EUROPEAN UNION AGENCY
FOR CYBERSECURITY

SECURITY FRAMEWORK FOR QUALIFIED TRUST SERVICE PROVIDERS

Technical guidelines of qualified trust service providers

MARCH 2021

ABOUT ENISA

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

CONTACT

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

CONTRIBUTORS

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

EDITORS

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

ACKNOWLEDGEMENTS

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

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-439-8 - DOI: 10.2824/06258

TABLE OF CONTENTS

1. INTRODUCTION 5

1.1 THE ROLE OF ENISA 5

1.2 BACKGROUND ON QUALIFIED TRUST SERVICE PROVISIONING 5

1.3 TARGET AUDIENCE 9

1.4 PURPOSE AND STRUCTURE OF THIS DOCUMENT 9

1.5 DISCLAIMER 10

2. RISK MANAGEMENT 12

2.1 RECOMMENDATIONS FOR QTSPs 12

3. SECURITY INCIDENT MANAGEMENT 14

3.1 RECOMMENDATIONS FOR QTS 14

4. QUALIFIED TRUST SERVICES SECURITY MEASURES 15

4.1 SECURITY MEASURES FOR ALL QTSPs 15

4.2 SECURITY MEASURES FOR PROVISION OF SPECIFIC QTS 17

5. REFERENCES 20

5.1 ENISA PUBLICATIONS 20

5.2 APPLICABLE LEGISLATION / REGULATION 20

5.3 STANDARDS AND OTHERS 20

ABBREVIATIONS

CA	Certification Authority
CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
CEN	Centre Européen de Normalisation
EN	European Standard
ERDS	Electronic Registered Delivery Service
ETSI	European Telecommunications Standards Institute
ETSI TS	ETSI Technical Specifications
eSig	electronic Signature
eSeal	electronic Seal
EU	European Union
GDPR	General Data Protection Regulation
ISO	International Organization for Standardisation
MS	Member State
PKI	Public Key Infrastructure
QERDS	Qualified Electronic Registered Delivery Service
QESeal	Qualified Electronic Seal
QESig	Qualified Electronic Signature
QTS	Qualified Trust Service
QTSP	Qualified Trust Service Provider
QTSP/QTS	Qualified Trust Service Provider and the Qualified Trust Service it provides
QREMS	Qualified Registered Electronic Mail Service
RA	Registration Authority
REMS	Registered Electronic Mail Service
SB	Supervisory Body
TS	Trust Service
TSP	Trust Service Provider
TSP/TS	Trust Service Provider and the Trust Service it provides

EXECUTIVE SUMMARY

Regulation (EU) No 910/2014 (also known as the "eIDAS Regulation"), on electronic identification and trust services for electronic transactions in the internal market, provides a regulatory environment for electronic identification of natural and legal persons and for a set of electronic trust services, namely; electronic signatures, seals, time stamps, registered delivery services and certificates for website authentication.

One objective of this Regulation is to enhance the trust of enterprises and consumers in the internal market and to promote the use of trust services and products. To that end, the Regulation introduces the notions of qualified trust service (QTS) and qualified trust service provider (QTSP) with a view to indicating their compliance with the eIDAS high-level security requirements and obligations. A QTSP is a TSP that has been granted a qualified status and is supervised by its national supervisory body (SB).

The aforementioned requirements and obligations are specified in:

- Article 5 on data processing and protection;
- Article 13 on liability;
- Article 15 on accessibility for persons with disabilities;
- Article 19 on security;
- Article 24.2 on requirements for qualified trust services providers; and
- Other articles on specific requirements regarding the QTS(s) provided by the QTSP.

This document proposes a security framework to achieve compliance with Article 19 of the eIDAS Regulation, to which both non-QTSP and QTSP are subject. Nevertheless, Article 19.1 states that the security measures *"shall ensure that the level of security is commensurate to the degree of risk"*. Because a security incident can have a different impact on the outputs of a QTSP than those of a TSP (e.g. loss of legal validity) and the QTSP itself (e.g. loss of qualified status and related business line), the degree of risk can be different for QTSPs and non-QTSPs.

It is also possible for a non-QTSP to meet the same (or even higher) standards of quality and trustworthiness as a QTSP. In fact, to achieve compliance with Article 19 (valid for both, QTSPs and non-QTSPs), this series of documents recommend that the level of security implemented by non-QTSP, expected to follow 'best practices' when operating with due diligence, is equivalent to the one of QTSP. For this reason, the security practices applied by QTSPs are also relevant to – and can also be followed by – non-QTSPs.

The background on trust service provisioning and the related security framework, on which qualified trust service provisioning relies, is presented in the [ENISA Security Framework for TSPs], to be considered as a pre-requisite to this document.The framework based is on guidelines for TSPs, taking into account the type of provided trust services, regarding policies, procedures, and processes in order to achieve compliance with the security requirements defined in eIDAS under Articles 19.1 and 19.2.

This document completes the latter with recommendations specific to QTSP/QTS, in particular in order to achieve compliance with the security requirements defined in eIDAS under Article 24.2, and the other articles on specific requirements regarding the QTS(s) provided by the QTSP.

1. INTRODUCTION

1.1 THE ROLE OF ENISA

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

ENISA also supports the national supervisory bodies in implementing their breach reporting by aggregating their annual summary reports on trust service provider security breaches. The Agency releases Annual Reports on Trust Services Security Incidents. Moreover, in a means to support an efficient, effective process of reporting, the Agency has released the Visual Tool - CIRAS to increase the transparency of cybersecurity incidents. The online tool is accessible to the public[1].

1.2 BACKGROUND ON QUALIFIED TRUST SERVICE PROVISIONING

1.2.1 Definitions of qualified trust services

The eIDAS Regulation ([eIDAS, 2014]) provides a regulatory environment for electronic identification of natural and legal persons and for trust services in the internal market.

