EUROPEAN UNION AGENCY
FOR CYBERSECURITY

SECURITY FRAMEWORK FOR TRUST SERVICE PROVIDERS

Technical guidelines on trust services

MARCH 2021

ABOUT ENISA

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

CONTACT

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

CONTRIBUTORS

Olivier Barette (Nowina), 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: 978-92-9204-440-4 – DOI: 10.2824/36142

TABLE OF CONTENTS

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
QREMS	Qualified Registered Electronic Mail Service
RA	Registration Authority
REMS	Registered Electronic Mail Service
SB	Supervisory Body
TS	Trust Service
TSP	Trust Service Provider

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.

It is possible to use the output of 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 on the sole basis that they are electronic but have to assess them in the same way they would do for their paper equivalent.

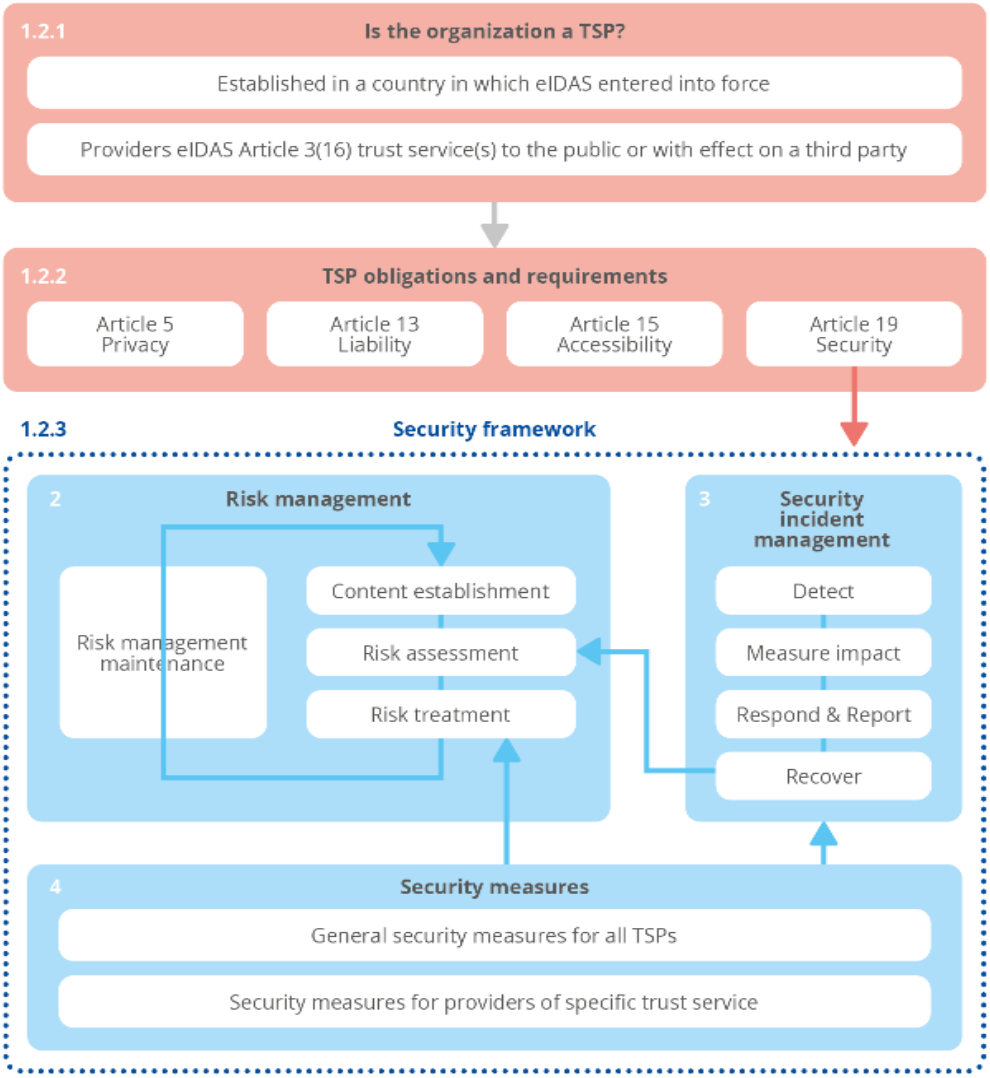
A natural or a legal person established in one of the Member States in which the Regulation entered into force and providing one or more of the eIDAS trust services is called a Trust Service Provider (TSP). A TSP is subject to eIDAS requirements and in particular to:

- Article 5 on data processing and protection;
- Article 13 on the liability of the TSP;
- Article 15 on accessibility for persons with disabilities; and
- Article 19 on security.

This document proposes a security framework to achieve compliance with Article 19 of the eIDAS Regulation. As illustrated below, this security framework includes specific guidelines for TSP on:

- **Risk management** related to the security of the eIDAS trust services and based on ISO/IEC 27005 general approach;
- **Security incident management** by using the appropriate measures to efficiently detect, measure the impact, respond, report, and recover from security incidents as part of the eIDAS Regulation;
- **Security measures** recommended to TSPs from “technical” standards and best practices to treat the risks and contribute to the security incident management. The level of security of these measures is to be selected by the TSP to be commensurate to the degree of risk bound to the context of the TSP (determined during the “context establishment”).

Figure 1: Structure of "Security Framework for Trust Service Providers" document



The Annex A illustrates the guidelines for the risk and security incident management presented in this document through practical examples.

This document can be used for guidance by TSPs that are interested in understanding their obligations as a consequence of being a TSP, in particular the required security framework to be implemented pursuant to Article 19 of eIDAS.

1. INTRODUCTION

1.1 THE ROLE OF ENISA

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

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

1.2 BACKGROUND ON EIDAS TRUST SERVICE PROVISIONING

1.2.1 Definitions of 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. It is possible to use the output of 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 on the sole basis that they are electronic but have to assess them in the same way they would do for their paper equivalent.

The eIDAS Regulation defines a trust service in Article 3(16) as "*an electronic service normally provided for remuneration which consists of:*

a. *the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or*
b. *the creation, verification, and validation of certificates for website authentication; or*
c. *the preservation of electronic signatures, seals or certificates related to those services."*

As such, eIDAS covers a limited and explicitly enumerated list[1] of trust services: the list of eIDAS trust services is a closed list[2].

A natural or a legal person established in one of the Member States in which the Regulation entered into force and providing one or more of the above trust services is called a Trust Service Provider (TSP). A TSP established outside of the European Union is not subject to the

[1] The present document has been drafted at the moment of the launch by the European Commission of the Open Public Consultation regarding the review of the eIDAS Regulation (Article 49). The outcomes in terms of update of the Regulation are not yet known and might include a review of this list of trust services.
[2] Member States may apply (and some Member States have actually used this possibility in practice) a similar trust framework to comparable categories of services providers, such as archiving service providers or digitization service providers, and may require such service providers to also follow the requirements of eIDAS. Such service providers can be considered as TSPs under those national laws, although it is worth noting that they are not TSPs as defined by eIDAS, and therefore also cannot benefit from an automatic legal recognition in other Member States under eIDAS.

obligations of the eIDAS Regulation (Article 2.1), nor can they benefit from legal equivalence to qualified service providers in the EU in the absence of an agreement between the Union and the country in question or with an international organisation (Article 14.1). However, since eIDAS not only regulate the TSPs themselves but also their services (even if the TSP is established outside of the EU), the legal value in the EU of their output (e.g. timestamp) or of artefacts based on their outputs (e.g. electronic signature) would still be assessed under the rules of eIDAS.

The eIDAS Regulation explicitly excludes its application to services used exclusively within closed systems between a defined set of participants, which have no effect on third parties (Article 2.2). Consequently, if a natural or legal person answers the following questions positively, they can be considered as an eIDAS TSP:

1. Is the person established in a country in which the eIDAS Regulation entered into force?
2. Does service provided comply with Article 3(16) definition of a trust service?
3. Is the service provided to the public or does it impact on a third party?

