enisa

THE EU CYBER SECURITY AGENCY

w9/haa9b5!¢Lhb{ FOR QTSPs BASED ON STANDARDS

Technical guidelines on trust services

DECEMBER 2017

About ENISA

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

Contact

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

Acknowledgements

We would like to thank all those who contributed to this study and reviewed it, specifically the experts and the members of national supervisory bodies, conformity assessment bodies and various trust service providers.

ISBN: 978-92-9204-191-5
doi: 10.2824/721561 Catalogue number: TP-06-16-342-EN-N

Table of Contents

Executive Summary

Regulation (EU) No 910/2014[1] (hereafter 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[2].

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 in particular the trust of small and medium-sized enterprises (SMEs) and consumers in the internal market and to promote the use of trust services and products, the eIDAS Regulation introduces the notions of **qualified trust service** and **qualified trust service provider** with a view to indicating requirements and obligations that ensure high-level security and a higher presumption of their legal effect.

Following the publication of the eIDAS Regulation, a set of secondary and co-regulatory acts had to be published in order to provide technical guidance on how to implement the specific requirements of the eIDAS Regulation (in the TSP part of eIDAS, the European Commission decided to publish only the mandatory ones). ENISA aimed to develop a concise set of technical guidelines implementing the eIDAS Regulation in the non-mandatory articles, for voluntary use of all stakeholders, including Trust Service Providers, Supervisory Bodies and Conformity Assessment Bodies.

The objective of this document is to provide guidelines for fulfilling requirements originating from the following articles of the eIDAS Regulation:

- Art. 24.5 – Requirements for qualified trust service providers;
- Art. 28.6 – Qualified certificates for electronic signatures;
- Art. 32.3 – Requirements for the validation of qualified electronic signatures;
- Art. 33.2 – Qualified validation service for qualified electronic signatures;
- Art. 34.2 – Qualified preservation service for qualified electronic signatures;
- Art. 38.6 – Qualified certificates for electronic seals;
- Art. 42.2 – Requirements for qualified electronic time stamps;
- Art. 44.2 – Requirements for qualified electronic registered delivery services;
- Art. 45.2 – Requirements for qualified certificates for website authentication

[1] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

1. Introduction

1.1 General overview

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 (eIDAS Regulation) and repealing Directive 1999/93/EC[2] is a milestone for providing a predictable regulatory environment enabling secure and seamless electronic interactions between businesses, citizens and public authorities.

The eIDAS Regulation:

- Ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other Member States where eIDs are available and identification scheme is notified to the European Commission.
- Creates a European internal market for trust services (eTSs) - namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication.

In a nutshell, this Regulation renders that electronic identification (eID) and electronic Trust Services (eTS) as key enablers for secure cross-border electronic transactions and central building blocks of the Digital Single Market.

Since 1 July 2016 the eIDAS Regulation is directly applicable in EU Member States. It provides legal certainty and encourages the usage of electronic identification means and trust services for online access and online transactions at EU level.

The eIDAS Regulation ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other Member States where eIDs are available and identification scheme is notified to the European Commission. It also creates an EU wide internal market for electronic trust services by ensuring they will be recognised and functional across borders and have the same legal status as traditional paper based procedures. National eIDs are recognised by foreign public services if :

- These eIDs are delivered in a notified scheme;
- The public service accepts another notified eID of level substantial or high.

Qualified trust services have legal effects, but they are not necessarily the same as traditional paper based procedures (with the exception of the qualified signature which is equivalent to a handwritten signature).

Following the publication of the eIDAS regulation, a set of secondary and co-regulatory acts could be published in order to provide technical guidance on how to implement the specific requirements of the eIDAS Regulation (in the TSP part of eIDAS, the European Commission decided to publish only the mandatory ones). ENISA aimed to develop a concise set of technical guidelines implementing the eIDAS Regulation in the non-mandatory articles, for voluntary use of all stakeholders, including Trust Service Providers, Supervisory Bodies and Conformity Assessment Bodies. However it is encouraged to stakeholders to verify that these guidelines are accepted by their national Supervisory Body.

[2] See Annex B [No. 4] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093

Furthermore, to effectively bring about the objectives of the eIDAS Regulation, such as improving customer protection in internet transactions, work needs to be carried out to communicate on risks and promote the acceptance and adoption of trust services in Europe. To achieve this, understanding the main aspects of ENISA guidelines mentioned above can be helpful. Through better understanding the risk management can be improved.

ENISA is supporting the implementation of the eIDAS Regulation since 2013 by:

- providing security recommendations for a correct implementation of trust services,
- mapping technical and regulatory requirements,
- promoting the deployment of qualified trust services in Europe,
- informing relying parties and end users on how to secure their electronic transactions using trust services, etc.

1.2 Scope of the document

Taking into account the complexity of the subject, wide sgacope of services and number of potentially applicable standards, it is extremely relevant to provide an extensive and an as far as possible up-to-date set of standards enabling all stakeholders to understand and perform eIDAS compliant activities. Most of the standards are currently created by European Standardisation Organisations under standardisation requests from the European Commission (former mandate m/460). This set of standards builds on a number of existing internationally recognised standards and guidelines from ISO, ITU-T, CAB Forum and IETF.

The objective of this document, following the ENISA deliverable from 2015, “Analysis of standards related to Trust Service Providers - Mapping of requirements of eIDAS to existing standards” is to review and produce guidelines for fulfilling requirements originating from the following articles of the eIDAS Regulation:

- Art. 24.5 – Requirements for qualified trust service providers;
- Art. 28.6 – Qualified certificates for electronic signatures;
- Art. 32.3 – Requirements for the validation of qualified electronic signatures;
- Art. 33.2 – Qualified validation service for qualified electronic signatures;
- Art. 34.2 – Qualified preservation service for qualified electronic signatures;
- Art. 38.6 – Qualified certificates for electronic seals;
- Art. 42.2 – Requirements for qualified electronic time stamps;
- Art. 44.2 – Requirements for qualified electronic registered delivery services;
- Art. 45.2 – Requirements for qualified certificates for website authentication

Other articles, where standards could prove to be useful to CABs and SBs in assessing the compliance with the Regulation are 5.1, 13.2, 15, 19.1, 19.2, 24.1, 24.2 (except e & f), 24.3, 24.4, 26, 28.3, 28.4, 28.5, 36, 38.3, 38.4, 38.5.

This guideline will help all stakeholders to understand the mapping between the articles mentioned above and reference numbers of standards, as well as practical recommendations for their usage. sIt is important to note that some of eIDAS' requirements are not covered by standards yet, e. g. standards for electronic registered delivery are only being developed in ETSI STF 523.

Many of the standards contain references to other standards, often several levels deep. Sometimes the clauses with delegation include some additional requirements. Thus, a detailed set of requirements

corresponding to a particular article from eIDAS Regulation is a collection of requirements from the last referenced document up to the first one.

The process approach is a method of dynamic security and compliance management. Its origins can be traced to the classical school of management: the organization of production processes and ergonomic research. The process approach was described in the ISO 9001:2000[3] standard. In previous standards, this approach did not exist, the systems were implemented according to the standard points. The second amendment of ISO 9000 standard issued in the year 2000 changed the structure of the standard, and described the process approach principle thereby facilitating implementation. Currently, a process approach is the main, fundamental principle in all management standards and best practices.

In the process management approach, each activity can be described as a set of interconnected processes. Each process has goals and an owner, who is accountable for achieving process goals by controlling process performance. Processes transform input into output utilizing resources. Processes have suppliers (input) and clients (output). Input, output, resource utilization and overall process performance can be measured and defined as goals for the accounting process owner, and also for process improvement. Processes flow horizontally through an organization in contrast to vertical organization structure.

Generally, there are three main types of processes: management, core and support, but in this document we will use other taxonomy based on rareness of processes. Some processes exist in each organization, they are called herein after general processes, for example HR, finance. Other processes are common for some common activities independently from TSP, for example Information Security Management System (ISMS described in ISO/IEC 27001[4] standard) or IT service management system (described in ISO/IEC 20000[5] standard). These processes may exist or should be implemented in an organization by process owners not only for TSP purposes. These processes should be shared throughout an organization. There is no other reason to deploy this processes independently for TSP. This approach simplifies process deployment to become TSP. Processes called herein after specific are core TSP processes, required especially for TSP. These processes should be deployed according to an organizational culture similarly to other activities, but requirements for them can be found only in formal standards regarding TSP activity.

To better understand their relations, the authors of these guidelines took into consideration stakeholders of the processes, their requirements, obligations and benefits.

The structure of the document is organised to provide information and guidelines with regards to: the equirements of each article mentioned above

- content
- guideline
- list of standards and other documents (guidelines, recommendations), referred to as ‘standards’
- TSP’s process
- external stakeholders

[3] http://www.iso.org/iso/catalogue_detail?csnumber=21823
[4] See Annex B [No. 61]
[5] See Annex B [No. 60]

It is important to note that the scope of this document is restricted to qualified trust service providers and qualified trust services, with the exception of article 32 which applies to both qualified and non-qualified validation services.

The verbs “shall”, “should” and “may” in this document should be used in accondance with ETSI guide[6].

[6] https://portal.etsi.org/Portals/0/TBpages/edithelp/Docs/AGuideToWritingWorldClassStandards.pdf

2. Requirements for qualified trust service providers

A Qualified Trust Service Provider (QTSP) provides one or more qualified trust services. The TSP needs to submit a notification of its intention to provide qualified trust services together with a conformity assessment report issued by a conformity assessment body to the supervisory body. The supervisory body will analyse whether the TSP meets the applicable eIDAS requirements based on the notification and the conformity assessment report. In case of a positive outcome of this analysis, the qualified status is granted by the supervisory body to the TSP.

Qualified trust service providers are audited at least every 24 months by a conformity assessment body. The audit confirms fulfilment of the requirements laid down in the eIDAS Regulation. The general requirements for qualified trust service providers are laid down in Article 24 of eIDAS Regulation.

The Commission may establish reference numbers of standards for trustworthy systems and products, which comply with the requirements under points (e) and (f) of Article 24 (2). This chapter covers guidelines for TSP's based on standards complying with Article 24 requirements.

2.1 Article 24.1.

CONTENT

Article 24.1. 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*

GUIDELINE

It is recommended to follow chapters EN 319 411-1[7](6.2.2, 6.2.3) and corresponding chapters EN 319 411-2[8] (6.2.2, 6.2.3) in particular, which present the identity verification process. It must be stressed that this process is a critical part of the registration procedure for issuing a qualified certificate.

Generally, the identity verification process in the certificate issuance process have a lot in common with identity proofing process during (notified) issuance of electronic identification means[9]. Therefore, it is advised to familiarize oneself and re-use as a good practice (whenever applicable) technical standards set out by the Commission Implementing Regulation (EU) 2015/1502 for the high and substantial assurance levels of electronic identification means.

The above mentioned EN standards distinguish two types of identity verification:

- initial identification described in EN 319 411-1(6.2.2) and EN 319 411-2 (6.2.2), where the issuance of a certificate is meant for a person not registered (never before) by the QTSP,
- in the re-keying process described in EN 319 411-1 (6.2.3) and EN 319 411-2 (6.2.3), which means in the process of issuance of a new certificate for the person who has already been registered by the QTSP (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 verification (as in chapter 6.2.2).

Further from above mentioned standards, identity verification must be carried out in accordance with the national law of a Member State in which the QTSP has been granted the qualified status. TSPs operating in a cross border situation (for example when enrolment takes place in a different country that the one where QTSP is established) will require further guidance from supervisory bodies.

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

In short the eIDAS Regulation provides four methods of identity verification:

a) face to face,
b) based on electronic identification means,
c) based on a qualified electronic signature or on a qualified electronic seal,

---

[7]See Annex B [No. 28]
http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.01.01_60/en_31941101v010101p.pdf
[8]See Annex B [No. 29]
http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.01.01_60/en_31941102v020101p.pdf
[9] While there are similarities, there are also some differences. As an example, for issuance of electronic identification means, physical face-to-face (or equivalence with it) is not a requirement. While the use of qualified certificate or seal is permitted for the issuance of a qualified certificate (24.1.c), it is not for the issuance of electronic identification means.

d) other methods recognised at national level of the Member State providing equivalent assurance in terms of reliability to physical presence.

In a face to face identification process, where physical identity documents are used, the registration authority personnel must have qualifications with regard to (physical) verification of ID documents and their security features. This should be considered part of the general requirements for personnel of a QTSP as per Article 24.2b and ETSI EN 319 401[10] (see chapter 7.2 Human resources).

In a remote issuance process, electronic identification means (as defined by eIDAS) can be used for identity verification (art. 24.1b).

When issuing a qualified certificate remotely, the identity verification process must provide equivalent assurance in terms of reliability to physical presence. **Therefore, to be compliant (with art. 24.1b) it is (explicitly) mandatory to use electronic identification means for which physical presence was confirmed at any stage of certificate handling** (for exampleat the moment of generating the certificate, or when credentials are handed to the person).

When other methods are used (d), it is necessary to verify that the given method provides assurance equivalent to methods requiring physical presence. This will mean additional documentation needs to be prepared by a QTSP, and the method is to be confirmed by a conformity assessment body and recognised at national level.

Best practice has to yet to be established for how to meet the requirements of article 24.1 b) for physical presence.

ETSI EN 319 411 standard refers to CA/Browser forum documents (applicable in the context of websites) for details of verification procedure:

- EVCG CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates"[11] – see chapter 11,
- BRG CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates"[12] – see chapter 11

If in a given case discrepancies occur between mentioned standards and acts, the priority is as follows:

- eIDAS Regulation,
- implementing and delegated acts related to eIDAS Regulation,
- national legislation,
- standards published by standardization bodies (e.g. CEN/CENELEC/ETSI/ISO)
- guidelines and documents by other bodies (e.g. CA/B forum, IETF)
- other standards.