One objective of this Regulation is to enhance the trust of enterprises and consumers in the internal market and to promote the use of trust services and products. To that end, the Regulation introduces the notions of QTS and QTSP with a view to indicating their compliance with the eIDAS high-level security requirements and obligations. A QTSP is a TSP that has been granted a qualified status by its national SB. The background on trust service provisioning and the related security framework, on which qualified trust service provisioning relies, is presented in the [ENISA Security Framework for TSPs], to be considered as a pre-requisite to this document.

The eIDAS Regulation defines 9 types of QTS:

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

[1] https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

1.2.2 Trust Framework

1.2.2.1 Requirements and obligations

Firstly, all QTSPs and the QTSs they provide (hereinafter collectively referred to as QTSPs/QTSs) are subject to a set of common obligations and requirements, defined in:

- Article 5 on data processing and protection;
- Article 13 on liability;
- Article 15 on accessibility for persons with disabilities;
- Article 19 on security; and
- Article 24.2 on requirements for qualified trust services providers.

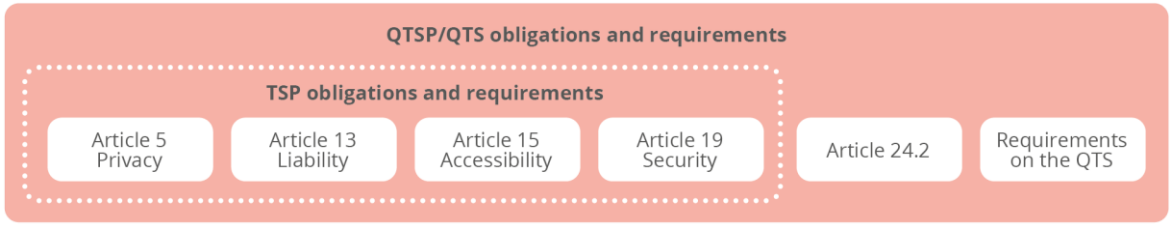
Secondly, there are specific requirements on the QTS(s) provided by the QTSP (Articles 24, 28, 29, 32, 34, 38, 39, 40, 42, 44, and 45).

Each aforementioned article is further covered in [ENISA Recommendations for QTSPs based on standards].

Both QTSPs and non-QTSPs are subject to Article 5, 13, 15, and 19, however, the eIDAS Regulation stresses a significant difference between the liability of non-QTSP and QTSP in Article 13.1: *"The intention or negligence of a QTSP shall be presumed unless that QTSP proves that the damage occurred without the intention or negligence of that QTSP"*. Considering this difference, measures selected by the QTSP may be taken in the light of this burden of proof. In particular, but not only, the collection of evidence by the QTSP may also be seen as essential to prove, in case of litigation, that the QTSP acted with due diligence. This topic will be covered further throughout this document.

Requirements that apply to QTSP/QTS are summed up and illustrated as follows:

Figure 1: QTS/QTS obligations and requirements



1.2.2.2 Compliance supervision

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

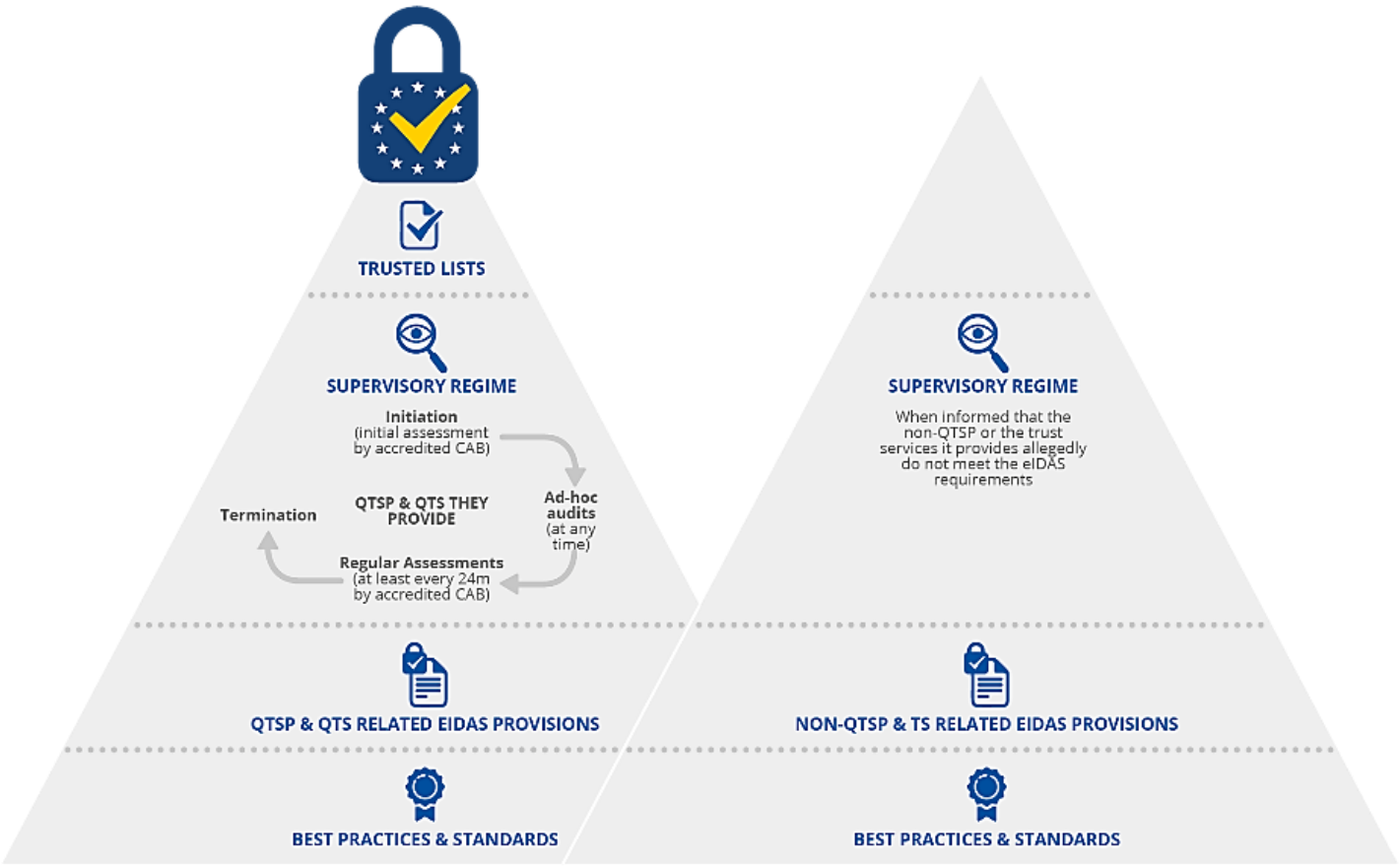
- **At initiation, on regular basis, and at any time** to ensure high-level security of QTSs: When a TSP without qualified status intends to start providing QTS or when a QTSP needs to confirm (as part of a regular assessment or an *ad hoc* audit) that the QTS it provides fulfils the eIDAS requirements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