Based on these criteria, examples of TSPs include software companies that host one of their electronic signature solutions and private companies offering a signature platform to their customers[3]. Examples for non-TSPs are systems set up in businesses or public administrations making use of trust services to manage internal procedures.

Finally, a TSP is either '**qualified'** or '**non-qualified'**: a qualified TSP (QTSP) is a TSP that provides one or more qualified trust services (i.e. a sub-set of Article 3(16) trust service that meets the eIDAS applicable requirements) and is granted the qualified status by the supervisory body (SB). These notions of qualified trust services and QTSP have been introduced with a view to indicating requirements and obligations that guarantee a high level of quality and trustworthiness of whatever qualified trust services and products are used or provided.

For completeness, and to better understanding this document, it should be noted that a qualified trust service is not necessarily superior to a non-qualified service in terms of security and quality. The only clear difference is the level of guarantees provided to third parties: the compliance of a QTSP with the requirements of eIDAS and with recognised international standards has been independently assessed by a conformity assessment body (CAB), and it is independently monitored by a national supervisory body (SB). It is however perfectly possible for a non-qualified trust service (non-QTSP) to meet the same (or even higher) standards of quality and trustworthiness as a QTSP. As shown below, the level of security of a trust service, expected to follow 'best practices', is not necessarily lower than one of QTSP. The security framework will rather result from the context (business, sector) of the (Q)TSP and the related risks the (Q)TSP is ready to accept. For this reason, the security practices are relevant to both non-QTSPs and QTSP. The degree of strength of these practices may be influenced by the qualified status (see [ENISA Security Framework for QTSPs]).

1.2.2 Trust Framework

Although they do not explicitly apply to a qualified status, non-QTSPs still fall under eIDAS requirements as they are identified as TSP. Indeed, in order to ensure due diligence, inclusion, transparency, and accountability of the operations and services of both QTSP and non-QTSP, all TSPs are subject to a common set of requirements, in particular on:

- Data processing and protection, as defined in Article 5;
- Liability, as defined in Article 13;

[3] Arguments could also be made that trusted shop evaluators providing "verified valuations and valuation ranking" services may be considered as eIDAS TSPs issuing (non-qualified) certificates for website authentication (i.e. "WACs").

NOTE: Pursuant to Article 13.1, while both QTSP and non-QTSP are liable for damage caused to any natural or legal person, only the intention or negligence of the QTSP is presumed. Regarding non-QTSP, the burden of proving intention or negligence lies with the natural or legal person claiming the damage.