LIST OF STANDARDS

- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (TSP-QC)

[10]See Annex B [No. 27]
http://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.01.01_60/en_319401v020101p.pdf
[11]See Annex B [No. 56] https://cabforum.org/wp-content/uploads/EV-V1_6_0.pdf
[12]See Annex B [No. 7]

- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (TSP-QC)
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- EVCG CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates" (TSP-QC)
- BRG CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates". (TSP-QC)
- Commission Implementing Regulation (EU) 2015/1502

TSPs PROCESS

- Identity Proofing and Verification[13]
- Human resources
- Compliance Management

EXTERNAL STAKEHOLDERS

- Member State Personal Data Protection Authority
- National authorities
- Signatory
- Creator of a Seal
- Identity Provider

[13] See Annex A

2.2 Article 24.2

Article 24.2 of eIDAS Regulation specifies 11 requirements for TSP's providing qualified trust services. Following subchapters 24.2.a - 24.2.k refer to each requirement and propose standardisation for compliance with it.

2.2.1 Article 24.2.a

CONTENT

[A qualified trust service provider providing qualified trust services shall:]

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

GUIDELINE

This is a new provision compared to Directive 1999/93/EC[14]. There are no detailed rules of such communication in standards, this is a **gap in eIDAS related standardization and good practices should apply**. General provisions somehow applicable to this article are:

- EN 319 401[15] – chapter 6.1 item g) and h), 7.11 and 7.12,
- EN 319 411-1[16] and EN 319 411-2[17] (for certification services),
- EN 319 421[18] (for time stamp services),
- ISO/IEC 27002[19] – chapter 12.1.2.

The gap can be met in a following way:

- For changes in trust services: by simple extension to requirement EN 319 401 clause 6.1,
- For intent to terminate: by EN 319 401 7.12 b i) which is required to be applied "before the TSP terminates".

Implementation of article 24.2.a is strictly 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 based on risk. Informing a supervisory body about changes in provision of qualified trust services, especially about termination, is a countermeasure for subscribers and trusting entities against unnoticed, illegitimate use of trusted mechanisms.

The reporting mechanism should provide event driven triggers and communication channels to report changes to a supervisory body 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.

EN 319 411 part 1 and 2 do not impose any specific requirements / rules related to communication (see chapter 6.8.11). However, it is recommended that such rules should be defined and information about

[14] See Annex B [No. 4]
[15] See Annex B [No. 27]
[16] See Annex B [No. 28]
[17] See Annex B [No. 29]
[18] See Annex B [No. 35]
http://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf
[19] See Annex B [No. 62]

them be included in the Trust Service Practice Statement or Certification Practice Statement. This is derived from EN 319 401, chapter 6.1 (items g and h) requirements. It (item g) states, that "a TSP shall notify of changes it intends to make in its practice statement and shall […] make the revised TSP practice statement available immediately […]". As "any change in the provision of its qualified trust services" (as per provision of this eIDAS article) is in many cases reflected through practice statement change, it is suggested to perform communication with a supervisory body at the same time as subscribers and relying parties, and therefore "immediately". In other cases (changes not reflected in a practice statement), it is suggested to keep the same communication rules, with the exception that intention to terminate activities by its nature should be communicated to a supervisory body earlier (than in the actual termination process).

General requirements regarding a practice statement are also specified in EN 319 411-1 and EN 319 411-2 chapter 5.2 (for certification services) and in EN 319 421 chapter 6.2 (for time stamp services).

Best practices regarding the Change Management process can be found in chapter 12.1.2 of ISO/IEC 27002 standard.

LIST OF STANDARDS

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (TSP-QC, TSP-TS)
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (TSP-QC)
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (TSP-QC)
- ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls (TSP-QC, TSP-TS)

TSPs PROCESS

- Change Management[20]
- Communication Plan
- Practice Statement maintenance

EXTERNAL STAKEHOLDERS

- Member State's Supervisory Bodies
- Relying Parties
- Signatory
- Creator of a Seal

[20] See Annex 1

2.2.2 Article 24.2.b

CONTENT

[A qualified trust service provider providing qualified trust services shall:]

b) 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;

GUIDELINE

It is recommended to follow:

- ETSI EN 319 401[21] - chapter 7.2,
- ISO/IEC 27002[22] – chapter 6.1.1, 6.1.2 and 7,
- ETSI EN 319 411-1[23] and ETSI EN 319 411-2[24] chapters 6.4.4 (for certification services; refers to and amends provisions of ETSI EN 319 401 chapter 7.2),
- ETSI EN 319 421[25] – chapter 7.3 (for time stamp services; fully refers to provisions of EN 319 401 chapter 7.2),
- BRG CA/Browser Forum[26], chapter 14.1.2.

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 an appropriate human resources process and procedures, education programs and keep records of such activities.

This process 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 trust service providers) are set by EN 319 401, chapter 7.2. For detailed provisions this standard refers to ISO/IEC 27002.

Best practices regarding human resources security, security roles and responsibility and segregation of duties countermeasures can be reached in chapter 6.1.1, 6.1.2, 7 of ISO/IEC 27002 standard.

---

[21] See Annex B {No. 27]
[22] See Annex B {No. 62]
[23] See Annex B {No. 28]
[24] See Annex B {No. 29]
[25] See Annex B {No. 35]
[26] See Annex B {No. 7]

For trust service providers issuing certificates, provisions of EN 319 401 are amended with requirements specific to such services (see chapters 6.4.4 in EN 319 411-1 and -2).

In relation to Publicly-Trusted Certificates some additional requirements are provided by the BRG CA/Browser Forum document ("Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates") in chapter 14.1.2.

For trust service providers issuing time stamps, general requirements are applicable – EN 319 421 does not impose any additional requirements in relation to EN 319 401.

LIST OF STANDARDS

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (TSP-QC, TSP-TS)
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (TSP-QC)
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (TSP-QC)
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps; (TSP-TS)
- BRG CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (TSP-QC)
- ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls (TSP-QC, TSP-TS)

TSPs PROCESS

- Human Resources[27]
- Compliance Management

EXTERNAL STAKEHOLDERS

- (none)

[27] See Annex A

2.2.3 Article 24.2.c

CONTENT

[A qualified trust service provider providing qualified trust services shall:]

c) 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;

GUIDELINE

There is no standard defining how to meet this requirement, this is an identified **gap in standardisation**. This matter is only referred to in ETSI standards, with no more guidance than in the Regulation:

- EN 319 401[28] - chapter 7.1.1 item c),
- EN 319 411-1[29] and EN 319 411-2[30] chapter 6.8.2 (fully refers to EN 319 401),

The gap can be addressed by extension to the requirement of EN 319 401 7.1.1 item c), to recommend that the assessment of "financial resources and/or obtain appropriate liability insurance" required should be based on a risk assessment (see clause 5), which takes into account commercial and financial issues.

This area should be treated based on the local (national) rules and legislation (if any) and good practices, as part of risk management. Risk based approach is now the main one in all management systems standards. As a common base, regardless of subject matter, the International Organization for Standardization (ISO) established in 2011 a standard for risk management (ISO 27005[31]) that contains principles and guidelines, and is recommended to use for risk analysis (taking into account financial and commercial aspects) by EN 319 401. At this moment there are no European standards for risk management, and it can be considered as another **standardisation gap** in the eIDAS context.

The most common approach towards treatment of risk of liabilities for damage is **risk sharing**, and the most common countermeasure is **insurance** against the risks. A QTSP should check 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 the activity. This will allow identification of regulatory expectations as well as enable meeting of its liability to external parties.

This is part of Compliance Management. If a regulator expects a TSP to declare an amount of liabilities, it is the most cost effective to establish a Risk Management Process. Analysis of threats and potential losses per service allow a TSP to calculate an amount of money to allocate to assure compensation for potential damages or define insurance requirements and conditions.

Best practices regarding risk management process can be reached in ISO 31000 standard.

LIST OF STANDARDS

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (TSP-QC, TSP-TS)
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (TSP-QC)

[28] See Annex B [No. 27]
[29] See Annex B [No. 28]
[30] See Annex B [No. 29]
[31] See Annex B [No. 63]

- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (TSP-QC)
- ISO 31000:2009 Risk management - Principles and guidelines

TSPs PROCESS

- Compliance Management[32]
- Risk Management

EXTERNAL STAKEHOLDERS

- Member States Supervisory Bodies
- Relying Parties
- Signatory
- Creator of a Seal

[32]See Annex A

2.2.4 Article 24.2.d

CONTENT

[A qualified trust service provider providing qualified trust services:]

d) 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;

GUIDELINE

It is recommended to follow:

- EN 319 401[33] – chapter 6.2
- EN 319 411-1[34] – chapter 6.1 items c), d), e), f), 6.3.4 items a), b), c) and chapter 6.9.4, Annex A (for trust services, where applicable),
- EN 319 411-2[35] - chapter 6.1, 6.3.4; 6.9.4 (for qualified trust services, where applicable),
- BRG CA/Browser Forum[36], clause 9.6.3, 9.8 (for Publicly-Trusted Certificates),
- EVCG CA/Browser Forum[37], clause 11.8 (for Extended Validity Certificates),
- EN 319 421[38], chapter 6.3 (for time stamp; it fully relies on EN 319 401 chapter 6.2).

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 by stakeholders.

To fulfil this requirement a QTSP may create a Service Policy document that contains all necessary information (as listed in chapter 6.2 of EN 319 401) and include it as an attachment to the subscriber agreement, as well as make it available in an electronic form (eg. PDF file) on the QTSP's web page. The good practice is "involving" an acceptance method, such as a mandatory acceptance box or necessity of scrolling down and an acceptance button at the end.

In case of use of electronic communication channels, a QTSP should assure availability and integrity of the document with its terms and conditions. In the case of qualified certificates, it should be signed with an Advanced Electronic Signature or an Advanced Electronic Seal as specified by eIDAS Regulation.

The content of such a document should include items as specified in above mentioned standards.

EN 319 401 in chapter 6.2 defines general requirements for content of the terms and conditions information regarding its services, that shall be available to all subscribers and relying parties. These terms and conditions shall specify for each trust service information such as: service policy being applied, limitations on the use of the service (e.g. lifetime of public key certificates), information for relying parties on how to verify the trust service token, subscribers' obligations, limitations of liability, TSP contact information and other. Terms and conditions shall be made available through durable means of

[33] See Annex B [No. 27]
[34] See Annex B [No. 28]
[35] See Annex B [No. 29]
[36] See Annex B [No. 7]
[37] See Annex B [No. 56]
[38] See Annex B [No. 35]

communication, in particular it can be transmitted electronically. These are requirements that are independent of the type of TSP. Other standards (described below) refine and extend these requirements as applicable to particular forms of TSP.

For certification services, there are additional conditions defined in EN 319 411-1 and -2.

For Publicly-Trusted Certificates clause 9.6.3 and 9.8 (with the exception indicated in EVCG clause 18) of BRG should apply additionally.

For Extended Validity Certificates, EVCG clause 11.8 should apply additionally.

The terms and conditions may use the model “PKI disclosure statement” given in annex A of EN 319 411-1. PDF/A file format is highly recommended.

The document, containing terms and conditions of a qualified trust service, should be maintained as a part of the Documentation Management process. The process should be effective and under control.

LIST OF STANDARDS

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (TSP-QC, TSP-TS)
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (TSP-QC)
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (TSP-QC)
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (TSP-TS)
- EVCG CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates" (TSP-QC)
- BRG CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (TSP-QC)
- ISO/IEC 20000-1:2011 Information technology -- Service management -- Part 1: Service management system requirements (TSP-QC, TSP-TS)
- ISO/IEC Directives, Part 1, Annex SL (TSP-QC, TSP-TS) – as guidance

TSPs PROCESS

- Documentation management[39]

EXTERNAL STAKEHOLDERS

- Relying Parties
- Signatory
- Creator of a Seal

[39] See Annex A

2.2.5 Article 24.2.e

CONTENT

[A qualified trust service provider providing qualified trust services shall:]

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

GUIDELINE

There are no definitions of "trustworthy system" and "trustworthy products". These terms can be defined differently depending on the type of the service.

Depending on the purpose, a "trustworthy" system or product can be made of a certified hardware component (hardware security module) or non-certified hardware (e.g. servers) or certified or non-certified software components or combination of all the aforementioned.

In addition, general means can/should be applied to achieve "trustworthiness" of a system or product:

- EN and ETSI standards,
- international standards (e.g. ISO), national and industry standards,
- best practises,
- security evaluation and certification by an independent body,
- declaration of conformity,
- technical, procedural and organisational means,
- hardware and software.

It is assumed that for any "trustworthy" system all basic requirements are met, in particular:

- EN 319 401[40] - chapter 7.4 items a) and f), 7.5, 7.6, 7.7 and 7.8 (for all trust service providers),
- EN 319 411-1[41] – chapter 6.5 (additional for trust service providers issuing certificates),
- EN 319 411-2[42] chapter 6.5 (additional for trust service providers issuing qualified certificates),
- EN 319 421[43] – chapter 7.6, 7.8, 7.9, 7.10 (for trust service providers issuing time stamps),
- ISO/IEC 27002[44] – chapter 9, 10, 12, 14, 15.

With regard to certificate management, detailed requirements for "trustworthy system" are provided in CEN/TS 419 261.

With regard to remote (server) signature, detailed requirements for "trustworthy system" are provided in EN 419 241-1 (under drafting).

For certification and time stamp services, with regard to (secret) key generation and storage, a trustworthy system is a Hardware Security Module (HSM) – see EN 319 411-1 (clause 6.5.2) and EN 319 421 (clause 7.6.2 and 7.6.3) accordingly.

[40] See Annex B [No. 27]
[41] See Annex B [No. 28]
[42] See Annex B [No. 29]
[43] See Annex B [No. 35]
[44] See Annex B [No. 62]

Generally, article 24.2 e covers a wide range of security management process issues. Requirements included in European standards are additional countermeasures to well known, internationally accepted best practices, i.e. ISO/IEC 27002.

These requirements do not relate only to trustworthy systems and products that appear in dedicated QTSPs processes, polices, etc. (i.e. key management, certification policy, etc.), but they are also related to supporting processes.

Therefore, it is recommended that QTSP takes into account the above mentioned requirements and according to them develops security means and controls in the following supporting processes:

- Supplier service delivery management,
- System acquisition, development and maintenance management,
- Communications security management,
- Operations security management,
- Access control management.

Additional information about supporting processes and security issues can be found in ISO/IEC 27002:2013 and ISO/IEC 20000-1:2011[45]

With regard to technical security, hardware security modules (HSMs) are recommended, and security certification is a common and recommended way of ensuring conformity with security requirements and achieving "trustworthiness" in the context of eIDAS Regulation.