application of provisions on termination plans in cases where QTSPs cease their activities.

On the other hand, non-QTSPs are subject to a light touch and reactive *ex post* supervision model that is justified by the nature of their services and operations. This supervisory regime does not require audits by CABs. In fact, the national SB has no general obligation to supervise non-QTSPs and should only take action when it has been informed of a non-compliance with eIDAS.

These supervision models are the foundation of the trust framework as defined by eIDAS. It is setting up two distinct complete pyramids of trust; one for the QTSPs and the QTS they provide, and one for the non-QTSP, which are illustrated below.

Figure 2: eIDAS QTSP pyramid of trust (on left) and non-QTSP pyramid of trust (on right)



On top of the QTSP pyramid of trust are the trusted lists (i.e. files including information related to the QTSPs, together with information related to the QTSs provided by them) and the EU trust mark. More information on the trusted lists and the EU trust mark can be found in ENISA series on initiation[2], supervision[3], and termination[4] of QTS and [ENISA Recommendations for QTSP based on standards].

[2] https://www.enisa.europa.eu/publications/tsp-initiation
[3] https://www.enisa.europa.eu/publications/tsp-supervision
[4] https://www.enisa.europa.eu/publications/tsp-termination

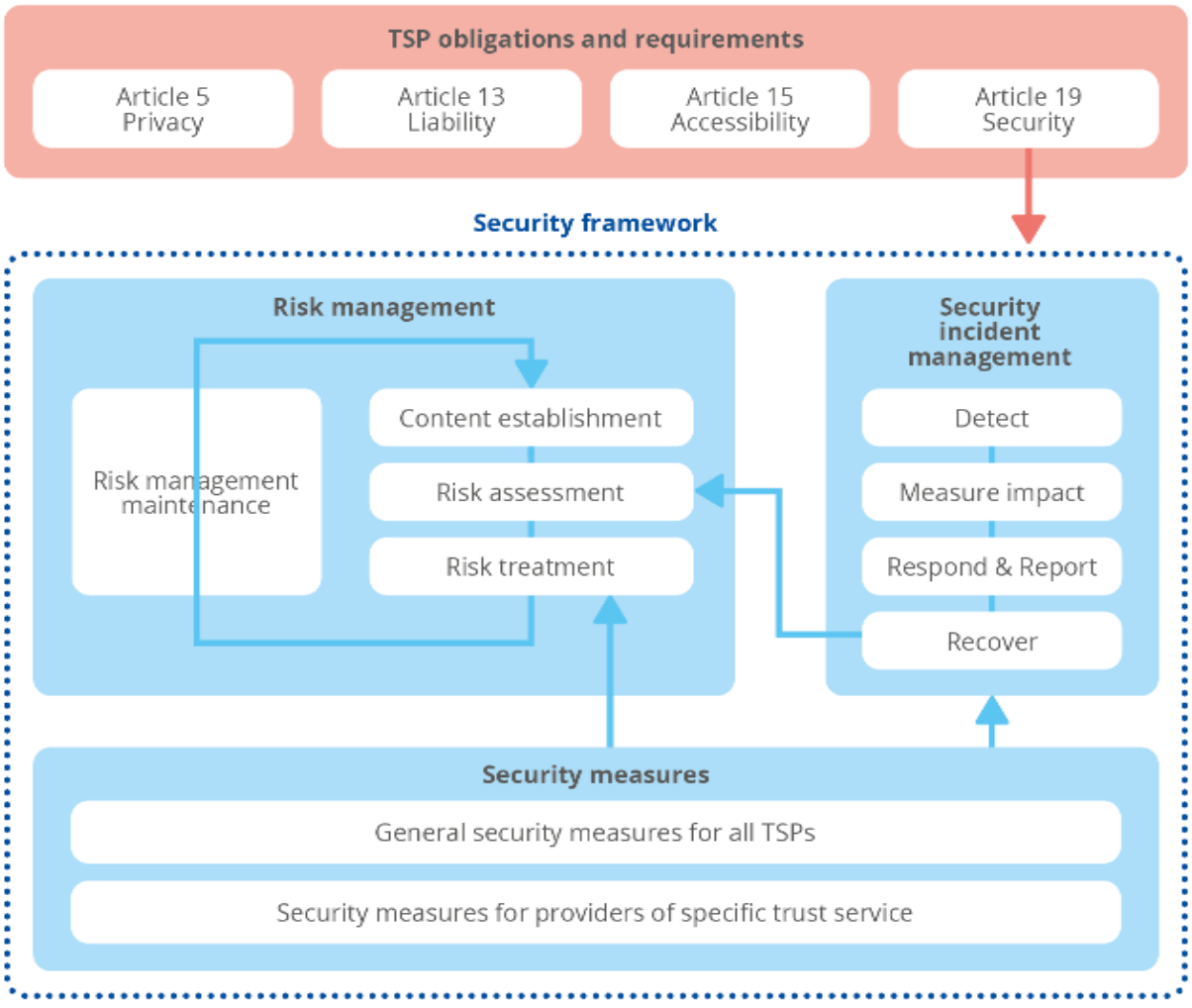
1.2.3 Security Framework

