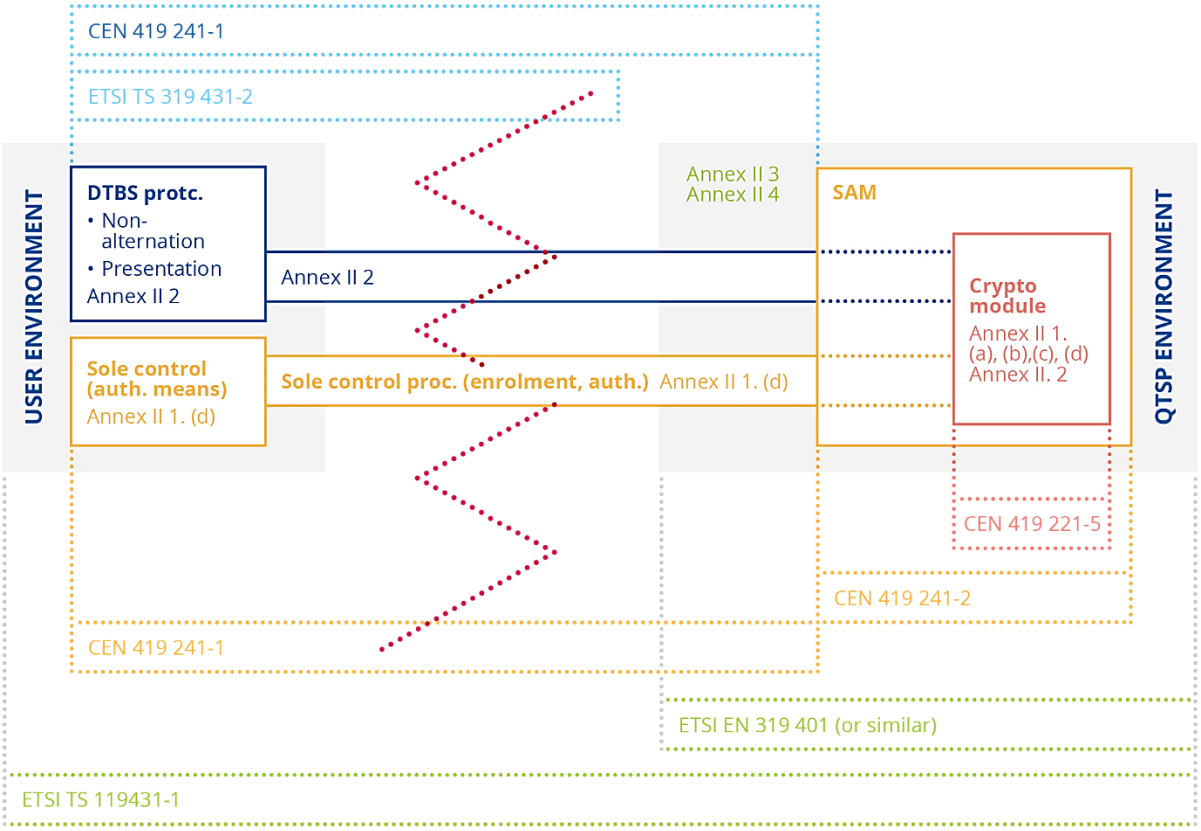
  NOTE: It is worth noting the interrelation between the two. If the QTSP managing the remote QSCD loses its qualified status because its "last" QTS loses its qualified status, the remote QSCD may no longer be considered as a QSCD, although the device may be listed in the European Commission's Compilation of Member States notification on SSCDs and QSCDs[41] (the listing of such certified devices clearly states that a condition for the listed device to be considered as QSCD is to be operated by a QTSP). This has a direct impact on the QTSP issuing the qualified certificates for which the private keys reside on this remote QSCD. The QSCD "status" of these

[37] SSASCD stands for Server Signing Application Service Component.
[38] The availability of new standards does not mean that Article 30.3(b) cannot be called anymore; this article still foresees alternatives in the absence of referred standards to in point (a) of Article 30 or when a security evaluation process referred to in point (a) is ongoing.
[39] It is worth noting that [EN 419 241-1] specifies two assurance levels regarding the sole control on the key by the signatory.
[40] At the time of writing, the update of [CID 2016/650] is under discussion between the European Commission and the Member States. No planning is publicly available.
[41] https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

qualified certificates may not be considered as correct anymore, and signatures created with these private keys may no longer be considered as qualified.