This is to be stressed, that generally a “trustworthy system” may not be limited to a HSM only.

EN 319 411-1 (clause 6.5.2) and EN 319 421 (clause 7.6.2 and 7.6.3) mandate that for certification and time stamp services subscribers’ and authorities’ cryptographic (private) keys are generated and stored in a certified HSM (“trustworthy system”). The HSMs should be certified at assurance level EAL4 or higher in accordance with ISO/IEC 15408 (Common Criteria), ISO/IEC 19790 or FIPS 140-2 L3 (all listed by EN 319 411-1), or equivalent national or internationally recognized evaluation criteria for IT security. With the general availability of devices which meet ISO 15408, it is expected that ISO 19790 and FIPS PUB 140-2 will no longer be acceptable.

ENISA recommends to use Common Criteria evaluated devices, based on protection profiles delivered by ETSI and CEN (described below), to create a presumption of compliance and ease conformity assessment.

ENISA recommends to use certified HSMs for the generation and storage of cryptographic keys and sensitive material for any kind of trust service.

ETSI and CEN WG17 provide guidelines and Protection Profiles for certification in the series of standards EN 419 2x1.

For certification of HSM dedicated for QTSP root certification authority operations (signing, key generation) CEN EN 419 221-2[46], -3[47] and -4[48] can be applied in accordance to their purposes, or CEN EN

[45] See Annex B [No. 60]
[46] See Annex B [No. 14]
[47] See Annex B [No. 15]
[48] See Annex B [No. 16]

419 221-5[49] (a new, generic PP for trust services), once it is finalised by CEN (at the time of this report, works are still ongoing).

For certification of a trustworthy system / HSM for time stamp services, CEN EN 419 231[50] can be applied or CEN EN 419 221-5 (a new, generic PP for trust services), once it is finalised by CEN (for the time of this report, works are still ongoing). Alternatively, ANSSI DCSSI-PP 2008/07[51] can be used, which is currently the only Common Criteria evaluated protection profile for a timestamping system.

It is recommended to comply with this kind of service and aim to meet requirements of art. 30 and 39 of the eIDAS. It is expected that this will be referenced in eIDAS through the Commission Implementing Decision "laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2)[…]"[52]and becomes obligatory in the near future.

However, at the time of writing this report, this standard has not yet been issued (works are still ongoing in CEN)[53]. Until the moment CEN TS 419 241-2[54]is available and referenced in an implementing act, alternative standards / Protection Profiles can be used (for performing evaluation and certification of a trustworthy system for server signature) provided they ensure a comparable security level. An example of such a standard is Protection Profile DCSSI-PP 2008/07 issued (and certified) by ANSSI. When the alternative standards are applied by a TSP, however, a Conformity Assessment Body and an auditor may require additional proof of adequacy of such standards to the given purpose and/or additional security measures might be necessary for the TSP. This may mean for example documentation describing relevance of such standards and/or mapping of actual trustworthy system components, expert opinion, etc. Any alternative certification scheme can only be valid if it has first been notified to the European Commission as required by Article 30(3)(b) of the eIDAS Regulation. Some alternative methods have been already notified[55].

LIST OF STANDARDS

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (TSP-QC, TSP-TS)
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (TSP-QC)
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (TSP-QC)
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (TSP-TS)
- BRG CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (TSP-QC)

---

[49] See Annex B [No. 8]
[50] See Annex B [No. 9]
[51] See Annex B [No. 5]
[52]Current act reference is Commission Implementing Decision (EU) 2016/650
[53]For such a standard, being a protection profile, it means the text be must be adopted, as well as it must be evaluated and certified by and independent security certification body. After this it can be used to certify actual products or system.
[54] See Annex B [No. 11]
[55] https://ec.europa.eu/futurium/en/content/list-alternative-processes-notified-commission-accordance-article-303b-and-392-eidas

- ETSI TS 119 312 (an update is in progress) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites (TSP-QC)
- CEN/TS 419 261:2015 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures (TSP-QC)
- CEN EN 419 221-1 Protection profiles for TSP Cryptographic modules – Part 1: Overview
- CEN EN 419 221-2 Protection profiles for TSP Cryptographic modules – Part 2: Protection profile for Cryptographic module for CSP signing operations with backup
- CEN EN 419 221-3 Protection profiles for TSP Cryptographic modules – Part 3: Protection profile for Cryptographic module for CSP key generation services
- CEN EN 419 221-4 Protection profiles for TSP Cryptographic modules – Part 4: Protection profile for Cryptographic module for CSP signing operations
- (draft) CEN EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services (not publicly available and not security evaluated yet)
- CEN EN 419 231, "Security requirements for trustworthy systems supporting time-stamping"
- CEN TS 419 241-1, "Trustworthy systems supporting server signing" Part 1: Security requirements (UNDER DRAFTING)
- (draft) CEN TS 419 241-2, "Trustworthy systems supporting server signing" Part 2:Protection Profile for QSCD for Server Signing (UNDER DRAFTING)
- Protection Profile ANSSI DCSSI-PP 2008/07
- ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls (TSP-QC, TSP-TS)
- ISO/IEC 20000-1:2011 Information technology -- Service management -- Part 1: Service management system requirements (TSP-QC, TSP-TS).
- ISO/IEC 15408 (parts 1 to 3): Information technology - Security techniques - Evaluation criteria for IT security
- ISO/IEC 19790:2006, Information technology - Security techniques - Security requirements for cryptographic modules[56]
- FIPS 140-2

TSPs PROCESS

- Security management[57]
- Security evaluation and certification

EXTERNAL STAKEHOLDERS

- Suppliers
- Subcontractors
- Security Evaluators
- Certification body

[56] See Annex B [No. 59]
[57] See Annex A

2.2.6 Article 24.2.f

CONTENT

[A qualified trust service provider providing qualified trust services shall:]

f) 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;

GUIDELINE

This is a new provision compared to Directive 1999/93/EC where there was no explicit requirement to use "trustworthy systems" to store (personal) data.

This article expands article 24.2.e by additional aspects concerning personal data handling. Therefore it is recommended that all general requirements as per chapter 2.2.5 of this document are met whenever applicable, in particular:

- EN 319 401[58] – chapters 7.4 – 7.9,
- EN 319 411-1[59] – chapter 6.4.3; 6.4.6; 6.5.5; 6.5.7,
- EN 319 411-2[60] – chapter 6.4.3; 6.4.6; 6.5.5; 6.5.7,
- ISO/IEC 27002[61] – chapter 9.

It should be noted that personal data is part of sensitive information a QTSP acquires during standard operations. Personal data protection is mentioned in article 24.2.j.

Such data should be preserved for a specified period of time. This period should be determined on a GRC (Governance, Risk, Compliance) basis. It is recommended to implement data preservation for sensitive information according to ETSI TS 101 533-1.

ETSI TS 101 533 standard is based on TS 102 573, ISO/IEC 27001[62] and ISO/IEC 27002 standards.

TS102 573 provides requirements for trust service providers in respect to the storage of data for digital accounting. The purpose of this document is to provide a common, objective and reliable basis for preservation service providers to implement and manage secure Data Preservation Systems, meeting the information security related quality addressed by the EU Directive 2006/123/EC on personal data protection (replaced in 2016 by the EU General Regulation on Data Protection, 2016/679G). This covers organisational and legal aspects, as well as technical ones, like those related to use and maintenance of an electronic signature (for data preservation), storage access authorisation, authenticity and integrity.

[58] See Annex B [No. 27]
[59] See Annex B [No. 28]
[60] See Annex B [No. 29]
[61] See Annex B [No. 62]
[62] See Annex B [No. 61]

ISO/IEC 27002 provides clauses in relation to disposal handling and labelling of (storage) media, logging (of security events), user access management and network access control.

There is a difference between “storage of data” and “preservation”:

- (data) preservation service: service to which data objects are submitted to achieve specified preservation goals over the long-term which at least include proof of integrity and proof of existence and which can maintain the validity status of digital signatures.
- long-term: over technological changes such as crypto algorithms, key sizes or hash functions or of storage technology

LIST OF STANDARDS

- All standards mentioned within Article 24.2.e in scope of trustworthy systems.
- ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management"; (TSP-QC)
- ETSI TS 101 533-2: Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 2: Guidelines for Assessors[63]
- ISO/IEC 27001 "Information technology -- Security techniques -- Information security management systems - Requirements"
- ISO 27002 "Information technology -- Security techniques -- Code of practice for information security controls"
- ETSI TS 102 573: "Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data for digital accounting".

TSP PROCESS

- Security management[64]
- Compliance

EXTERNAL STAKEHOLDERS

- Subcontractors

[63] See Annex B [No. 40]
http://www.etsi.org/deliver/etsi_TR/101500_101599/10153302/01.02.01_60/tr_10153302v010201p.pdf
[64] See Annex A

2.2.7 Article 24.2.g

CONTENT

[A qualified trust service provider providing qualified trust services shall:]

g) take appropriate measures against forgery and theft of data;

GUIDELINE

This requirement is strongly related to the aspect of "trustworthiness" of a (TSP's) system and data protection, as per article 24.2 clauses e) and f). Therefore, it is recommended to follow standards and guidelines related to these articles.

In addition, it is necessary to highlight the importance of the ISO/IEC 27002[65] in this area, with respect to information security management.

Protection against forgery and theft of data has organizational and technical aspects. Requirements within the scope of a trustworthy system (part of technical aspect) are the same as in article 24.2.e and f. In the field of data preservation, requirements are the same as in the article 24.2.f.

Implementation of other remaining requirements should be preceded by risk analysis. QTSP should identify assets, vulnerabilities and countermeasures to minimalize the risk of forgery and theft. It is recommended that this analysis is part of the whole risk management process of a QTSP organisation.

It is recommended that QTSP use recommendations from standard ISO/IEC 27005[66] which is dedicated to information security.

The catalogue of countermeasures is available as standard ISO/IEC 27002 expanded by countermeasures derived from ETSI/CEN standards related to 24.2 clauses e) and f), in particular: ETSI EN 319 401[67] clauses 7.6 and 7.7, ETSI EN 319 411[68] and ETSI TS 101 533[69].

LIST OF STANDARDS

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (TSP-QC, TSP-TS)
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (TSP-QC)
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (TSP-QC)
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (TSP-TS)
- BRG CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (TSP-QC)

---

[65] See Annex B [No. 62]
[66] See Annex B [No. 63]
[67] See Annex B [No. 27]
[68] See Annex B [No. 28/29]
[69] See Annex B [No. 44]

- ETSI TS 119 312 (an update is in progress) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites (TSP-QC)
- ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management"; (TSP-QC)
- ETSI TS 101 533-2: Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 2: Guidelines for Assessors[70]
- ETSI TS 102 573: "Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data for digital accounting".
- CEN/TS 419 261:2015 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures (TSP-QC)
- CEN EN 419 221-1 Protection profiles for TSP Cryptographic modules – Part 1: Overview
- CEN EN 419 221-2 Protection profiles for TSP Cryptographic modules – Part 2: Protection profile for Cryptographic module for CSP signing operations with backup
- CEN EN 419 221-3 Protection profiles for TSP Cryptographic modules – Part 3: Protection profile for Cryptographic module for CSP key generation services
- CEN EN 419 221-4 Protection profiles for TSP Cryptographic modules – Part 4: Protection profile for Cryptographic module for CSP signing operations
- (draft) CEN EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services (not publicly available and not security evaluated yet)
- CEN EN 419 231, “Security requirements for trustworthy systems supporting time-stamping”
- CEN TS 419 241-1, “Trustworthy systems supporting server signing” Part 1: Security requirements (UNDER DRAFTING)
- (draft) CEN TS 419 241-2, “Trustworthy systems supporting server signing” Part 2:Protection Profile for QSCD for Server Signing (UNDER DRAFTING)
- Protection Profile ANSSI DCSSI-PP 2008/07
- ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls (TSP-QC, TSP-TS)
- ISO/IEC 20000-1:2011 Information technology -- Service management -- Part 1: Service management system requirements (TSP-QC, TSP-TS).
- ISO/IEC 15408 (parts 1 to 3): Information technology - Security techniques - Evaluation criteria for IT security
- ISO/IEC 19790:2006, Information technology - Security techniques - Security requirements for cryptographic modules[71]
- ISO/IEC 27001 "Information technology -- Security techniques -- Information security management systems - Requirements"
- ISO 27002 "Information technology -- Security techniques -- Code of practice for information security controls"
- ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management

TSP PROCESS

- Information Security Management[72]

[70] See Annex B [No. 40]
http://www.etsi.org/deliver/etsi_TR/101500_101599/10153302/01.02.01_60/tr_10153302v010201p.pdf
[71] See Annex B [No. 59]
[72]See Annex A

EXTERNAL STAKEHOLDERS

- Subscribers

2.2.8 Article 24.2.h

CONTENT

[A qualified trust service provider providing qualified trust services shall:]

h) 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;

GUIDELINE

Article 24.2.h should be read together with the Article 17 4.i:

[Supervisory body]

4. For the purposes of paragraph 3 and subject to the limitations provided therein, the tasks of the supervisory body shall include in particular:

(i) 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);

It is recommended to follow EN 319 401[73] chapter 7.10 generally for any kind of (qualified) trust service. These requirements can be met, for example, through the use of write-only media, a record of each removable media used and the use of off-site backup.

For a TSP issuing certificates for signature and seal, clauses 6.4.5 and 6.4.6 from EN 319 411-1[74] and -2[75] are additionally applicable. There are some more requirements for qualified certificates (than for non-qualified) in this respect (see EN 319 411- chapter 6.4.5).

Some additional provisions are also given by:

- EN 319 401 – clauses 7.7 e), 7.8 h) , 7.12,
- EN 319 411-1 – clauses 6.2.2.l), 6.3.4.d), e), f) and h), 6.3.8 a), 6.4.5.c), 6.4.9
- EN 319 411-2 clause 6.4.9 (fully refers to EN 319 411-1),

With regard to Publicly-Trusted Certificates, it is recommended to follow BRG CA/Browser Forum[76] base requirement document, chapters 5.4 and 5.5.