Both non-QTSPs and QTSPs are subject to Article 19 on security requirements (more general information about Article 19 and security framework can be found in Section 1.2.3 of [ENISA Security Framework for TSPs]). Nevertheless, Article 19.1 states that the security measures *"shall ensure that the level of security is commensurate to the degree of risk"*. As further covered in Section 2, because a security incident often has a more significant impact on the outputs of a QTSP than those of a TSP (e.g. loss of legal validity), the degree of risk can be seen as higher than for a TSP and it therefore requires a higher level of security. Qualified services are usually used to handle more sensitive information, or in more secure environments, therefore the breach of security can have a stronger impact. It is however perfectly possible for a non-QTSP to meet the same (or even higher) standards of quality and trustworthiness as a QTSP.

To ensure that the minimum level of security is implemented by the QTSP, Article 24 "Requirements for qualified trust service providers" defines requirements to ensure that some specific security aspects are properly addressed by the QTSP. Related to this, besides Article 24, eIDAS also defines additional requirements for QTSP depending on the QTS(s) they provide, through Articles 28, 29, 32, 34, 38, 39, 40, 42, 44, and 45.

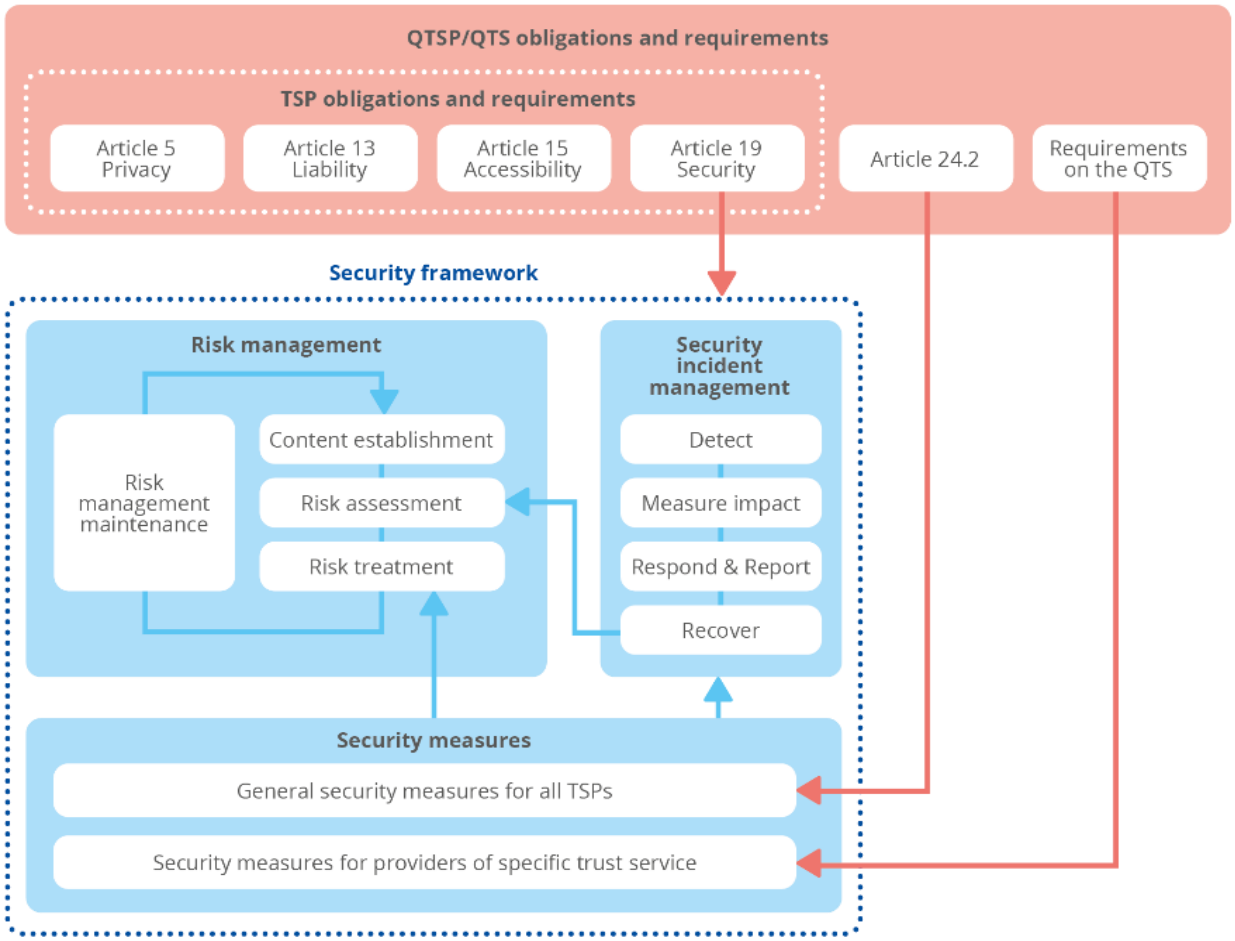
In Section 1.2.3 of [ENISA Security Framework for TSPs], the security framework for non-QTSP is illustrated as follows:

Figure 3: Security Framework for TSPs



Related to what is stated in this section, the security framework for QTSPs can be illustrated as follows:

Figure 4: Security framework for QTSPs



1.3 TARGET AUDIENCE

The audience of this document is **TSPs, prospective QTSPs, and QTSPs** looking for guidelines for fulfilling requirements originating from the eIDAS Regulation.