The [Assessment of standards related to eIDAS] report is suggested for additional guidelines relating to the standards listed in the present section. The report also provides, in Section 4.6 and reproduced here below, a figure illustrating how the elements of Annex II that apply in the case where a QTSP manages the QSCDs are covered by existing standards:

Figure 14: Elements of eIDAS Annex II and applicability of the standards



Of particular interest are [CEN 419 221-5] and [ETSI TS 119 431-1] which further provide a mapping between specific clauses and respectively Annex II requirements for the former, elements of the eIDAS Recitals and Annex II requirements for the latter.

4. REFERENCES

4.1 ENISA PUBLICATIONS

ID	Description
ENISA Analysis of standards related to TSP	Analysis of standards related to Trust Service Providers - Mapping of requirements of eIDAS to existing standards https://www.enisa.europa.eu/publications/tsp_standards_2015
ENISA Article 19 Incident reporting	Article 19 Incident reporting - Incident reporting framework for eIDAS Article 19 https://www.enisa.europa.eu/publications/article19-incident-reporting-framework
ENISA Conformity assessment of qualified trust service providers	Assessment of qualified trust service providers. Conformity assessment https://www.enisa.europa.eu/publications/assessment-of-qualified-trust-service-providers/
ENISA Security Framework for TSPs	Security Framework for TSPs https://www.enisa.europa.eu/publications/security-framework-for-trust-providers/
ENISA Security Framework for QTSPs	Security Framework for QTSPs https://www.enisa.europa.eu/publications/security-framework-for-qualified-trust-providers
ENISA Guidelines on Initiation of Qualified Trust Services	Guidelines on Initiation of Qualified Trust Services - Technical guidelines on trust services https://www.enisa.europa.eu/publications/tsp-initiation
ENISA Guidelines on Supervision of Qualified Trust Services	Guidelines on Supervision of Qualified Trust Services - Technical guidelines on trust services https://www.enisa.europa.eu/publications/tsp-supervision
ENISA Guidelines on Termination of Qualified Trust Services	Guidelines on Termination of Qualified Trust Services - Technical guidelines on trust services https://www.enisa.europa.eu/publications/tsp-termination
ENISA Towards global acceptance of eIDAS audits	Towards global acceptance of eIDAS audits https://www.enisa.europa.eu/publications/towards-global-acceptance-of-eidas-audits

4.2 APPLICABLE LEGISLATION

ID	Description
eIDAS, 2014	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. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
CID 2015/1505	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. OJ L 235, 9.9.2015, p. 26–36. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015D1505
CID 2016/650	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. OJ L 109, 26.4.2016, p. 40–42 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016D0650
ANSSI, 2017	Organismes d'évaluation de la conformité des prestataires de service de confiance. Critères de reconnaissance au titre du règlement eIDAS. Available from http://www.ssi.gouv.fr.
NSA-CS	NSA, Certifikačná schéma pre eIDAS, Verzia 0.3 http://ep.nbu.gov.sk/kca/tsl/CertifikacnaSchemaNBU.pdf
DKPv2	Ministry of Interior of the Czech Republic, A document specifying the requirements for qualified providers of trust services and their qualified trust services, version 2i, 12.03.2018. https://www.mvcr.cz/mvcren/ViewFile.aspx?docid=22021696

4.3 STANDARDS AND OTHERS

ID	Description
ANSSI DCSSI-PP	DCSSI-PP-2008/07: Time-stamping System Protection Profile
CA/B Forum network security guide	CA/Browser Forum: "Network and certificate system security requirements"
CA/B Forum baseline requirements	CA/Browser Forum: “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”
CA/B Forum EV guidelines	CA/Browser Forum: “Guidelines For The Issuance And Management Of Extended Validation Certificates”
FIPS PUB 140-2	FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules"
Recommendation ITU-T X.509	ISO/IEC 9594-8/Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks"
RFC 5280	IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
ISO/IEC 15408	ISO/IEC 15408-1:2009: ”Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model”
ISO/IEC 19790	ISO/IEC 19790:2012: ”Information technology — Security techniques — Security requirements for cryptographic modules”
ISO/IEC 20000-1	ISO/IEC 20000-1:2018: “Information technology — Service management — Part 1: Service management system requirements”
ISO/IEC 27001	ISO/IEC 27001:2013: "Information technology — Security techniques — Information security management systems — Requirements"
ISO/IEC 27002	ISO/IEC 27002:2013: “Information technology — Security techniques — Code of practice for information security controls”
ISO/IEC 27005	ISO/IEC 27005:2018: “Information technology — Security techniques — Information security risk management”
ISO/IEC 27099	ISO/IEC CD 27099.2: “Information Technology — Security techniques — Public key infrastructure — Practices and policy framework” (Draft / Under development)
ISO/IEC 27701	ISO/IEC 27701:2019: “Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines”