[73] See Annex B [No. 27]
[74] See Annex B [No. 28]
[75] See Annex B [No. 29]
[76] See Annex B [No. 7]

With regard to Extended Validation Certificates, it is recommended to follow EVCG CA/Browser Forum[77] chapter 15 and 17.

It is suggested to follow ETSI TS 101 533-1[78] for preserving records. They should be preserved for a specified period of time, which should be determined on a GRC (Governance, Risk, Compliance) basis.

Keeping and preservation of the records should also be part of a TSP termination procedure. Records should be transferred to a reliable party and this must be addressed in a TSP termination plan as per EN 419 401 chapter 7.12 item b) iii. For TSP issuing certificates, clause 6.4.9 of EN 319 411-1 should be applied additionally. See also provisions for article 24.2. h.

Recommendations contained herein are to protect the QTSP against various claims. Keeping records in conjunction with an internal audit programme is a countermeasure for various threats, i.e. forgery, theft, fraud. It may also help the trusting parties to prevent the discrepancy of trusted relation.

QTSP should record and keep accessible activity-related data - issued and received - even after cessation of a service. Partially the content of the records is mentioned in clauses 6.2.2 l, 6.3.4.e and f, 6.3.8.a, 6.4.5.c of ETSI EN 319 411-1.

Below are examples of records:

- records from the identification process,
- audit logs,
- records of evaluation of protections of CA, RA and Repository,
- certificates and subscribers data base,
- issued CRLs,
- paper and electronic correspondence between QTSP and subscribers and relying parties during the operation of certificates life cycle.

For QTSPs delivering qualified timestamping services, additional provisions are given by ETSI EN 319 421. For other QTSPs, additional requirements depending on the type of qualified service have to be defined.

LIST OF STANDARDS

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (TSP-QC, TSP-TS)
- ETSI EN 319 411-1Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (TSP-QC)
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (TSP-QC)
- ETSI TS 101 533-1 Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management (TSP-QC)
- BRG CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (TSP-QC)

[77] See Annex B [No. 56]
[78] See Annex B [No. 44]

- EVCG CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates" (TSP-QC)

TSP PROCESS

- Information Security Management[79]
- Business Continuity
- Compliance

EXTERNAL STAKEHOLDERS

- Subscribers
- Signatory
- Creator of a seal
- Relying Parties

[79] See Annex A

2.2.9 Article 24.2.i

CONTENT

[A qualified trust service provider providing qualified trust services shall:]

i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body;

GUIDELINE

It is recommended to follow:

- EN 319 401[80] – chapter 7.12,
- EN 319 411-1[81] – chapter 6.4.9 (for TSP issuing certificates additionally),
- EN 319 411-2[82] – chapter 6.4.9 (for TSP issuing qualified certificates additionally).

A termination plan is a document that 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 them up-to-date.

According to this requirement, the document should be verified by a supervisory body.

For QTSPs delivering qualified timestamping services, additional provisions are given by ETSI EN 319 421. For other QTSPs, additional requirements depending on the type of qualified service have to be defined.

LIST OF STANDARDS

- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (TSP-QC)
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (TSP-QC)
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (TSP-QC, TSP-TS)

TSP PROCESS

- Business continuity
- Compliance
- Conformity Assessment

EXTERNAL STAKEHOLDERS

- Supervisory body
- Subscribers

[80] See Annex B [No. 27]
[81] See Annex B [No. 28]
[82] See Annex B [No. 29]

2.2.10 Article 24.2.j

CONTENT

[A qualified trust service provider providing qualified trust services shall:]

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

GUIDELINE

Itis important to highlight that the Directive 95/46/EC is now obsolete. Member States law based on directive 95/46/EC is effective until May 2018. After this date QTSP should implement requirements of regulation (EU) 2016/679 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).

The requirement of this article is related to compliance management. It is recommended that a TSP follows EN 319 401[83] chapter 7.13 provisions generally. For TSPs issuing certificates, standard EN 319 411 does not bring additional provisions (see chapter 6.8.4 of EN 319 411-1[84] and -2[85]). However the mentioned standards do not contain detailed information on how to meet such requirement. Such (new) requirements resulting from the introduction of "privacy (data protection) by default" and "privacy (data protection) by design" rules will affect technical solutions. Especially systems related to trust services provided remotely (where user authentication or personal data processing occur, for instance server signature) will need to comply with these requirements.

The domain of data protection and privacy partially overlaps:

- security,
- confidentiality,
- anonymity,
- concepts of appropriate use,
- protection of information.

So generally provisions related to security presented in earlier chapters are also applicable here (refer to guidelines for Art. 24.2. b),e),f), g) and h)).

Based on the new General Data Protection Regulation, fundamental principles of privacy are:

- Purpose limitation
- Data minimisation
- Data security – appropriate technical protection against unauthorised access, alteration, destruction or disclosure
- Control of the individual over his personal data:
    - Right of access,
    - Right to rectification,
    - Right to request the deletion of personal data,
    - Right to be informed about the identity of the data controller, the purposes of the processing, etc.”

[83] See Annex B [No. 27]
[84] See Annex B [No. 28]
[85] See Annex B [No. 29]

- Lawfulness of data processing

The general technical rules for products and systems are “privacy by design” and “privacy by default”. Privacy by design means ensuring that privacy mechanisms are built in the products. Privacy by default means that by default only necessary personal data is processed. It is therefore recommended that a QTSP’s technical solutions (products and systems) for any services provided on-line to trust service subscribers, provide the following key features (whenever applicable):

- identification and authentication of parties,
- explicit user consent,
- selective disclosure and data minimisation,
- secure storage and transfer,
- user control,
- anonymity and pseudonymity.

In respect to trust services delivered on-line (for example server signature), user authentication concerns processing of only adequate identification data, relevant but not excessive to grant access to that service online.

There are various technologies available, which would help process personal data according to data protection rules. A set of privacy and data protection related standards/reports is under development by European Standard Organisations[86] as a part of mandate M/530[87]. These documents are meant to address privacy management in the design and development and in the production and service provision processes of security technologies, as well as provide practical guidelines for implementation. However, this is beyond the scope of this guideline. It is simply suggested that the reader familiarises himself with these standards (once published in the future) and assess the impact to the TSP activities and their related ICT systems.

In addition, it is worth mentioning, that a new version of EN 419 212 standard (related to smart cards / secure element based technology for signature and strong authentication) has been adopted, where its Part 4 provides a set of privacy-oriented protocols that could be used to build (privacy protecting) user authentication solutions.

LIST OF STANDARDS

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (TSP-QC, TSP-TS)
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (TSP-QC)

---

[86] CEN / CENELEC Joint Working Group 8 ‘Privacy management in products and services’

[87] See Annex B [No. 67]
http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548#
Commission Implementing Decision of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive95/46/EC of the European Parliament and of the Council and in support of Union’s security industrial policy

- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (TSP-QC)
- Standards delivered in the scope of mandate M/530

TSP PROCESS

- Certification Authority Operations[88]
- Information Security Management
- Compliance

EXTERNAL STAKEHOLDERS

- Subscribers
- Signatory
- Creator of a seal
- Suppliers, product and system vendors

[88] See Annex A

2.2.11 Article 24.2.k

CONTENT

[A qualified trust service provider providing qualified trust services shall:]

k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database;

GUIDELINE

It is recommended to follow:

- EN 319 411-1[89] – chapter 6.1,
- EN 319 411-2[90] – chapter 6.1 (fully relies on EN 319 411-1).

QTSP should maintain a certificate database. This database should be protected to ensure availability and integrity. It should be maintained on an operational basis, as part of the service delivery management. General requirements for systems and security from EN 319 401[91] and EN 319 411 are applicable. QTSP may decide to provide access to external stakeholders, and in that case should provide secure electronic communication channels to the database for external stakeholders.

For more information on service delivery management it is suggested to refer to ISO/IEC 20000[92].

LIST OF STANDARDS

- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (TSP-QC)
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (TSP-QC)
- ISO/IEC 20000-1:2011 Information technology -- Service management -- Part 1: Service management system requirements (TSP-QC)

TSP PROCES

- Certification Authority operations[93]
- Business Continuity

STAKEHOLDERS

- Subscribers
- Signatory
- Creator of a seal
- Relying parties

[89] See Annex B [No. 28]
[90] See Annex B [No. 29]
[91] See Annex B [No. 27]
[92] See Annex B [No. 60]
[93] See Annex A

2.3 Article 24.3 and 24.4

CONTENT

3. 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.]

4. 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.

GUIDELINE

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:

- ETSI EN 319 411-1[94] chapters 6.3.9 and 6.3.10,
- ETSI EN 319 411-2[95] chapters 6.3.9 and 6.3.10.

For Organizational Validation Certificates and Domain Validation Certificates clause 4.10.2 of BRG CA/Browser Forum applies additionally.

For Extender Validation Certificates clause 13 EVCG CA/Browser Forum[96] applies additionally.

For Publicly-Trusted Certificates, Clause 4.9 of the BRG CA/Browser Forum[97] applies additionally.

It is believed that EN 319 411-2 does not yet include sufficient provisions with regard to the CRL and OCSP profile and creation process in order to meet the requirements of these articles. ETSI is working on further requirements to be included in a revised version of EN 319 411-2 for the use of CRL and OCSP beyond the certificate validity period.

Generally, validity and 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 Practise Statement.

Two methods of providing validity and revocation status are the most popular: through a Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP). Use of OCSP is recommended.

In case both methods are supported by a TSP, the information provided by all services should be consistent over time, different delays in updating the status information for all these methods should be taken into account. An exception to this is when an OCSP responder can answer with status 'unknown' if the certificate has not been issued legitimately by the QTSP.

---

[94] See Annex B [No. 28]
[95] See Annex B [No. 29]
[96] See Annex B [No. 56]
[97] See Annex B [No. 7]

Availability of certificate revocation information is crucial. QTSP should assure practically continuous access to this information. Therefore, QTSP should identify assets, vulnerabilities and countermeasures to minimalize risk of loss of availability. It is recommended these aspects are included in a global risk management process, and ISO/IEC 27005[98] is suggested here.

For more information about availability of service assurance refer to ISO/IEC 20000-1:2011[99] clause 6.

LIST OF STANDARDS

- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (TSP-QC)
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (TSP-QC)
- BRG CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (TSP-QC)
- EVCG CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates" (TSP-QC)
- ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management
- ISO/IEC 20000-1:2011 Information technology — Security techniques — Information security management systems — Requirements

TSP PROCESS

- Information Security Management[100]
- Business Continuity

EXTERNAL STAKEHOLDERS

- Subscribers
- Signatory
- Creator of a seal
- Relying parties

[98] See Annex B [No. 63]
[99] See Annex B [No. 60]
[100] See Annex A

3. Qualified certificates for electronic signatures and for electronic seals

This chapter concerns specific requirements in relation to qualified certificates for electronic signatures and qualified electronic seals.

'Electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form (e.g. a document), and which is used by the signatory to sign, whereas 'electronic seal' is to ensure the origin and integrity of "other" electronic data (e.g. a document).

Qualified electronic signature (QES) is a particular kind of electronic signature. QES is an advanced electronic signature that meets requirements of eIDAS Regulation Art. 26. QES is created using a qualified electronic signature creation device (QSCD) and is based on a qualified certificate for electronic signature (QC). Requirements for QC are laid down in eIDAS Regulation Annex I and for QSCD in Annex II.

Qualified electronic seal (QESeal) is an advanced electronic seal that meets requirements laid down in eIDAS Regulation Art. 36 and created using a qualified electronic seal creation device. QESeal is based on a qualified certificate for electronic seals. Requirements for a qualified certificate for electronic seals are laid down in eIDAS Regulation Annex III. Requirements for a qualified electronic seal creation device are the same as for QSCD.

3.1 Articles 28.1, 2, 3 and 38.1, 2, 3

CONTENT

28.1. Qualified certificates for electronic signatures shall meet the requirements laid down in Annex I.

28.2. Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex I.

28.3. 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.

38.1. Qualified certificates for electronic seals shall meet the requirements laid down in Annex III.

38.2. Qualified certificates for electronic seals shall not be subject to any mandatory requirements exceeding the requirements laid down in Annex III.

38.3. 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.

GUIDELINE

Requirements set out by these articles apply to TSPs issuing qualified certificates for signatures (which are used by a signatory to sign, for instance a contract) and seals (which confirm origin and integrity of other data, for instance a document). These requirements concern the content of the certificates.

Annex I and III 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 and Annex III to be present, but other information can be added by a QTSP.

It is recommended to follow:

- ETSI EN 319 412-1[101] (general provisions),
- ETSI EN 319 412-2[102] (certificates for natural persons),
- ETSI EN 319 412-3[103] (certificates for legal persons),
- ETSI EN 319 412-5 (indication that a certificate is qualified)[104]
- ETSI EN 319 411-1[105] chapter 6.6.1,
- ETSI EN 319 411-2[106] chapter 6.6.1 (fully refers to ETSI EN 319 411-1),

All the certificate profiles specified in ETSI EN 319 412 series are based upon IETF RFC 5280[107] for generic profiling of Recommendation ITU-T X.509 | ISO/IEC 9594-8. The certificate profiles specify profiles for both EU Qualified and non-qualified certificates as relevant. Reference is made to ETSI EN 319 412-5[108] for requirements relating to "QCStatement". QTSP using ITU-T X.509 should ensure that corrigendum 1[109] and 2[110]are applied to base standard.

Implementing additional attributes should be developed according to the same rules. During development of additional fields in certificate structure TSP may use ETSI EN 319 412 -1 standard. 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.

Keeping a certificate profile adequate to regulations is part of the compliance management process.