In particular, TSPs aiming to become qualified might be interested in identifying, based on this document, the additional security requirements to those proposed for non-QTSPs in order to be granted the qualified status.

1.4 PURPOSE AND STRUCTURE OF THIS DOCUMENT

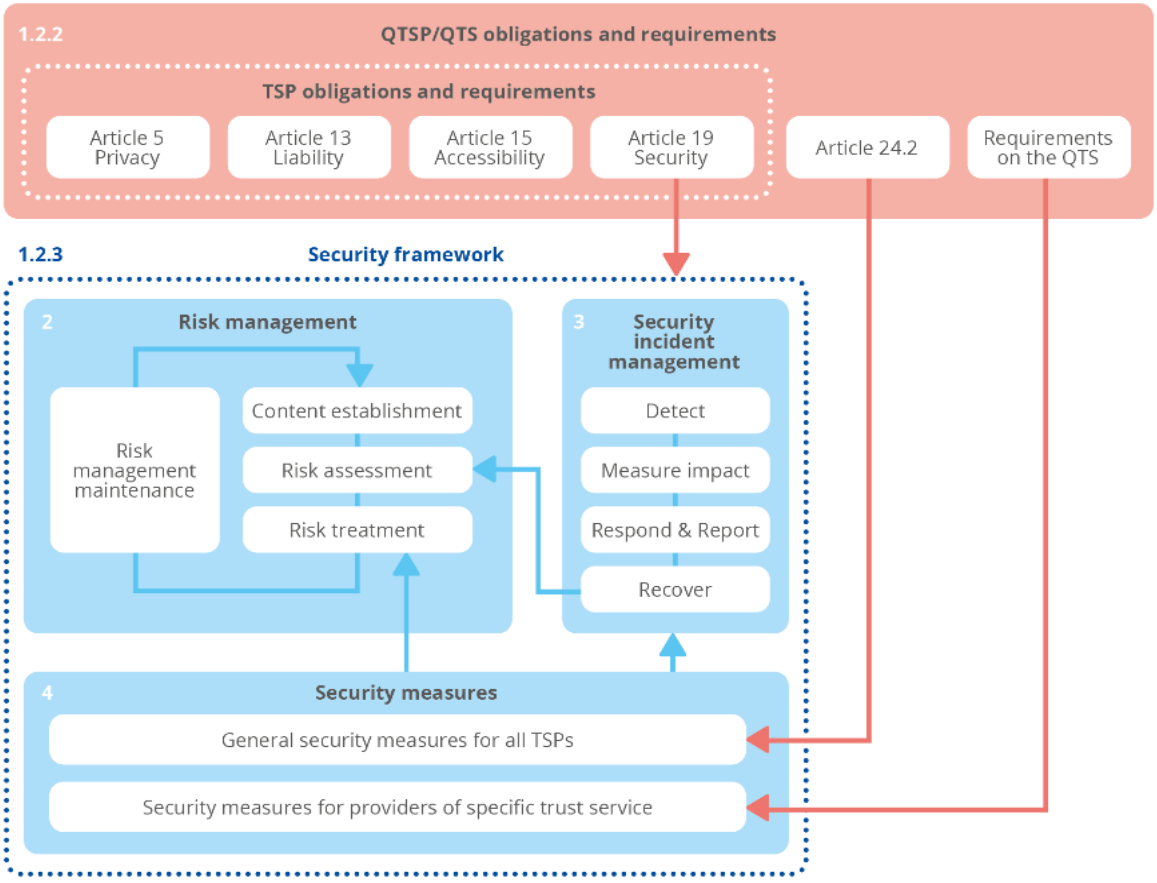
This document is to be used in addition to the security framework common to all TSPs, proposed in [ENISA Security Framework for TSPs], that proposes a security framework based on guidelines for TSPs, taking into account the type of provided trust services, regarding policies, procedures, and processes in order to achieve compliance with the security requirements defined in eIDAS under Articles 19.1 and 19.2.

This document completes the latter with elements peculiar to QTSP/QTS, particularly in order to achieve compliance with the security requirements defined in eIDAS under Article 24, and, depending on the qualified trust service, Articles 28, 29, 32, 34, 38, 39, 40, 42, 44, and 45.

The structure of this document is consistent with the latter. In particular:

- **Section 2** "Risk management" provides recommendations that are specific to QTSPs when performing the risk management proposed in [ENISA Security Framework for TSPs].
- **Section 3** "Security incident management" provides recommendations that are specific to QTSPs when managing security incidents as proposed in [ENISA Security Framework for TSPs].
- **Section 4** "Trust services security measures" proposes a list of references to help to mitigate the risks identified in Section 2 and monitoring security events that might be relevant for notification and remediation as identified in Section 3. The proposed references come from "technical" standards and best practices to address the risks both in general (Section 4.1) and in relevance to the specific trust services provided (Section 4.2).

Figure 5: Structure of the document



This document refers to ETSI and ISO/IEC standards (see disclaimer below). The ETSI standards in particular, tailor generic risk management to eIDAS trust services and provide requirements that answer directly to eIDAS requirements (i.e. not necessarily linked to the security framework). These standards are consequently and logically also referred in [ENISA Recommendations for QTSPs based on standards] as benchmarks to achieve compliance with eIDAS, including the related security obligations. [ENISA Recommendations for QTSP based on standards] will provide key references to this document.