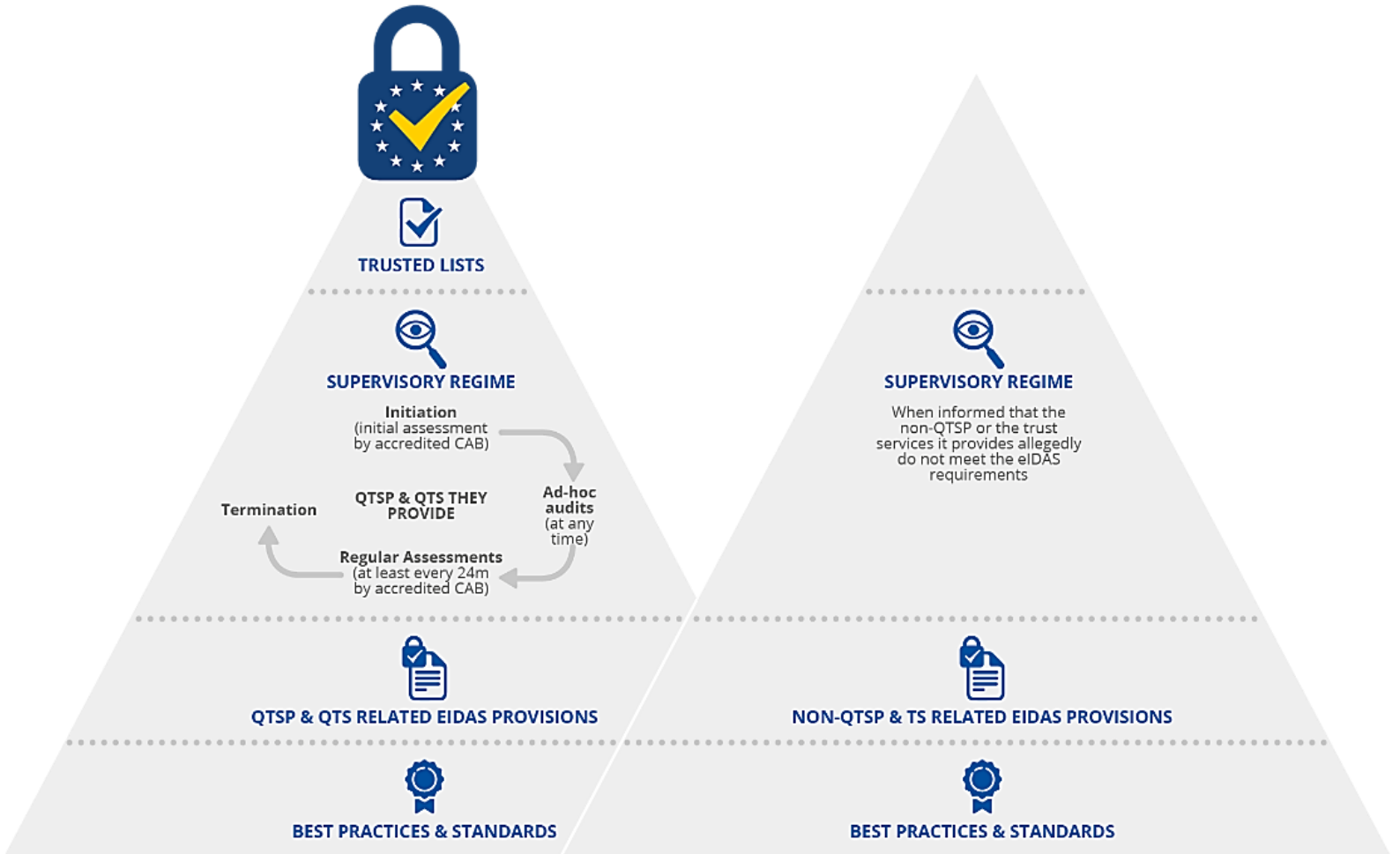
- Accessibility for persons with disabilities, as defined in Article 15; and
- Security, as defined in Article 19.1 and 19.2.

In line with one of the objectives of the eIDAS Regulation to enhance the trust of enterprises and consumers in the market and to promote the use of trust services, eIDAS establishes a supervisory regime for all TSPs to supervise the compliance of TSPs with the eIDAS requirements. The supervisory regime is however different for QTSP and non-QTSP:

- QTSPs and the QTSs they provide are subject to strict *ex ante* and *ex post* supervision model by a supervisory body (SB), making use of initiation, ad hoc, and regular audits by an eIDAS-accredited conformity assessment body (CAB).
- Non-QTSPs, on the other hand, 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 accredited 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 the above-mentioned articles of eIDAS.

These supervision models form the foundation of the trust framework as defined by eIDAS. It is actually setting up two distinct complete pyramids of trust, one for the QTSPs and the QTSs they provide and one for the non-QTSP and the TS they provide. These are are illustrated in Figure 2.

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



This trust framework implies for example that a non-QTSP is still subject to inquiry of the SB, and as a consequence should structure its activities and keep records to prove due diligence to the SB in case of such inquiry. This is why a sound security framework within eIDAS will draw a significant attention to evidence logs and tracing of activities.

1.2.3 Security Framework

As mentioned in the previous section, both QTSPs and non-QTSPs are subject to a common set of requirements. Focusing on security aspects, common requirements are defined in Article 19.1 and 19.2.