LIST OF STANDARDS

- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;

---

[101] See Annex B [No. 30] http://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.01_60/en_31941201v010101p.pdf
[102] See Annex B [No. 31] http://www.etsi.org/deliver/etsi_en/319400_319499/31941202/02.01.01_60/en_31941202v020101p.pdf
[103] See Annex B [No. 32] ttp://www.etsi.org/deliver/etsi_en/319400_319499/31941203/01.01.01_60/en_31941203v010101p.pdf
[104] ETSI EN 329 412-5 renders mandatory the presence in the QcStatements a link to the PKI disclosure statements, which is not required by eIDAS.
[105] See Annex B [No. 28]
[106] See Annex B [No. 29]
[107] See Annex B [No. 73] https://www.ietf.org/rfc/rfc5280.txt
[108] See Annex B [No. 34] http://www.etsi.org/deliver/etsi_en/319400_319499/31941205/02.01.01_60/en_31941205v020101p.pdf
[109] See Annex B [No. 65] https://www.itu.int/rec/T-REC-X.509-201505-S!Cor1/en
[110] See Annex B [No. 66] https://www.itu.int/rec/T-REC-X.509-201604-S!Cor2/en

- ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons;
- ETSI EN 319 412-5 V2.1.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (TSP-QC)
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (TSP-QC)
- IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- Recommendation ITU-T X.509;
- Recommendation X.509 (2012) Corrigendum 1 (05/15);
- Recommendation X.509 (2012) Corrigendum 2 (04/16)

TSP PROCESS

- Compliance management[111]
- Change management

EXTERNAL STAKEHOLDERS

- Supervisory Bodies
- Relying Party
- Signatory (for Signatures)
- Creator of a Seal (for Seals)

3.2 Article 28.4 and 38.4

CONTENT

28.4. 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.

38.4. If a qualified certificate for an electronic seal 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.

GUIDELINE

With regard to certificate revocation generally, it is recommended to follow:

- EN 319 411-1[112] – chapter 6.3.9 (for all certificates),
- EN 319 411-2[113] – chapter 6.3.9 (for qualified certificates; fully refers to EN 319 411-1).

For Organizational Validation Certificates and Domain Validation Certificates, a TSP should keep its certificate status information, clause 4.10.2 of BRG CA/Browser Forum[114]should apply.

[111]See Annex A
[112] See Annex B [No. 28]
[113] See Annex B [No. 29]
[114] See Annex B [No. 7]

For Extended Validation Certificates, TSP should comply with EVCG CA/Browser Forum[115], clause 13.

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 choose an appropriate technology which prevents reinstating revoked certificates.

Before a TSP issues a certificate, some obligation 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.

The TSP should revoke certificates in a timely manner based on authorized and validated certificate revocation requests mentioned in EN 319 411-1 and -2, chapter 6.2.4.

LIST OF STANDARDS

- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- BRG CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (TSP-QC)
- EVCG CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates" (TSP-QC)

TSP PROCESS

- Revocation management
- Risk management

EXTERNAL STAKEHOLDERS

- Relying Parties
- Signatory
- Creator of a Seal

[115] See Annex B [No. 56]

3.3 Article 28.5 and 38.5

CONTENT

28.5. 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.

38. 5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of qualified certificates for electronic seals:

(a) if a qualified certificate for electronic seal 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.

GUIDELINE

Requirement applies only to a TSP issuing qualified certificates.

Since certificate suspension is subject to national regulation, it may vary between Member States. A TSP should perform a compliance management process to ensure compliance to local regulation of the Member state in which it is granted the qualified status.

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

- EN 319411-1[116] chapters 6.2.4, 6.3.9 and 6.3.10,
- EN 319411-2[117] chapters 6.2.4, 6.3.9 and 6.3.10.

Generally, it is recommended to meet requirements and apply standards as defined for certificate revocation and validity status in reference to articles 24.3 and 24.4 (refer to this document).

If Certificate Revocation Lists are used, they should be as defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 or IETF RFC 5280[118].

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

LIST OF STANDARDS

- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;

[116] See Annex B [No. 28]
[117] See Annex B [No. 29]
[118] See Annex B [No. 73]

- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;
- BRG CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (TSP-QC)[119]
- EVCG CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates" (TSP-QC)[120]
- ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management[121]
- ISO/IEC 20000-1: 2014 Information technology — Security techniques — Information security management systems — Requirements[122]

TSP PROCESS

- Compliance management[123]
- Certificate Status Management

EXTERNAL STAKEHOLDERS

- Supervisory Body
- Relying Parties
- Signatory

[119] See Annex B [No. 7]
[120] See Annex B [No. 56]
[121] See Annex B [No. 63]
[122] See Annex B [No. 60]
[123] See Annex A

4. Requirements for the validation of qualified electronic signatures

This chapter concerns requirements for TSPs providing validation service of qualified electronic signatures.

Validation of qualified electronic signature is the process of verifying and confirming that a qualified electronic signature is valid. Requirements for validation service of qualified electronic signature are laid down in article 32 of eIDAS Regulation.

Validity of the signature is essential for electronic transactions and allows any relying party to trust signed data and documents. Validation service provided to the relying parties shall be secure and based on standards.

4.1 Article 32.1

CONTENT

1. 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.

GUIDELINE

According to eIDAS Regulation validation means the process of verifying and confirming that an electronic signature or a seal is valid. Validation process of a qualified electronic signatures is not yet specified by published standards. Recommendations bellow are based on draft version of ETSI TS 119 172-4[124]. An important part in guidance for a qualified validation services is ETSI EN319 102-1[125] clause 5 which contains basic requirements and rules for an electronic signature validation. It is important to note that

[124] See Annex B [No. 53]
[125] See Annex B [No. 18]
http://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf

indeterminate results exceeding requirements of the Regulation do not have to be part of a verification report.

All requirements laid down in the regulation for qualified validation of qualified electronic signatures are explained below respectively to each requirement “a” to “h”.

4.1.1 Article 32.1.a, b and f

The certificate validity status of the certificates must be verified during the certificate path validation process (ETSI EN 319 102-1 and IETF RFC 5280), for all certificate types (e.g. certificates issued to signer, to CAs, to OCSP responders, to CRL Issuers, to Time-Stamping Units) and either OCSP or CRL checks must be carried out.

According to the European Commission Implementing Decision (CID) (EU) 2015/1505[126], Trusted Lists are the single formal way to verify that a claimed qualified trust service is indeed granted a qualified status. The validation procedure must verify that the qualified certificate was issued by a qualified trust service provider by verifying its status on a Trusted List. Moreover, compliance with Annex A.1 ETSI 319 412-5[127] should be assessed.

4.1.2 Article 32.1.c, d and e

This information should be provided as part of the validation report in the validation process:

- All supported (in Certification Policy) formats (XAdES, CAdES, PAdES, ASiC), which are mentioned in EU 2015/1505 should be correctly validated.
- A signing certificate should be included in a validation report
- Since indication of the use of a pseudonym is included in the Subject field of the certificate, it has to appear also in the validation report

More details can be found in ETSI TS 319 102, clause 5.1.3[128] - Status indication of the signature validation process and signature validation report in table 5 and 6.

4.1.3 Article 32.1.g and h

The integrity of the signed data is checked by performing cryptographic verifications and guaranteed by a supported signature validation model which depends on the TSP. Validation service procedures for establishing whether an electronic signature or electronic seal is technically valid should rely on the process described in ETSI TS 319 102, especially clause 5.1.3 where one can find a description of a validation signature model, basic building blocks that are useable in the signature validation process for

[126] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D1505&from=en
[127] See Annex B [No. 34]
http://www.etsi.org/deliver/etsi_en/319400_319499/31941205/02.01.01_60/en_31941205v020101p.pdf
[128] Status indication of the signature validation process and signature validation report in table 5 and 6, page 30

basic signatures, for time-stamps and for signatures with time and signatures with long-term or archival validation data.

LIST OF STANDARDS

- Draft ETSI TS 119 172-4 Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists;
- ETSI EN 319 102-1 v.1.1.1Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

TSPs PROCESS

- Validation process[129]

EXTERNAL STAKEHOLDERS

- Relying Parties – if validation response is reliable and efficient Relying Party trusts the response and can base its various business activities on it.

[129]See Annex A

4.2 Article 32.2

CONTENT

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

GUIDELINE

A system used for validation of qualified signatures should be reliable and consist of technically evaluated security products protected against unauthorized modifications.

To provide the correct result of the signature validation process to the relying party, the validation report should be done by a validation service in the correct format – for example when a human user is involved, the report is presented in a way meaningful to the user – human readable form (PDF).

Elements, mentioned below, should be presented in a legible way to the verifier:

a) The text or a similar indication of the scope of the validation executed on the validated signature: According to draft version of ETSI TS 119 172-4[130] it could be for example:
Signature validation policy for European qualified electronic signatures/seals using trusted lists
Validation of digital signature to identify whether it can be considered as a European qualified electronic signature/seal using EUMS trusted lists in the sense of the applicable European legislation at the time of signing, i.e. either Directive 1999/93/EC or Regulation (EU) No 910/2014;
b) the complete set of data representing the signer in its certificate,
c) the use of any pseudonym is clearly indicated if a pseudonym was used at the time of signing;
d) the time reference against which the results of the signature validation procedure are provided (i.e. "time of signing")
    a. If a valid qualified timestamp is present, then the time reference can be taken from this timestamp;
    b. If no timestamp is present, then the time reference is the time of the validation;
    c. If a non-qualified timestamp is present, then the QTSP must define in its validation policy what is the time reference in this case.
e) the presentation of the data that has been covered by the signature (signed data),
f) any signature attributes that have been included in the signature (signed and not signed attributes),
g) the overall status of the signature validation according to ETSI EN 319 102-1[131] . Information related to cryptographic suites used to generate the signature being validated and potential security related issues against either national rules or ETSI TS 119 312[132],
h) the detailed outcome of each validation step.

Additionally, for better understanding ETSI TS 119 101 V1.1.1 should be followed, in particular:

- main validation functionalities (as specified in clause 8.2.2);
- validation process rules enforcement (as specified in clause 8.2.3);
- validation policy (as specified in clause 8.2.4);

[130] See Annex B [No. 53]
[131] See Annex B [No. 18]
[132] See Annex B [No. 54]
http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v010101p.pdf

- validation user interface (as specified in clause 8.2.5); and
- validation input/output relative conformance (correctness of the implemented validation procedure) (as specified in clause 8.2.6).

LIST OF STANDARDS

- Draft ETSI TS 119 172-4 Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists;
- ETSI EN 319 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- ETSI TS 119 101 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation

TSPs PROCESS

- Validation process[133]

EXTERNAL STAKEHOLDERS

- Relying Parties – if validation response is reliable and efficient, a Relying Party can trust the response and can base its various business activities on it.

[133] See Annex A

5. Qualified validation service for qualified electronic signatures

This chapter concerns requirements for TSPs providing qualified validation service for qualified electronic signatures. Requirements for TSP's providing validation are covered in the previous chapter. Here special requirements convenient for qualified validation service for qualified electronic signatures are listed.

5.1 Article 33

CONTENT

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.

GUIDELINE

There are several options and possibilities for QTSPs to provide validation services. The selection of these options is driven by a specific policy of the QTSP. Additionally, legal requirements can be provided through specific policies, e.g. in the context of qualified electronic signatures as defined in the eIDAS Regulation.

Besides there are some additional requirements mentioned below:

- Art.33.1(a) with regard to the validation process to be provided in compliance with Art.32.1. (aligned(a) to (h)).
- Art.33.1(b) for the provision of the validation result in an automated manner that needs:
    - to provide to the relying party the correct result of the validation process and should allow the relying party to detect any security relevant issues (in conjunction of Art.32.2);
    - to be reliable and efficient; and
    - to bear the advanced electronic signature or advanced electronic seal of the QTSP providing the qualified validation service.

All these elements are part of audit activities under the compliance management process.

To assure that the result of the validation process is reliable and efficient, it should be taken into consideration to build and deploy a redundant system designed and maintained on actual requirements concerning the availability of validation service. Requirements for redundancy should be derived from actual regulations, incident reviews and identified risks. Besides that, the QTSP should provide a comprehensive report of validation with all details obtained during the validation process for instance:

- status indicator of the results of validation process;
- indicator of the policy against which signature/seal has been validated;
- time and date for which the validation status and validation data was determined or;
- status of validation process

Additionally, to assure that response is reliable, QTSP should sign or seal responses with a valid advanced electronic signature or seal. Guidance for authorized responses can be found in clause 4.2.2.2 of the RFC 6960[134]. Response should be signed or sealed with keys listed on the European Union Member State trusted list, or issued by a Certification Authority listed on the European Union Member State trusted list.

LIST OF STANDARDS

- RFC 6960 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP
- ETSI EN 319 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation[135]

TSPs PROCESS

- Validation process[136]
- Compliance management
- Risk management
- Incident management
- Change management

EXTERNAL STAKEHOLDERS

- Relying Parties – if validation response is automatic, reliable and efficient allowed Relying Party can trust the response and can base its various business activities on it.

[134] See Annex B [No. 74]
[135] See Annex B [No. 18]
[136] See Annex A

6. Qualified preservation service for qualified electronic signatures and seals

This chapter concerns requirements for TSPs providing qualified preservation service for qualified electronic signatures and TSPs providing qualified preservation service for qualified electronic seals. Requirements for qualified preservation service for qualified electronic signatures is laid down in Article 34 of eIDAS Regulation. Requirements for a qualified preservation service for qualified electronic seals are laid down in Article 40 of eIDAS Regulation.

The purpose of a preservation trust service is to ensure the legal validity of electronic signatures and electronic seals over extended periods of time and guarantee that they can be validated irrespective of future technological changes.

6.1 Articles 34 and 40

CONTENT

[Article 34]

1. 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.

[Article 40]

Article[s 32, 33 and] 34 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals.

GUIDELINE

Requirements for QTSPs providing preservation services for qualified signature (and seals) are these applicable to all TSPs/QTSPs, amended with the requirements laid down in the art. 34.

According to European Commission "Questions & Answers on Trust Services under eIDAS"[137], *the eIDAS Regulation sets rules for the preservation of eSignatures, eSeals or certificates related to trust services. Preservation is different from electronic archiving (which is not a trust service under eIDAS). The objectives and targets of the process will make a distinction between the two activities:*

- *preservation under eIDAS aims at guaranteeing the trustworthiness of a qualified electronic signature or qualified electronic seal through time. The technology underpinning such trust service therefore targets the electronic signature or seal;*
- *Electronic archiving aims at ensuring that a document is stored in order to guarantee its integrity (and other legal features). The technology underpinning electronic archiving therefore targets the document. Electronic archiving remains the competence of Member States.*

[137] https://ec.europa.eu/digital-single-market/en/news/questions-answers-trust-services-under-eidas

Whilst document integrity is not part of the legal requirements of the regulation some technologies covered in the regulation, such as time-stamping, are applicable to the preservation of the integrity of archived document as for preservation of electronic signatures. ETSI is working on the development of standards in this area.