1.5 DISCLAIMER

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

- Different approaches based on different technologies than the ones exposed in this document can lead to eIDAS compliance;
- Compliance against the standards (or other standards) is not mandatory to achieve compliance against eIDAS requirements;
- Compliance against these standards does not automatically imply conformance to eIDAS requirements. Although these standards may be seen as best practices, there is no automatic presumption of compliance[5] to eIDAS after following the said standards.

[5] Some nationally-defined schemes (e.g. in Czech Republic, France, Netherlands, Slovakia) specify conformity criteria based on the ETSI standards, along with a limited set of additional requirements, that provide presumption of compliance to the eIDAS requirements.

2. RISK MANAGEMENT

As mentioned in Section 1.1.3, the eIDAS Regulation requires that TSP shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide and to minimize the impact of security incidents. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk.

Many standards already provide guidelines for risk management. One of them is [ISO/IEC 27005]. It provides guidelines for information security risk management in an organization, supporting the requirements of information security management (ISMS) according to [ISO/IEC 27001]. However, this standard does not provide any specific method for information security risk management.

Based on [ISO/IEC 27005] general approach, [ENISA Security Framework for TSPs] aims at presenting more specific and practical guidelines for TSPs regarding the management of risks posed to the security of their trust services.

The guidelines for QTSPs are proposed to be similar to those for TSPs. The QTSPs are suggested to consult [ENISA Security Framework for TSPs] for a method to manage the risks posed to the security of its qualified trust services.

2.1 RECOMMENDATIONS FOR QTSPs

Besides the guidelines proposed in [ENISA Security Framework for TSPs], this document recommends the following.

2.1.1 Level of security required by the qualified status

The eIDAS Regulation introduced the notions of qualified trust service (QTS) and qualified trust service provider (QTSP) with a view to indicating requirements and obligations that ensure **high-level security** and a **higher presumption of their legal effect**. Because of this higher presumption of legal effects (e.g. Qualified Electronic Signature, QES, has the equivalent legal effect to handwritten signature), the consequences of a security incident can have a higher impact on a QTSP than those of a non-QTSP, in particular for customers of the QTSP: e.g. previously issued QES may *a posteriori* lose their qualified status, issued certificates cannot be used for QES anymore, previous validations of QES may be questioned, QES may be wrongly preserved because badly secured. Besides the impact on customers, the withdrawal of the qualified status of a QTSP may have dramatic consequences on the viability of the QTSP; the consequence of a security incident may cause the withdrawal of its qualified status and so the loss of its business line and customers (e.g. customers which need qualified certificates). This must be considered by the QTSP when estimating the **level of impact** of security incident on an asset (see Section 2.2.1.5 “Identification of consequences” and Section 2.2.2.2 “Estimation of the level of impacts” of [ENISA Security Framework for TSPs]).

Following the formula provided in Section 2.2.2.3 of [ENISA Security Framework for TSPs]:

$$\boldsymbol{Risk = Threat \times Vulnerability \times Impact}$$

As the *Impact* increases, the degree of risk also increases and so the level of security required for QTSP may be higher than one for non-QTSP.

Related to this, the QTSP must also **formulate appropriate risk acceptance criteria**, used to evaluate the significance of a risk and to determine whether the risk is acceptable or tolerable, which ensure that the level of security is commensurate to the degree of risk. The risk acceptance criteria will influence the **risk treatment measures**.

2.1.2 Presumption of negligence

Formulating an appropriate risk acceptance criteria and implementing the adequate controls is particularly important regarding the liability of the QTSP. The eIDAS Regulation states in Article 13: "*The intention or negligence of a QTSP shall be presumed unless that QTSP proves that the damage* […] *occurred without the intention or negligence of that QTSP.*" This means that, in order to prove that the QTSP operated without intention or negligence, it is essential that the QTSP is able to demonstrate that it operated with due diligence. It is therefore highly recommended when implementing the adequate controls to attach importance to **collection** of the records, audit, and monitoring of these controls. This topic, that is certainly a best practice for TSP, can be seen as a self-protective measure for a QTSP. Particular attention must also be paid to the **protection** of such records and therefore their associated level of impact if they are compromised.

2.1.3 Conformity assessments

Although this is a valid point for TSPs, it takes an additional importance for QTSPs to undergo a conformity assessment (also called "audit"), since most, if not all, audit schemes require the TSP to perform a risk assessment and to produce the related mitigation plan.

2.1.4 Measures against forgery and theft of data

The eIDAS Regulation states in Article 24.2(g) that the QTSP shall *"take appropriate measures against forgery and theft of data"*. It thereby emphasizes the fact that, among the technical and organisational measures to manage the risks posed to the security of its trust services, the QTSP shall particularly pay attention to the forgery and theft of data. This should be considered when identifying threats (see Section 2.2.1.2 "Identification of threats" of [ENISA Security Framework for TSPs]).

3. SECURITY INCIDENT MANAGEMENT

[ENISA Security Framework for TSPs] already presents guidelines supporting TSP in fulfilling the part of Article 19.1 and Article 19 by using the appropriate measures to efficiently **detect**, **measure**, **respond**, **report**, and **recover** from security incidents.

The guidelines for QTSP are proposed to be identical for TSP. The QTSP is then suggested to consult this document for more information about the appropriated measures related to security incident management.

3.1 RECOMMENDATIONS FOR QTS

Besides the guidelines proposed in [ENISA Security Framework for TSPs], this document recommends the following.

3.1.1 Termination plan

[ENISA Security Framework for TSPs] recommends in Section 3.4 “Recover from the incident” to be prepared before an incident occurs with a termination plan. Such a termination plan is mandatory for QTSP following Article 24.2(i) of eIDAS. A termination plan is a key document regarding a QTSP/QTS. As stated in Recital (41), Article 17(4) and Article 24.2(i) of eIDAS, this document shall be verified by the SB because of its particular importance regarding the sustainability and durability of QTSs and to boost users’ confidence in the continuity of qualified trust services, such as in exceptional/unfortunate cases of QTSP unscheduled termination (e.g. bankruptcy). Detailed information on the termination plan can be found in the related section of [ENISA Recommendations for QTSPs based on standards].