First, Article 19.1 states that:

> **ARTICLE 19.1**
> Qualified and non-qualified TSPs shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk.
>
> In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.

In other words, both QTSP and non-QTSP shall take appropriate **security measures** as part of:

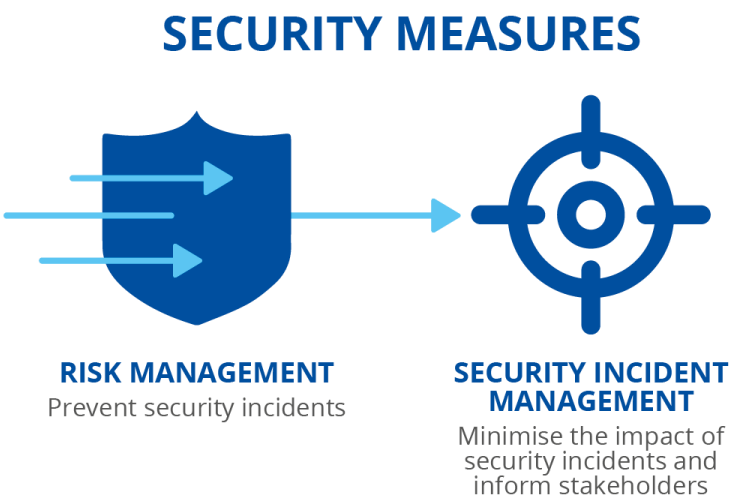
- **Risk management**: When risks have been identified and assessed relating to the context of the TSP, the TSP shall treat these risks (and thereby prevent security incidents) with appropriate measures. These measures are deemed appropriate if they ensure a sufficient level of security comparing to the degree of risk.
- **Security incident management**: In case of security incidents, the TSP must be prepared to efficiently minimise the impacts and inform the relevant stakeholders of such incidents.

As part of security incident management, Article 19.2 states that:

> **ARTICLE 19.2**
> Qualified and non-qualified TSPs shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.
>
> Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the TSP shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.
>
> *[Obligations for supervisory bodies]*

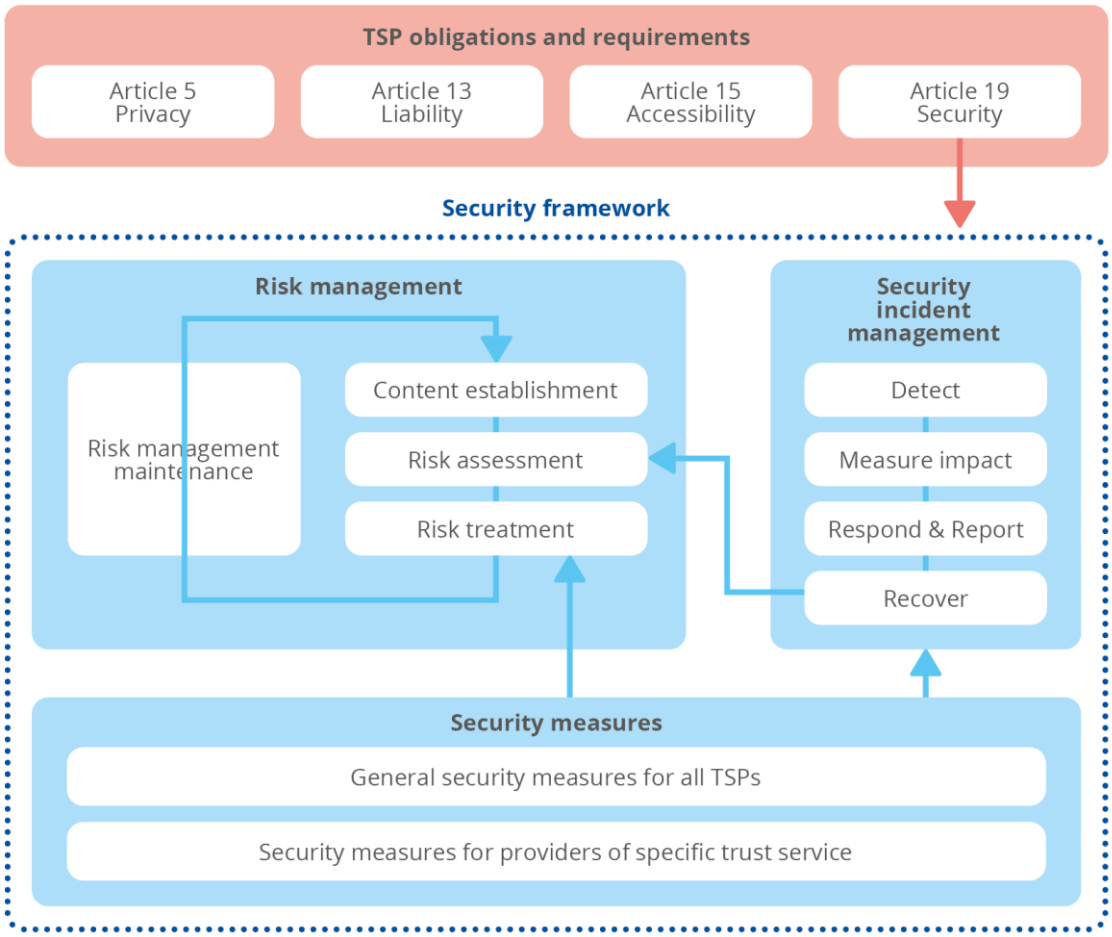
Relation between security measures, risk management, and security incident management can be illustrated as follows:

Figure 3: Security Framework for TSPs (high-level view)



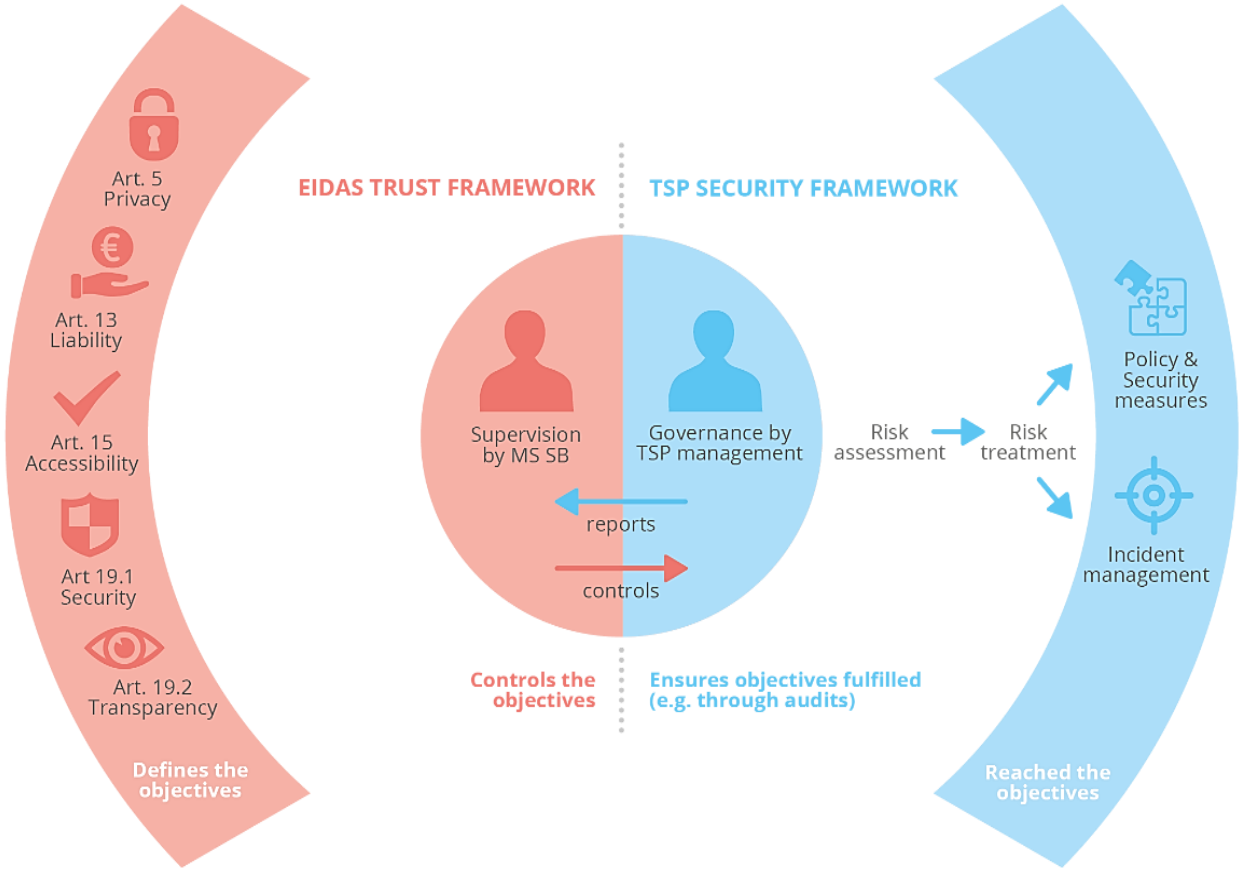
At a finer level of detail, related to the guidelines provided in this document, the security framework of TSP can be illustrated as follows:

Figure 4: Security Framework for TSPs (detailed view)



Related to the trust framework introduced in Section 1.2.2, the security framework applicable to TSP can be seen as a direct consequence of the trust framework defined by eIDAS and is managed within the eIDAS umbrella. This can be pictured as follows:

Figure 5: Relation between the trust framework and the security framework



On top of common security requirements for QTSP and non-QTSP, and as a consequence of the above articles, each trust service offered by trust providers, whether qualified or not, needs to address specific security requirements, reflecting state-of-the-art security practices.

1.3 TARGET AUDIENCE

The audience for this document is **service providers** who are interested in knowing their obligations as a consequence of being a TSP, in particular regarding Article 19. This audience may find in this document guidelines on how to reach a defined level of security, trustworthiness, and overall quality. It provides information on standardisation frameworks such as the ETSI Electronic Signatures and Infrastructures (ESI) 119/319 000 series on TSP/TS or the ISO 27000 series on Information Security Management Systems (ISMS).

This document may also be useful for **relying parties** willing to evaluate how compliant a TSP is with the eIDAS security requirements, and how aware they are of TSP obligations. As detailed in Sections 1.1.2 and 1.1.3 above, because the trust framework for non-QTSPs may be seen as lighter, reactive and ex post, further verification might be considered as important by a prospective client or a relying party before, respectively, entering into a contractual relationship, or more generally using the outcome of the corresponding trust services (e.g. certificates, timestamps, signatures, validation reports, etc.). For the same reason, on the other side of the relationship, the non-QTSPs may use this document to demonstrate that their compliance with the required security requirements. A typical way to make this demonstration is to publish

practice statements, describing the way the service is offered. Such documents can be built taking into account standards and guidelines referred in this report. By looking at these practice statements, clients and relying parties may assess the security of the services provided and their compliance with eIDAS.

Finally, as this document is the baseline for [ENISA Security Framework for QTSPs], this document is to be read along with the latter by **prospective QTSP and QTSP**.