It is recommended that QTSP use technologies and procedures to create a Long Time Validation form of a AdES signature[138]. The archive form of the signature should be prepared according to an appropriate ETSI standard listed below (XAdES, CAdES, PAdES), respectively to chosen format of the signature. Systems and polices should be prepared accordingly to respective standards listed below.

Whilst XAdES, CAdES, PAdES have a role to play in signature preservation, it is important to note the ongoing standardisation in ETSI relating to signature and document preservation and use of standards such as defined in RFC 4998, TS 101 533 as well upcoming standards in this area.

LIST OF STANDARDS

- ETSI EN 319 132-1 Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures[139];
- ETSI EN 319 132-2 Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures[140];
- ETSI EN 319 122-1 Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures[141];
- ETSI EN 319 122-2 Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures[142];
- ETSI EN 319 142-1 Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures[143];
- ETSI TS 119 142-2 Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles[144];
- ETSI TS 101 533 Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management[145]

---

[138] The electronic archiving method, as long as the signature/seal is validated before archiving, and provided that all necessary metadata (e.g. the validation report) are archived with the signature/seal, can also be a reasonable option. For high volumes of electronic signatures/seal, the creation and maintenance of Long Time Validation form can prove quite costly

[139] See Annex B [No. 21]
http://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.01.01_60/en_31913201v010101p.pdf

[140] See Annex B [No. 22]
http://www.etsi.org/deliver/etsi_en/319100_319199/31913202/01.01.01_60/en_31913202v010101p.pdf

[141] See Annex B [No. 19]
http://www.etsi.org/deliver/etsi_en/319100_319199/31912201/01.01.01_60/en_31912201v010101p.pdf

[142] See Annex B [No. 20]
http://www.etsi.org/deliver/etsi_en/319100_319199/31912202/01.01.01_60/en_31912202v010101p.pdf

[143] See Annex B [No. 23]
http://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.01.01_60/en_31914201v010101p.pdf

[144] See Annex B [No. 24]
http://www.etsi.org/deliver/etsi_ts/119100_119199/11914202/01.00.01_60/ts_11914202v010001p.pdf

[145] See Annex B [No. 44]
http://www.etsi.org/deliver/etsi_ts/101500_101599/10153301/01.03.01_60/ts_10153301v010301p.pdf

- ETSI TS 101 533 Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors[146]
- RFC 4998 – Evidence Record Syntax (ERS)

TSPs PROCESS

- Compliance management[147]
- Digital data preservation

EXTERNAL STAKEHOLDERS

- Subscribers
- Relaying parties

[146] See Annex B [No. 40]
http://www.etsi.org/deliver/etsi_TR/101500_101599/10153302/01.02.01_60/tr_10153302v010201p.pdf
[147] See Annex A

7. Requirements for the qualified electronic time stamp

This chapter concerns requirements for TSPs issuing qualified electronic time stamps.

The purpose of an electronic time stamp is to provide evidence of data existing at a particular point in time. A time stamp binds the stamped data to a particular time and protects its integrity. Time stamps are issued by a time stamping trust service provided by TSP.

A Qualified electronic time stamp is a time stamp issued by qualified trust service provider and meets requirements laid down in eIDAS Regulation Article 42. A Qualified time stamp enjoys legal presumption of the accuracy of the date, the time and presumption of the integrity of stamped data from the time of stamping.

7.1 Article 42

CONTENT

1. 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.

GUIDELINE

There are a few basic standards defining requirements for binding of date and time and for accurate time sources:

- ETSI EN 319 421[148]- Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps
- ETSI EN 319 422[149]- Time-stamping protocol and electronic time-stamp profiles
- CEN EN 419 231[150] - Protection profile for trustworthy systems supporting time stamping

To fulfil all requirements, it is necessary to consider general TSP standards:

- ETSI EN 319 401[151] - General Policy Requirements for Trust Service Providers
- ETSI TS 119 312[152] - Cryptographic Suites

[148] See Annex B [No. 35]
[149] See Annex B [No. 39]
http://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf
[150] See Annex B [No. 9]
[151] See Annex B [No. 27]
[152] See Annex B [No. 54]
http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v010101p.pdf

A Qualified Trust Service Provider providing qualified time-stamping service (QTSA) has responsibility for the provision of the time-stamping services and time stamping management. The QTSA has responsibility for the operation of one or more units which creates and signs on behalf of the QTSA. These units should be trustworthy using:

a) requirements for trustworthy systems EN 319 401 clauses clause 7.4 items a) and f), 7.5, 7.6, 7.7 and 7.8 and EN 319 421 clause 7.6.2 and 7.6.3, or
b) commonly recognised or standardized Protection Profile conforming to ISO/IEC 15408, such as in CEN TS 419 231

ANSSI DCSSI-PP 2008/07 is currently the only Common Criteria evaluated protection profile for a timestamping system, but CEN EN 419 231 is planned to supersede it when it is published.

A QTSA is a trust service provider as described in ETSI EN 319 401 which issues time stamps and fulfils all obligations of Qualified Trust Service Provider laid down in the eIDAS Regulation.

The QTSA should establish and make available to subscribers and relying parties the time stamp policy and include the identifier for the policy in each issued time stamp. The following requirements should be fulfilled:

a) The QTSA should maintain and protect all time signing systems in a secure zone.
b) The QTSA should configure all time signing systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the QTSA's operations.
c) Only trusted parties should access secure zones and high security zones.

According to ETSI EN 319 421 the policy should specify:

a) at least one hashing algorithm used to represent the datum being time-stamped;
b) the accuracy of the time in the time-stamps with respect to UTC;
c) any limitations on the use of the time-stamping service;
d) the subscriber's obligations, if any;
e) the relying party's obligations;
f) information on how to verify the time-stamp such that the relying party is considered to "reasonably rely" on the time-stamp and any possible limitations on the validity period; and
g) any claim to meet the requirements on time-stamping services under national law.

To fulfil obligations laid down in eIDAS Regulation 42 (1.a) some obligations to the relying party are needed. Basing on ETSI EN 319 421 these obligations are:

a) verify that the time-stamp has been correctly signed and that the private key used to sign the time-stamp has not been compromised up to the time of the verification;
b) take into account any limitations on the usage of the time-stamp indicated by the time-stamp policy; and
c) take into account any other precautions prescribed in agreements or elsewhere.

According to ETSI EN 319 421 QTSA operates units creating Time Stamps, the following requirements apply:

a) The generation of signing key(s) should be undertaken in a physically secured environment by personnel in trusted roles under, at least, dual control. The personnel authorized to carry out this function should be limited to those required to do so under the QTSA's practices.

b) The generation of signing key(s) should be carried out within a secure cryptographic device which is a trustworthy system which:
   - is assured to EAL 4 or higher in accordance with ISO/IEC 15408[153], or equivalent national or internationally recognized evaluation criteria for IT security. If standard specifying common criteria protection profiles CEN TS 419 221-2,3,4,5 is published, this protection profile should be used as an evaluation criteria
   - alternatively, meets the requirements identified in ISO/IEC 19790[154] or FIPS PUB 140-2[155], level 3.

c) The key generation algorithm, the resulting signing key length and signature algorithm used for signing time-stamps key should be as specified in ETSI TS 119 312.
d) A signing key should not be imported into different cryptographic modules.
e) If there are same keys in different cryptographic modules, they should be associated with the same public key certificate into all the different cryptographic modules.
f) One time signing unit should have a single time-stamp signing key active at a time.

The time signing unit private keys should remain confidential and their integrity should be maintained. The private signing key should be held and used within a cryptographic module which compels the same evaluation criteria as unit used for the generation of signing keys. CEN EN 419 231 may establish additional requirements for private key protection.

Time-stamps should conform to the time-stamp profile as defined in ETSI EN 319 422.

The time-stamps should be issued securely and should include the correct time. Detailed requirements for time-stamp issuance are defined in ETSI EN 319 421 chapter 7.7.1.

QTSA is responsible for logging all events identified in ETSI EN 319 401. In addition, the following records should be logged:

a) Records concerning all events relating to the life-cycle of time signing keys.
b) Records concerning all events relating to the life-cycle of time stamp certificates.
c) Records concerning all events relating to synchronization of a time signing system clock to UTC (concerning normal re-calibration or synchronization of clocks used in time-stamping).
d) Records concerning all events relating to detection of loss of synchronization.

For all QTSA Qualified Time Stamps, signature verification (public) key certificate should be issued by a certification authority fulfilling general requirementsof QTSPs. The relying party is expected to use a Trusted List to establish whether the time-stamp unit and the timestamp are qualified. If the public key of the time stamping service is listed in the Trusted List and the service it represents is a qualified time-stamping service, or Certification Authority is listed in the Trusted List, representing a qualified time-stamping service then the time-stamps issued by this TSU can be considered as qualified.

---

[153]See Annex B [No. 58]
[154]See Annex {No. 59]
ISO/IEC 19790:2012 the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems, defines four security levels for cryptographic modules.
[155]FIPS PUB 140-2is a National Institute of Standards and Technology standard, and it specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information, it also defines four security levels for cryptographic modules.

The QC Statement "esi4-qtstStatement-1" as defined in ETSI EN 319 422, can be used as an indication that the TSP claims the time-stamp to be a qualified electronic time-stamp.

According to ETSI EN 319 422, some requirements to Time Stamp Profile and Protocol should be placed:

a) A time-stamping server should support the time-stamping request and response as defined in IETF RFC 3161[156], clause 2.4.1 and 2.4.2 with the amendments defined in the following clauses.
b) Hash algorithms for the time-stamp data to be supported should be as specified in clause A.8 of ETSI TS 119 312
c) Certificate used for the time stamp verification should meet the requirements defined in ETSI EN 319 412-2[157] for the QTSA being a natural person or defined in ETSI EN 319 412-3[158] for the QTSA being a legal person with the amendments defined in the following clauses.

Trust Service Providers have certain responsibilities with regard to the algorithms they are using. Although any transition between algorithms is predominantly the work to be done by supervisory body, the following approach should be taken by TSPs:

- TSP shall actively seek cooperation with their users (especially public administration) with regard to transition between algorithms. Sufficient advice and timely warning shall be offered to all, not only customers but also relying parties.
- TSP shall encourage the specification, spread of knowledge and implementation of appropriate procedures.
- TSP shall plan ahead conservation solutions and updates in SCVA due to the changes of cryptographic suites, algorithm breaks or other vulnerabilities.
- TSP shall adapt in advance their own libraries and SCVA offered in their products. If TSP is not a developer than at least contact and incitement for changes is necessary. As much as possible they should assist also 3rd party developers helping them to prepare for change of algorithms in signatures and certificates.
- Change of algorithms should not economically hamper subscribers of trusted services. TSP shall handle change of algorithms without requesting customer to pay for new cards or certificates.
- In case of possible break of algorithms TSP shall inform publicly in plain language (not cryptographic slang) what and how to do to preserve electronically signed/sealed documents, avoid exploit and attacks etc.
- Exploiting economically cryptography techniques in your products requires responsibility for all users. TSP are responsible for development of knowledge on relying party systems and what resources may be affected with cryptographic changes.

LIST OF STANDARDS

- ETSI EN 319 421 – Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (QTSP-TS)

---

[156] See Annex B [No. 70] https://www.ietf.org/rfc/rfc3161.txt
[157] See Annex B [No. 31]
http://www.etsi.org/deliver/etsi_en/319400_319499/31941202/02.01.01_60/en_31941202v020101p.pdf
[158] See Annex B [No. 32]
http://www.etsi.org/deliver/etsi_en/319400_319499/31941203/01.01.01_60/en_31941203v010101p.pdf

- ETSI EN 319 422 – Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles (QTSP-TS)
- ETSI EN 319 412 – Electronic Signatures and Infrastructures (ESI);. Certificate Profiles;. Part 2: Certificate profile for certificates issued to natural persons
- CEN EN 419 231 - Protection profile for trustworthy systems supporting time stamping
- CEN EN 419 221-2[159] - Protection profiles for TSP Cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup
- CEN EN 419 221-3[160] - Protection profiles for TSP Cryptographic modules - Part 3: Cryptographic module for Cryptographic module for CSP key generation services
- CEN EN 419 221-4[161] - Protection profiles for TSP Cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup
- CEN EN 419 221-5 - Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic module for trust services
- IETF RFC 3161 (2001) - Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)
- IETF RFC 5816 - ESSCertIDV2 update to RFC 3161
- ETSI EN 319 401 - General Policy Requirements for Trust Service Providers
- ETSI TS 119 312 - Cryptographic Suites
- ANSSI DCSSI-PP 2008/07

TSPs PROCESS

- Compliance management[162]
- Time-stamping provision
- Time-stamping management

EXTERNAL STAKEHOLDERS

- Subscribers
- Relaying parties

[159] See Annex B [No. 14]
[160] See Annex B [No. 15]
[161] See Annex B [No. 16]
[162] See Annex A

8. Requirements for qualified electronic registered delivery services

This chapter concerns requirements for qualified electronic registered delivery services laid down in Article 44 of the eIDAS Regulation.

Qualified electronic registered delivery service (QERDS) is a service provided by a qualified trust service provider (QTSP). QERDS securely transmits documents and data between third parties by electronic means. QERDS may use other QERDS services to transfer data from the sender to addressee. QERDS provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data. QERDS protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations. QERDS identifies both sender and addressee of the data.

8.1 Article 44

CONTENT

1. 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.

GUIDELINE

All expected standards regarding qualified electronic registered delivery services have not yet been completed nor published. There are more gaps in this area than answers laid down in standards. ETSI ESI has started work on the development of standards for supporting qualified and non qualified electronic registered delivery services as defined in the eIDAS (they will be the ETSI EN 319 522, ETSI EN 319 532, ETSI EN 319 521, and ETSI EN 319 531, see the list of standards at the end of this clause and Annex B for further details). This effort also targets at supporting conformance and interoperability tests (ETSI TS 119 524 and ETSI TS 119 534).