4. QUALIFIED TRUST SERVICES SECURITY MEASURES

Section 4 of [ENISA Security Framework for TSPs], called “Trust services security measures”, proposes a list of security measures to help mitigating the risks identified in Section 2 and monitoring security events that might be relevant for notification and remediation as identified in Section 3. The proposed measures come from technical standards and best practices to address common for all and with relevance with specific trust services offered.

This section proposes a list of references above those proposed in [ENISA Security Framework for TSPs] that are targeted to QTSP/QTS.

It may be observed that the additional security measures to be implemented by QTSP/QTS are limited. As a matter of fact, when a TSP operates with due diligence, its security measures are similar to the security measures required to QTSP. The few additional security measures are further detailed in the below sections.

NOTE1**:** As mentioned in Section 1.4, to provide QTSP with further guidance and illustration on these policies, procedures, and processes, this document refers to ETSI and ISO/IEC standards. These standards are not made mandatory by the eIDAS Regulation. Regarding the ETSI standards, it is worth noting that they tailor generic risk management to eIDAS trust services and as such, the security measures they contain may be regarded as the benchmark / common answer to the risks that are typically identified when operating the corresponding QTS and their components. In that respect, the categories of security measures identified in the subsections below may be seen as “typical topics of concern” when operating a QTSP offering a specific type of QTS.

NOTE2: This section aims at introducing a list of security measures in the context of eIDAS Article 19 security framework, as well as pertinent security measures derived from eIDAS articles specific to QTSP/QTS. This section does not intend to provide guidelines to achieve full compliance of a QTSP/QTS with the requirements of eIDAS. For such guidelines, the reader may be interested in [ENISA Recommendations for QTSPs based on standards].

4.1 SECURITY MEASURES FOR ALL QTSPS

As previously mentioned, security measures for QTSPs and non-QTSP don’t deviate much. In fact, as part of this series of documents, the security measures proposed to QTSP/QTS are the same as the security measures for all TSPs proposed in [ENISA Security Framework for TSPs]. These security measures are based on [EN 319 401] and are further introduced in [ENISA Security Framework for TSPs].

However, one must note that some of the presented security measures are made mandatory for QTSPs in the eIDAS Regulation. These mandatory requirements for all QTSPs are laid down in Article 24.2. All of them are mapped below with their [EN 319 401] requirements (this mapping originates from Annex A of [EN 319 411-2]):

Article 24.2 states that *a QTSP providing QTSs shall:*	
a) inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities;	-
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;	Clause 7.2
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;	REQ-7.1.1-04
d) 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;	Clause 6.2
e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;	Clause 7.5
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;	Clause 7.6 REQ-7.4-02 REQ-7.4-03 REQ-7.4-10 Clause 7.7 Clause 7.8
g) take appropriate measures against forgery and theft of data[6];	Clause 7.2 to Clause 7.12
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;	Clause 7.12 REQ-7.7-07
i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4);	Clause 7.12
j) ensure lawful processing of personal data in accordance with Directive 95/46/EC;	REQ-7.13-05

Each of the points enumerated in this article are specifically covered in [ENISA Recommendations for QTSPs based on standards].

[6] This clause is discussed in Section 2.1.

An important note for all QTSPs concerns their liability pursuant to Article 13 of eIDAS: "*The intention or negligence of a QTSP shall be presumed unless that QTSP proves that the damage* […] *occurred without the intention or negligence of that QTSP.*" This means that in order to prove that the QTSP operated without intention or negligence, it is essential that the QTSP is able to demonstrate it operated with due diligence. It is therefore highly recommended to QTSP to attach a high importance to the **collection** and **protection** of the records and audits.

Regarding the collection and protection of the records and audits, it should be noted that pursuant to Article 24.2(h) of eIDAS, it is required that they shall be made accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased.

4.2 SECURITY MEASURES FOR PROVISION OF SPECIFIC QTS

4.2.1 Provision of qualified certificates

On top of the security measures for certification services provided in [ENISA Security Framework for TSPs], this section covers additional measures applicable to the provision of qualified certificates.

As mentioned in [ENISA Security Framework for TSPs], security requirements for the issuance of certificates are specified in ETSI EN 319 411 parts 1 and 2 "Policy requirements for TSP issuing certificates". In particular, [EN 319 411-2] provides specific requirements for QTSP issuing qualified certificates. Additional requirements related to the security framework are laid down in:

- **Clause 6.5.1** on "Key Pair Generation and Installation" (complements [EN 319 411-1] clause 6.5.1). The listed requirements concern the generation and installation of key pairs related to qualified certificates, where the private key resides on a QSCD.

QTSP issuing qualified website authentication certificates looking for their recognition by browsers may also be interested in [TSP Technical Best Practices], developed by representatives of Apple, Google, Microsoft, and Mozilla.

4.2.2 Qualified validation service for QESig/QESeal

Security and policy requirements for this service are specified in [TS 119 441] "Policy requirements for TSP providing signature validation services".

Additional requirements for QTSP providing qualified validation service are proposed in Annex B of this standard. Nevertheless, this Annex does not comprise any additional technical and organisational measures to manage the risks posed to the security of the provision of this trust service. Instead, it provides requirements to comply with Article 33 of eIDAS. This is covered further in [ENISA Recommendations for QTSPs based on standards].

Therefore, security measures described in [ENISA Security Framework for TSPs] for signature validation service also apply for QTSP providing qualified validation service for qualified signatures and/or qualified seals.

4.2.3 Qualified preservation service for QESig/QESeal

Security and policy requirements for this service are specified in [TS 119 511] "Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques".