TR 119 000	ETSI TR 119 000: “Electronic Signatures and Infrastructures (ESI); The framework for standardisation of signatures: overview”
EN 319 102-1	ETSI EN 319 102-1: “Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation”
TS 119 102-1	ETSI TS 119 102-1 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation"
TS 119 102-2	ETSI TS 119 102-2: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report"
EN 319 122	ETSI EN 319 122 series: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: "Building blocks and CAdES baseline signatures" Part 2: "Extended CAdES signatures"
EN 319 132	ETSI EN 319 132 series: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: "Building blocks and XAdES baseline signatures" Part 2: "Extended XAdES signatures"
EN 319 142	ETSI EN 319 142 series: Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: "Building blocks and PAdES baseline signatures" Part 2: "Additional PAdES signatures profiles"
TS 119 172	ETSI TS 119 172 series: Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: "Building blocks and table of contents for human readable signature policy documents" Part 2: "XML Format for signature policies" Part 3: "ASN.1 Format for signature policies" Part 4: "Signature validation policy for European qualified electronic signatures/seals using trusted lists"
TR 419 210	CEN TR 419 210: “Applicability of CEN Standards to Qualified Electronic Seal Creation Device under the EU Regulation N°910/2014 (eIDAS)”
EN 419 221-5	CEN EN 419 221-5: “Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services”
EN 419 231	CEN EN 419 231: "Protection profile for trustworthy systems supporting time stamping"
EN 419 241-1	CEN EN 419 241-1: "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements”
EN 419 241-2	CEN EN 419 241-2: "Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing”
TS 119 312	ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites"
EN 319 401	ETSI EN 319 401 (v2.2.1): "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
TS 119 403-3	ETSI TS 119 403-3: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers"
EN 319 411-1	ETSI EN 319 411-1 (v1.2.2): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements"
EN 319 411-2	ETSI EN 319 411-2 (v1.1.1): "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"
EN 319 412-2	ETSI EN 319 412-2 (v2.2.2): "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons"
EN 319 412-3	ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons"

EN 319 412-4	ETSI EN 319 412-4: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates"
EN 319 412-5	ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QcStatements"
EN 319 421	ETSI EN 319 421 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps"
EN 319 422	ETSI EN 319 422 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles"
TS 119 431-1	ETSI TS 119 431-1 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev"
TS 119 441	ETSI TS 119 441 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services"
TS 119 442	ETSI TS 119 442: "Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services"
TS 119 495	ETSI TS 119 495: “Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366”
TS 119 511	ETSI TS 119 511: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques"
TS 119 512	ETSI TS 119 512: "Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services"
EN 319 521	ETSI EN 319 521 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers"
EN 319 522	ETSI EN 319 522 series: Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1 (v1.1.1): "Framework and Architecture" Part 2: "Semantic contents" Part 3: "Formats" Part 4: "Bindings: Sub-part 1: "Message delivery bindings" Sub-part 2: "Evidence and identification bindings" Sub-part 3: "Capability/requirements bindings"
TS 119 524	ETSI TS 119 524 (all parts): "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Electronic Registered Delivery Services"
EN 319 531	ETSI EN 319 531 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers"
EN 319 532	ETSI EN 319 532 series: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 1 (v1.1.1): "Framework and Architecture" Part 2: "Semantic contents" Part 3: "Formats" Part 4: "Interoperability profiles"
TS 119 534	ETSI TS 119 534 (all parts): "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Registered Electronic Mail Services"
EN 301 549	EN 301 549: “Accessibility requirements for ICT products and services”
TS 119 612	ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists"

TS 119 615	ETSI TS 119 615: "Electronic Signatures and Infrastructures (ESI); Trusted Lists; Procedures for using and interpreting European Union Member States national trusted lists"
TR 103 684	ETSI TR 103 684: “Electronic Signatures and Infrastructures (ESI); Global Acceptance of EU Trust Services”

TP-01-20-723-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

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

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-438-1
DOI: 10.2824/777927