This guideline in some parts is based on trust application building experience and should be reviewed and updated after the publication of such relevant standards. Some security recommendations provided below for qualified registered electronic delivery service are based on standards developed for business data

exchange. These standards are the ETSI TS 102 640REM[163], OASIS AS4 Profile of ebMS 3.0 Version 1.0[164] and OASIS ebXML Messaging Services Version 3.0[165].

Art. 44 of the eIDAS Regulation requires the following on qualified electronic registered delivery services:

a) they are provided by one or more qualified trust service provider(s);

This point is not addressed in the standards. ETSI TS 102 640REM is not applicable in the context of eIDAS Article 44.

The boundaries of qualified electronic registered delivery service are established by a network of qualified trust service providers. QTSP should manage these relationships, and confirm that all "qualified electronic delivery network" is based on qualified trust service providers. Recognition of qualified trust service providers shall be based on Trust Lists.

Aspects covered in this chapter are part of the Service Level Agreement between trust service providers and business continuity management.

According to ETSI TS 102 640[166], some other (not qualified nor trusted) services can be involved in a qualified electronic delivery process, for example:

- notification of incoming delivery can be forwardFencryed via SMS/GSM network,
- documents can be forwarded by a non-qualified service after delivery confirmation,
- documents from non-qualified services origin delivered via a qualified electronic registered delivery service.

In the event of the data being transferred between two or more qualified trust service providers, the requirement in points (a) to (f) should apply to all the qualified trust service providers.

b) they ensure with a high level of confidence the identification of the sender;

Regarding the ETSI/CEN TS 102 640 standard, the choice of the authentication mechanism is left to the trust service provider. Specific requirements must hence be specified in standards to reflect those in the eIDAS Regulation.

---

[163]REM Registered Electronic Mail – standard based on e-mail protocols for Registered Electronic Delivery established by e-Sens (https://www.esens.eu) project.
[164] See Annex B [No. 69]
http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html
[165] See Annex B [No. 68]
https://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/cs02/ebms_core-3.0-spec-cs-02.html
[166]See Annex B [No. 46-50]
http://www.etsi.org/deliver/etsi_ts/102600_102699/10264001/02.01.01_60/ts_10264001v020101p.pdf
http://www.etsi.org/deliver/etsi_ts/102600_102699/10264002/02.01.01_60/ts_10264002v020101p.pdf
http://www.etsi.org/deliver/etsi_ts/102600_102699/10264003/02.01.01_60/ts_10264003v020101p.pdf
http://www.etsi.org/deliver/etsi_ts/102600_102699/10264004/02.01.01_60/ts_10264004v020101p.pdf
http://www.etsi.org/deliver/etsi_ts/102600_102699/10264005/02.01.01_60/ts_10264005v020101p.pdf

The Regulation defined Electronic Identification and Electronic Identification means, as part of the notified European network allowing common recognition of personal identification. The Regulation also defined levels of assurance of Electronic Identification means. If a qualified electronic registered delivery service uses an external electronic identification scheme/service for the identification of the sender this external system shall guarantee a high level of confidence of electronic identification. Identification scheme/service should be notified[167] or recognised on national level.

The identification of the sender should meet the requirements according to Art. 24.1. The authentication of a previously identified sender shall meet the requirements with regard to the authentication mechanisms for assurance level substantial.

Identification of the sender may be based on an advanced electronic signature of the sender. There are a few options available to achieve such a high level of confidence:

- a qualified electronic signature based on a qualified certificate of the sender;
- an advanced electronic signature based on a qualified certificate of the sender;
- an advance electronic signature based on an issued non-qualified certificate.

If an advanced electronic signature meets points 1 or 2, it may be assumed that the required high level of confidence of the identification of the sender is fulfilled. If an advanced electronic signature (point 3) is based on another certificate then qualified, additional risk evaluation should be performed and the qualified trust service policy should specify how such a requirement of a high level of confidence of the identification can be fulfilled.

Identification of the sender can also be done by another non-electronic way, for example in person. The procedure for verification of identity should be described in the policy and meet the high level of confidence requirement.

c) they ensure the identification of the addressee before the delivery of the data;

If qualified electronic delivery services are based on ETSI EN 319 532 under development (that evolve ETSI TS 102 640 REM specifications to fit within the framework of standards for supporting eIDAS), identification of the recipient is part of the REM protocolThe Regulation requires identification of the addressee and grants presumption of the identified addressee. For consistence with other trust services, it is recommended that the identification of the addressee meets the requirements according to Art. 24.1. The identification and subsequent authentications of the sender should at least meet the requirements of level “substantial” according to Commission Implementing Regulation (EU) 2015/1502. The authentication of a previously identified addressee shall meet the requirements with regard to the authentication mechanisms for assurance level “substantial”.A Qualified Trusted Service provider should establish and disseminate a trust service policy revealing how proof of receiving the data is confirmed. Some systems can be based on a verification of delivery receipt and verification of an electronic signature or an electronic seal of the recipient. It is a good practice to rely on qualified certificates verified through Trusted Lists, but also Qualified Trust Service provider can establish alternative trust points based on risk analysis and acceptance.

[167] eIDAS Article 9

It is important to mention that delivery of the data can be available to the recipient only after his proper identification. If this process is based on an advanced electronic signature, the signature verification should precede the delivery (availability) of the sent data.

If identification of the recipient is based on the identification process, it is highly recommended to conduct the whole process in a secured and controlled environment of the qualified trust service provider. All evidence of identification and delivery process should be gathered and protected.

Regarding eIDAS Regulation article 3 (36) electronic registered delivery service provides the proof of sending the data and protects transmitted data against the risk of loss, theft, damage and any unauthorized alternations. Identification and authentication of the recipient is part of countersigns against loss and theft of the delivered data. It is good practice to use end-to-end encryption from the sender to the recipient to ensure confidentiality of the message payload so that only the intended recipient can access it.

Evidence of identification process should be collected and secured for the appropriate time. This time should be established and described in the service policy.

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;

The QTSA is responsible for the operation of one or more units which creates and signs/seals on behalf of the QTSA the delivered data. Basing on ETSI TS 102 640, an advanced electronic signature or an advanced electronic seal should be created via a Secure Signature Creation Device..

It is good practice to make the data available to the sender signed/sealed by QTSP. The data should be secured by a signature/seal placed on the proof of sending, while ensuring the sent data is integrally linked to this proof.

The certificate allowing verification of an advanced electronic signature or an advanced electronic seal should be verifiable via a Trust Service List.

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;

The best practice is to deliver exactly the same data that was sent, but for interoperability reasons it may be necessary to alter it. If data is altered, information about this should be revealed to both, the sender and the recipient..

Indication about altered data should be part of the delivery process and should be available to the recipient before receiving the confirmation of proof of delivery. Proof of delivery should link in an integrated way the finally delivered data with the identification means of addressee and time of delivery.

f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.

Proof of sending and proof of receiving should be integrally linked to sent/delivered data and time stamped by a qualified time stamp. Qualified time stamp requirements are part of the previous chapter.

Future ETSI standardisation work on electronic registered delivery services will have leverage over the existing multipart TS 102 640 series addressing standardisation of registered electronic mail (REM) and align these specifications to the requirements of the eIDAS Regulation. Effective production of such REM

specifications and more general specifications addressing all other types of electronic registered delivery services has not been planned yet.

The standards could be used as a basis for a technical definition of the qualified electronic registered delivery services, under additional requirements (service profiles) covering the above elements. For instance, the requirement that sent data must be signed/sealed according to (d).

LIST OF STANDARDS

- Registered Electronic Mail (REM) (ETSI/CEN TS 102 640 (5 parts document))
- Functional specification for postal registered electronic mail (UPU S52-2)[168]
- Secured electronic postal services (SePS) interface specification (Parts A& B, (UPU S43a-4 & S43b-4))[169]
- Conformity assessment for REM service providers (ETSI EN 319 513) - missing[170]
- Policy and security requirements for registered electronic mail (REM) service providers (ETSI EN 319 511) - missing[171]
- Registered electronic mail (REM) services (ETSI EN 319 512) - missing[172]
- Testing compliance and interoperability of REM service providers (ETSI TS 119 514) – missing[173]
- AS4 Profile of ebMS 3.0 Version 1.0
- OASIS ebXML Messaging Services Version 3.0

TSPs PROCESS

- Electronic Registered Delivery Process[174]
- Interoperability management
- Electronic identification process
- Authentication process – if done by QTSP

EXTERNAL STAKEHOLDERS

- Subscribers
- Relying parties
- Other qualified electronic registered delivery services
- Other delivery and email services

[168] See Annex B [No. 77]
[169] See Annex B [No. 75/76]
[170] See Annex B [No. 38]
[171] See Annex B [No. 36]
[172] See Annex B [No. 37]
[173] See Annex B [No. 55]
[174] See Annex A

9. Requirements for qualified certificates for website authentication

This chapter concerns requirements for TSPs issuing qualified certificates for website authentication (QCWA). Requirements for a qualified certificate for website authentication are laid down in Article 45 of the eIDAS Regulation.

QCWA is a certificate for website authentication, which is issued by a qualified trust service provider (QTSP). Requirements for QCWA are laid down in Annex IV of the eIDAS Regulation.

The purpose of certificates for website authentication is providing an attested link to natural or legal person for whom the certificate was issued and to make it possible to authenticate and link a website to a user. Website authentication certificates are in common use, and are the common used safeguard against on-line service threats.

9.1 Article 45

CONTENT

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

Annex IV:

Qualified certificates for website authentication shall contain:

(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication;

(b) 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;

(c) for natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym. If a pseudonym is used, it shall be clearly indicated; for legal persons: at least the name of the legal person to whom the certificate is issued and, where applicable, registration number as stated in the official records;

(d) elements of the address, including at least city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records;

(e) the domain name(s) operated by the natural or legal person to whom the certificate is issued;

(f) details of the beginning and end of the certificate's period of validity;

(g) the certificate identity code, which must be unique for the qualified trust service provider;

(h) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;

(i) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point

(h) is available free of charge;

(j) the location of the certificate validity status services that can be used to enquire as to the validity status of the qualified certificate.

GUIDELINE

These requirements apply to a TSP issuing qualified certificates for website authentication only.

QTSP issuing qualified certificates for website authentication should prepare a certificate profile for this purpose. When certificates are issued as EU Qualified Certificates, they should include QCStatements. A QCStatement included in a certificate should be prepared accordingly to ETSI EN 319 412-5[175]. Issuance of qualified certificates for website authentication is regulated by a certification policy. The certification policy should comply with ETSI EN 319 411-2[176], and the certificate should include a certificate policies extension. Keeping a certificate profile appropriate to regulations is part of the compliance management process.

A certificate for website authentication contains the name of the legal or natural person to whom the certificate is issued and operated by their domain name. Verification of this data should be completed based on requirements laid down in Article 24 (1). Additional guidance from CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates[177] (on legal entities), standards for identity proofing for personal certificates (for natural persons).

NOTE: QTSP using ITU-T X.509 should ensure that corrigendum 1[178] and 2[179] is applied to base standard.

LIST OF STANDARDS

- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements[180];
- ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates"
- ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".[181]
- ETSI EN 319 412-4 : Certificate profile for web site certificates issued to organisations[182]
- CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".[183]
- CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates"

---

[175] See Annex B [No. 34]
http://www.etsi.org/deliver/etsi_en/319400_319499/31941205/02.01.01_60/en_31941205v020101p.pdf
[176] See Annex B [No. 29]
[177] See Annex B [No. 56]
[178] See Annex B [No. 65]
[179] See Annex B [No. 66]
[180] See Annex B [No. 28]
[181] See Annex B [No. 30]
[182] See Annex B [No. 33]
[183] See Annex B [No. 41]

- IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile; http://www.rfc-editor.org/rfc/rfc5280.txt
- ITU-T X.509; https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.509-201210-I!!PDF-E&type=items
    - Recommendation X.509 (2012) Corrigendum 1 https://www.itu.int/rec/dologin.asp?lang=e&id=T-REC-X.509-201505-I!Cor1!PDF-E&type=items
    - Recommendation X.509 (2012) Corrigendum 2 (04/16)https://www.itu.int/rec/dologin.asp?lang=e&id=T-REC-X.509-201604-P!Cor2!PDF-E&type=items

TSPs PROCESS

- Compliance management[184]
- Change management

EXTERNAL STAKEHOLDERS

- Member States Supervisory Bodies
- Relying Party – relies upon a Qualified Certificate for website authentication. Only Qualified Certificate for website authentication meeting the requirements laid down in Annex IV is fully recognized by a Relying Party.
- Subscribers – should be assured that they are using a Qualified Certificate for website authentication meeting the requirements laid down in Annex IV in their business processes.