Additional requirements for QTSP providing a qualified preservation service are proposed in Annex A of this standard. Nevertheless, this Annex does not comprise any additional technical

and organisational measures to manage the risks posed to the security of the provision of this trust service. Instead, it provides requirements to comply with Article 34 of eIDAS. This is covered further in [ENISA Recommendations for QTSPs based on standards].

Therefore, security measures described in [ENISA Security Framework for TSPs] for preservation service also apply for QTSP providing qualified preservation services.

4.2.4 Qualified time-stamping service

Security and policy requirements for this service are specified in [EN 319 421] "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

Additional requirements for QTSP providing qualified time-stamps are proposed in clause 8 of this standard. In a nutshell, it states that:

- The time-stamping unit (TSU) signature verification (public) key certificate is recommended to be issued by a certification authority operating under [EN 319 411-2] certificate policy;
- The TSU issuing qualified time-stamps shall not issue non-qualified electronic time-stamps. As stated in [EN 319 411-2] clause 8.1 note 2, *"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 TSU is listed in the Trusted List and the service it represents is a qualified time-stamping service, then the time-stamps issued by this TSU can be considered as qualified."*

4.2.5 Qualified electronic registered delivery service

Security and policy requirements for this service are specified in [EN 319 521] "Policy and security requirements for Electronic Registered Delivery Service (ERDS) Providers" and [EN 319 531] "Policy and security requirements for Registered Electronic Mail Service (REMS) Providers".

These standards explicitly indicate which requirements apply to the qualified services thanks to specific sections called "Provisions for EU QREMS/QERDS". The content of these sections is covered in this section; The section that applies to non-qualified electronic registered delivery services (non-QERDS) and non-qualified registered electronic mail services (non-QREMS), are further covered in [ENISA Security Framework for TSPs].

Regarding the management and operation of EU QREMS and QERDS, the only additional proposed security measure targets human resources (clause 7.2.2 of [EN 319 521]) and in particular, the necessity of an identity verification officer.

Regarding general provision on QERDS and on QREMS, clauses 5 of both standards provide **ad-hoc requirements** on the QTSP. Specifically, the delta for qualified services are included in the sections "Provisions for EU QREMS/QERDS" of the following clauses:

- **Clause 5.1** User content integrity and confidentiality;
- **Clause 5.2** Users Identification and Authentication**;**
- **Clause 5.3** Time reference;
- **Clause 5.4** Events and evidence;
- **Clause 5.5** Interoperability.

4.2.6 Remote QSCD services

The Regulation states through Recital (51) that it should be possible for the signatory (resp. creator of the seal) to entrust QSCDs to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory (resp. creator of the

seal) has sole control (resp. control) over the use of his electronic signature/seal creation data, and the qualified electronic signature/seal requirements are met by the use of the device.

As stated in eIDAS Recital (52), *in order to ensure that such electronic signatures*[/seals] *receive the same legal recognition as electronic signature*[/seals] *created in an entirely user-managed environment, remote electronic signature service providers should:*

1) *apply specific management and administrative security procedures; and*
2) *use trustworthy systems and products*.

Following 1), eIDAS requires that remote QSCDs may only be provided by QTSPs, even if this type of service is not a qualified trust service per se. The security measures proposed in Section 4.1 for all QTSPs therefore also apply to QTSP providing remote QSCD services. Additionally, on top of [EN 319 401], ETSI released [TS 119 431-1] proposing “Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev”.

Following 2), to ensure their trustworthiness, systems and products must implement appropriate technical measures to manage the risks posed to their security. Annex II of eIDAS made some of these security measures mandatory and also made, pursuant to Article 30(1) and 39(2) of eIDAS, the certification against these security measures mandatory. The security framework of such systems and products are provided in CEN [EN 419 241-2].

More information on the standards that can be used to comply with eIDAS requirements, and relevant security measures, can be found in the related section of [ENISA Recommendations for QTSPs based on standards].

5. REFERENCES

5.1 ENISA PUBLICATIONS

ID	Description
ENISA Article 19 Incident reporting	Article 19 Incident reporting - Incident reporting framework for eIDAS Article 19 https://www.enisa.europa.eu/publications/article19-incident-reporting-framework
ENISA Recommendations for QTSPs based on standards	Recommendations for QTSPs based on Standards https://www.enisa.europa.eu/publications/reccomendations-for-qtsps-based-on-standards/
ENISA Security Framework for TSPs	Security Framework for Trust Providers https://www.enisa.europa.eu/publications/security-framework-for-trust-providers/

5.2 APPLICABLE LEGISLATION / REGULATION

ID	Description
eIDAS, 2014	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014, p. 73–114. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

5.3 STANDARDS AND OTHERS

ID	Description
ISO/IEC 27001	ISO/IEC 27001:2013: "Information technology -- Security techniques -- Information security management systems -- Requirements".
ISO/IEC 27005	ISO/IEC 27005:2018: “Information technology — Security techniques — Information security risk management”
EN 419 241-2	CEN EN 419 241-2: "Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing”
EN 319 401	ETSI EN 319 401 (v2.2.1): "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
EN 319 411-1	ETSI EN 319 411-1 (v1.2.2): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".
EN 319 411-2	ETSI EN 319 411-2 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".
EN 319 421	ETSI EN 319 421 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".
TS 119 431-1	ETSI TS 119 431-1 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev".

TS 119 441	ETSI TS 119 441 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services".
TS 119 511	ETSI TS 119 511: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques".
EN 319 521	ETSI EN 319 521 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".
EN 319 531	ETSI EN 319 531 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers".

TP-02-20-994-EN-N

ABOUT ENISA

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

ENISA
European Union Agency for Cybersecurity

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

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

enisa.europa.eu

ISBN: 978-92-9204-439-8
DOI: 10.2824/06258