[184]See Annex A

Annex A – List of TSP processes

Process	Type	Description
Access Control	ISMS	Process of limiting system access privileges by the TSP's to authorize individuals.
Authentication	Specified	Electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;
Business continuity	ISMS	Business continuity encompasses planning and preparation to ensure that an organization can continue to operate in case of serious incidents or disasters and is able to recover to an operational state within a reasonably short period.
Certification Authority operations	Specified	The Certification Authority operations process refers to certificate lifecycle management via issuance, revocation and renewal of certificates.
Change Management	ISMS	Controls the lifecycle of all Changes. The primary objective of Change Management is to enable beneficial Changes to be made, with minimum disruption to other services and compliant with requirements.
Compliance Management	General	Ensures IT services, processes and systems comply with enterprise policies and legal requirements.
Configuration Management	IT – service management	Configuration management process is a systems engineering process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.
Conformity Assessment	General	Conformity Assessment process is activity to determine, directly or indirectly, that a process, product, or service meets relevant technical standards and fulfils relevant requirements
Digital Data Preservation	Specified	Digital data preservation is a service to which data objects are submitted to achieve specified preservation goals over the long-term which at least include proof of integrity and proof of existence and which can maintain the validity status of digital signatures.
Documentation management	General	Process used to track, manage and store documents. The process is related to digital asset management, document imaging, workflow systems and records management systems.
Electronic identification	Specified	Process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.
Electronic Registered Delivery Process	Specified	Means a process that makes it possible to transmit data between third parties by electronic means and provides evidence relevant to the handling of the transmitted data, including proof of sending and receiving the data, and that transmitted data is protected against the risk of loss, theft, damage or any unauthorised alterations.
Human Resources Management	General	Process designed to maximize employee performance in service of an employer's strategic objectives. HR is primarily concerned with the

Process	Type	Description
		management of people within organizations, focusing on policies and on systems.
Identity Proofing and Verification	Specified	Process to ensure that a person who is applying, or acting on behalf of another individual, is who they say they are and a process to meet identity verification requirements as a condition of eligibility.
Incident Management	ISMS	The purpose of the incident management process is to restore a normal service operation as quickly as possible and to minimize the impact on business operations, thus ensuring that the best possible level of service quality and availability is maintained.
Information Security Management	ISMS	Information security management describes controls that an organization needs to implement to ensure that it is sensibly managing these risks.
Publication	Specified	The purpose of a publication process is making certificates by The TSP available to subscribers, subjects and relying parties.
Revocation management	Specified	Process of revoking certificates by the TSP in a timely manner based on authorized and validated certificate revocation requests.
Risk Management	ISMS	Objective is to identify, assess and control risks. This includes analysing the value of assets to the business, identifying threats to these assets, and evaluating how vulnerable each asset is to these threats. Risk management allows securing revocation management process.
Security evaluation and certification	ISMS/Specified	The examination of a system to determine its degree of compliance with a stated security model, security standard, or specification.
Security management	ISMS	Security management is the identification of assets (including information assets), followed by the development, documentation, and implementation of policies and procedures for protecting these assets.
Time-stamping management	Specified	This process monitors and controls the operation of the time-stamping services to ensure that the service provided is as specified by the QTSP issuing time stamps. This process is responsible for the installation and de-installation of the time-stamping provision service.
Time-stamping provision	Specified	This process generates time-stamps.
Validation	Specified	The process of verifying and confirming that an electronic signature or a seal is valid. It can be done by TSP/QTPS.

Annex B – List of standards

No	Reference	Version	Title
1.	1501/2015 Implementing Regulation	8 September 2015	Commission implementing regulation on the interoperability framework pursuant to Article 12(8) 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. http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32015R1501
2.	1502/2015 Implementing Regulation	8 September 2015	Commission implementing regulation on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) 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. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002
3.	910/2014 eIDAS Regulation	23 July 2014	Regulation on electronic identification and trust services for electronic transactions in the internal market repealing Directive 1999/93/EC. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
4.	1999/93/EC Directive	13 December 1999	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999L0093&from=EN
5.	ANSSI DCSSI-PP	2008/07	Time-stamping System (CC3.1)
6.	CA/Browser Forum	1.3.9	Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.3.9.pdf
7.	CA/Browser Forum	V1.4.1	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.4.1.pdf
8.	CEN EN 419 221-5	2016	Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic module for trust services
9.	CEN EN 419 231	-	Security requirements for trustworthy systems supporting time-stamping.
10.	CEN TS 419 241-1	Draft	Trustworthy systems supporting server signing Part 1: Security requirements
11.	CEN TS 419 241-2	Draft	Trustworthy systems supporting server signing Part 2:Protection Profile for QSCD for Server Signing

No	Reference	Version	Title
12.	CEN TS 419 261	2015	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures.
13.	CEN/TS 419 221-1	2016	Protection Profiles for TSP cryptographic modules - Part 1: Overview
14.	CEN/TS 419 221-2	2016	Protection Profiles for TSP cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup
15.	CEN/TS 419 221-3	2016	Protection Profiles for TSP Cryptographic modules - Part 3: Cryptographic module for CSP key generation services
16.	CEN/TS 419 221-4	2016	Protection Profiles for TSP cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup
17.	DD CEN/TS 15121-1	2011	Secured electronic postal services (SePS) interface specification. Concepts, schemas and operations.
18.	ETSI EN 319 102-1	V1.1.1 (2016-05)	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation http://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf
19.	ETSI EN 319 122-1	V1.1.1 (2016-04)	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures http://www.etsi.org/deliver/etsi_en/319100_319199/31912201/01.01.01_60/en_31912201v010101p.pdf
20.	ETSI EN 319 122-2	V1.1.1 (2016-04)	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures http://www.etsi.org/deliver/etsi_en/319100_319199/31912202/01.01.01_60/en_31912202v010101p.pdf
21.	ETSI EN 319 132-1	V1.1.1 (2016-04)	Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures http://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.01.01_60/en_31913201v010101p.pdf
22.	ETSI EN 319 132-2	V1.1.1 (2016-04)	Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures http://www.etsi.org/deliver/etsi_en/319100_319199/31913202/01.01.01_60/en_31913202v010101p.pdf
23.	ETSI EN 319 142-1	V1.1.1 (2016-04)	Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures http://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.01.01_60/en_31914201v010101p.pdf
24.	ETSI EN 319 142-2	V1.1.1 (2016-04)	Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles http://www.etsi.org/deliver/etsi_en/319100_319199/31914202/01.01.01_60/en_31914202v010101p.pdf

No	Reference	Version	Title
25.	ETSI EN 319 162-1	V1.1.1 (2016-04)	Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers http://www.etsi.org/deliver/etsi_en/319100_319199/31916201/01.01.01_60/en_31916201v010101p.pdf
26.	ETSI EN 319 162-2	V1.1.1 (2016-04)	Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers http://www.etsi.org/deliver/etsi_en/319100_319199/31916202/01.01.01_60/en_31916202v010101p.pdf
27.	ETSI EN 319 401	V2.1.1 (2016-02)	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers http://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.01.01_60/en_319401v020101p.pdf
28.	ETSI EN 319 411-1	V1.1.1 (2016-02)	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.01.01_60/en_31941101v010101p.pdf
29.	ETSI EN 319 411-2	V2.1.1 (2016-02)	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 http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.01.01_60/en_31941102v020101p.pdf
30.	ETSI EN 319 412-1	V1.1.1 (2016-02)	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures http://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.01_60/en_31941201v010101p.pdf
31.	ETSI EN 319 412-2	V2.1.1 (2016-02)	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons http://www.etsi.org/deliver/etsi_en/319400_319499/31941202/02.01.01_60/en_31941202v020101p.pdf
32.	ETSI EN 319 412-3	V1.1.1 (2016-02)	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons http://www.etsi.org/deliver/etsi_en/319400_319499/31941203/01.01.01_60/en_31941203v010101p.pdf
33.	ETSI EN 319 412-4	V1.1.1 (2016-02)	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates http://www.etsi.org/deliver/etsi_en/319400_319499/31941204/01.01.01_60/en_31941204v010101p.pdf

No	Reference	Version	Title
34.	ETSI EN 319 412-5	V2.1.1 (2016-02)	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements http://www.etsi.org/deliver/etsi_en/319400_319499/31941205/02.01.01_60/en_31941205v020101p.pdf
35.	ETSI EN 319 421	V1.1.1 (2016-03)	Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps http://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf
36.	ETSI EN 319 511	Missing	Policy and security requirements for registered electronic mail (REM) service providers.
37.	ETSI EN 319 512	Missing	Registered electronic mail (REM) services
38.	ETSI EN 319 513	Missing	Conformity assessment for REM service providers
39.	ETSI EN 319 422	V1.1.1 (2016-03)	Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles http://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf
40.	ETSI TR 101 533-2	V1.2.1 (2011-12)	Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 2: Guidelines for Assessors http://www.etsi.org/deliver/etsi_TR/101500_101599/10153302/01.02.01_60/tr_10153302v010201p.pdf
41.	ETSI TR 101 564	V1.1.1 (2011-09)	Electronic Signatures and Infrastructures (ESI); Guidance on ETSI TS 102 042 for Issuing Extended Validation Certificates for Auditors and CSPs http://www.etsi.org/deliver/etsi_tr/101500_101599/101564/01.01.01_60/tr_101564v010101p.pdf
42.	ETSI TR 103 123	V1.1.1 (2012-11)	Electronic Signatures and Infrastructures (ESI); Guidance for Auditors and CSPs on ETSI TS 102 042 for Issuing Publicly-Trusted TLS/SSL Certificates http://www.etsi.org/deliver/etsi_tr/103100_103199/103123/01.01.01_60/tr_103123v010101p.pdf
43.	ETSI TR 119 000	V1.2.1 (2016-04)	Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview http://www.etsi.org/deliver/etsi_tr/119000_119099/119000/01.02.01_60/tr_119000v010201p.pdf
44.	ETSI TS 101 533-1	V1.3.1 (2012-04)	Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management http://www.etsi.org/deliver/etsi_ts/101500_101599/10153301/01.03.01_60/ts_10153301v010301p.pdf

No	Reference	Version	Title
45.	ETSI TS 102 573	V2.1.1 (2012-04)	Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data objectshttp://www.etsi.org/deliver/etsi_ts/102500_102599/102573/02.01.01_60/ts_102573v020101p.pdf
46.	ETSI TS 102 640-1	V2.1.1 (2010-01)	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture http://www.etsi.org/deliver/etsi_ts/102600_102699/10264001/02.01.01_60/ts_10264001v020101p.pdf
47.	ETSI TS 102 640-2	V2.1.1 (2010-01)	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 2: Data requirements, Formats and Signatures for REM http://www.etsi.org/deliver/etsi_ts/102600_102699/10264002/02.01.01_60/ts_10264002v020101p.pdf
48.	ETSI TS 102 640-3	V2.1.1 (2010-01)	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 3: Information Security Policy Requirements for REM Management Domains http://www.etsi.org/deliver/etsi_ts/102600_102699/10264003/02.01.01_60/ts_10264003v020101p.pdf
49.	ETSI TS 102 640-4	V2.1.1 (2010-01)	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Part 4: REM-MD Conformance Profiles http://www.etsi.org/deliver/etsi_ts/102600_102699/10264004/02.01.01_60/ts_10264004v020101p.pdf
50.	ETSI TS 102 640-5	V2.1.1 (2010-01)	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 5: REM-MD Interoperability Profiles http://www.etsi.org/deliver/etsi_ts/102600_102699/10264005/02.01.01_60/ts_10264005v020101p.pdf
51.	ETSI TS 119 101	V1.1.1 (2016-03)	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation http://www.etsi.org/deliver/etsi_ts/119100_119199/119101/01.01.01_60/ts_119101v010101p.pdf
52.	ETSI TS 119 142-2	V1.0.1 (2015-07)	Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles;http://www.etsi.org/deliver/etsi_ts/119100_119199/11914202/01.00.01_60/ts_11914202v010001p.pdf
53.	ETSI TS 119 172-4	Draft	Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists;
54.	ETSI TS 119 312	V1.1.1 (2014-11)	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v010101p.pdf
55.	ETSI TS 119 514		Testing compliance and interoperability of REM service providers

No	Reference	Version	Title
56.	ETSI TS 119 122-3		Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 3: Incorporation of ERS mechanisms in CAdES"
57.	ETSI EN 319 162-1		Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC Baseline containers
58.	ETSI EN 319 162-2		Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers
59.	ESI(16)000165 Draft DSR/ESI-0019510	v0.0.4	Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures
60.	EVCG CA/Browser Forum	1.6.0	Guidelines For The Issuance And Management Of Extended Validation Certificates https://cabforum.org/wp-content/uploads/EV-V1_6_0.pdf
61.	ISO 31000	2009	Risk management - Principles and guidelines
62.	ISO/IEC 15408	2009	Information technology - Security techniques - Evaluation criteria for IT security(parts 1 to 3)
63.	ISO/IEC 19790	2012	Information technology - Security techniques - Security requirements for cryptographic modules
64.	ISO/IEC 20000-1	2011	Information technology - Service management - Part 1: Service management system requirements
65.	ISO/IEC 27001	2013	Information technology - Security techniques - Information security management systems - Requirements
66.	ISO/IEC 27002	2013	Information technology - Security techniques - Code of practice for information security controls
67.	ISO/IEC 27005	2011	Information technology - Security techniques - Information security risk management
68.	ISO 14721:2012	2012	Space data and information transfer systems – Open archival information system (OAIS) – Reference model
69.	ISO 14533-1:2014	2014	Processes, data elements and documents in commerce, industry and administration – Long term signature profiles – Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)
70.	ISO 14533-2:2014	2014	Processes, data elements and documents in commerce, industry and administration – Long term signature profiles – Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)
71.	ISO/IEC Directives	2015	Annex SL, Part 1
72.	ITU-T X.509	(05/2015)	Recommendation ITU T X.509 (2012) – Technical Corrigendum 1 https://www.itu.int/rec/T-REC-X.509-201505-S!Cor1/en
73.	ITU-T X.509	(04/2016)	Recommendation ITU T X.509 (2012) – Technical Corrigendum 2 https://www.itu.int/rec/T-REC-X.509-201604-S!Cor2/en
74.	M/530	20.1.2015	COMMISSION IMPLEMENTING DECISION C(2015) on a standardisation request to the European standardisation organisations regarding European standards and European

No	Reference	Version	Title
			standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy. http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548#
75.	OASIS ebXML	3.0	Messaging Services https://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/cs02/ebms_core-3.0-spec-cs-02.html
76.	OASIS Standard	23 January 2013 Version 1.0	AS4 Profile of ebMS 3.0 http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html
77.	RFC 3161	2011	Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP) https://www.ietf.org/rfc/rfc3161.txt
78.	RFC 3647	April 2015	Template for a Certification Practice Statement (CPS) for the Resource PKI (RPKI) https://www.ietf.org/rfc/rfc3647.txt
79.	RFC 3739	March 2004	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile https://www.ietf.org/rfc/rfc3739.txt
80.	RFC 5280	May 2008	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile https://www.ietf.org/rfc/rfc5280.txt
81.	RFC 6960	June 2013	Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP https://tools.ietf.org/rfc/rfc6960.txt
82.	RFC 4998		Evidence Record Syntax (ERS)
83.	RFC 6283	2011	Extensible Markup Language Evidence Record Syntax (XMLERS)
84.	RFC 2630		Cryptographic Message Syntax
85.	UPU S43a-4		Part A: Concepts, schemas and operations
86.	UPU S43b-4		Part B: EPCM Service
87.	UPU S52-2	2015	Functional specification for postal registered electronic mail.

ENISA

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

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

Catalogue Number TP-06-16-342-EN-N

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

ISBN: 978-92-9204-191-5
DOI: 10.2824/721561