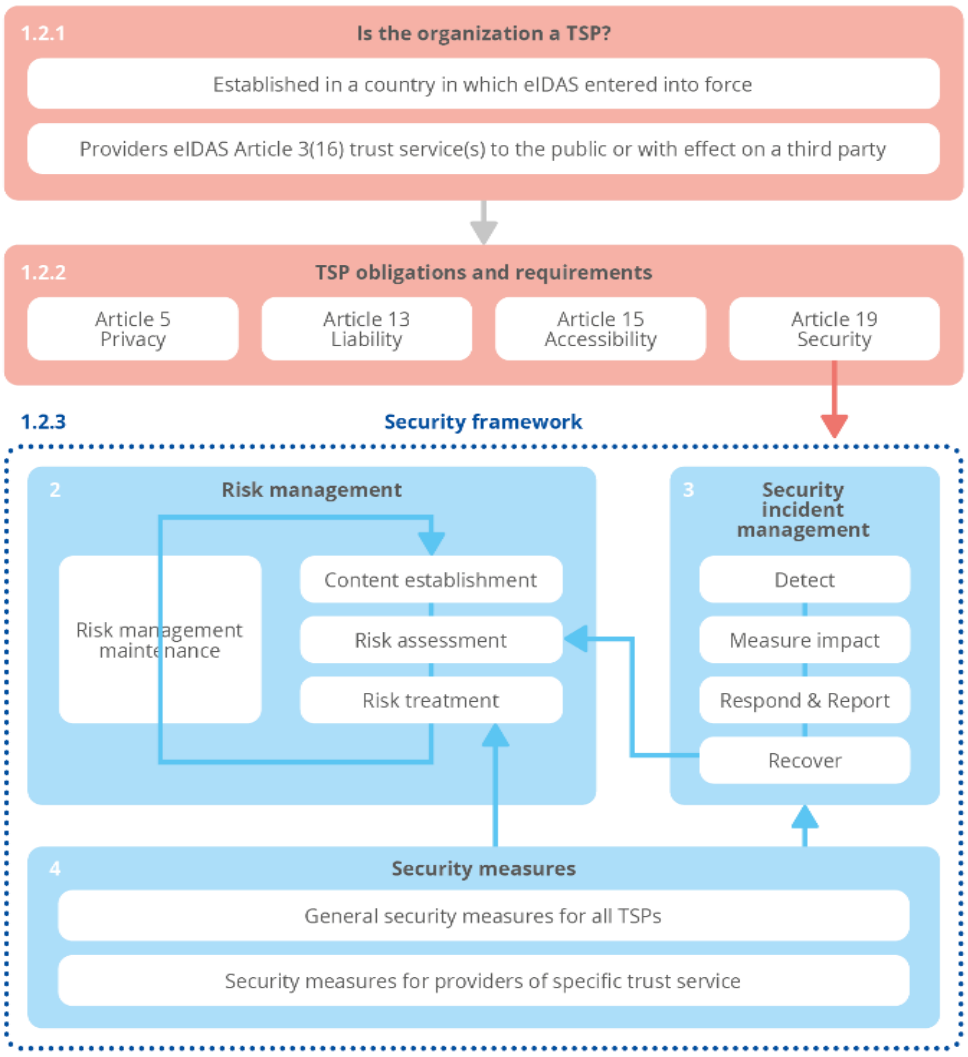
1.4 PURPOSE AND STRUCTURE OF THIS DOCUMENT

This document proposes a security framework based on guidelines for TSP, 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.

In particular, this document is structured as follows:

- **Section 2** "Risk management" aims at presenting specific and practical guidelines for TSP regarding the management of risks posed to the security of their trust services, pursuant to Article 19.1 and based on [ISO/IEC 27005] general approach.
- **Section 3** "Security incident management" presents guidelines supporting TSPs in fulfilling Article 19.1 and Article 19.2 by using the appropriate measures to efficiently detect, measure the impact, respond, report, and recover from security incidents.
- **Section 4** "Trust services security measures" proposes a list of security measures to support TSPs in treating the risks identified in Section 2 and security incident management proposed in Section 3. The proposed references come from "technical" standards & best practices to address the risks both in general (Section 4.1) and in relevance to the specific trust services provided (Section 4.2).
  NOTE: Additional security measures for QTSPs and the QTSs they provide are proposed in the [ENISA Security Framework for QTSPs], which is to be used in addition to the security measures listed in this document.
- **Annex A** provides examples which illustrate guidelines provided in Sections 2 and 3 of this document customised to a TSP issuing electronic certificates which is a trust service widely spread and well-known.

Figure 6: Structure of the 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[4] to eIDAS after following the said standards.

[4] 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.

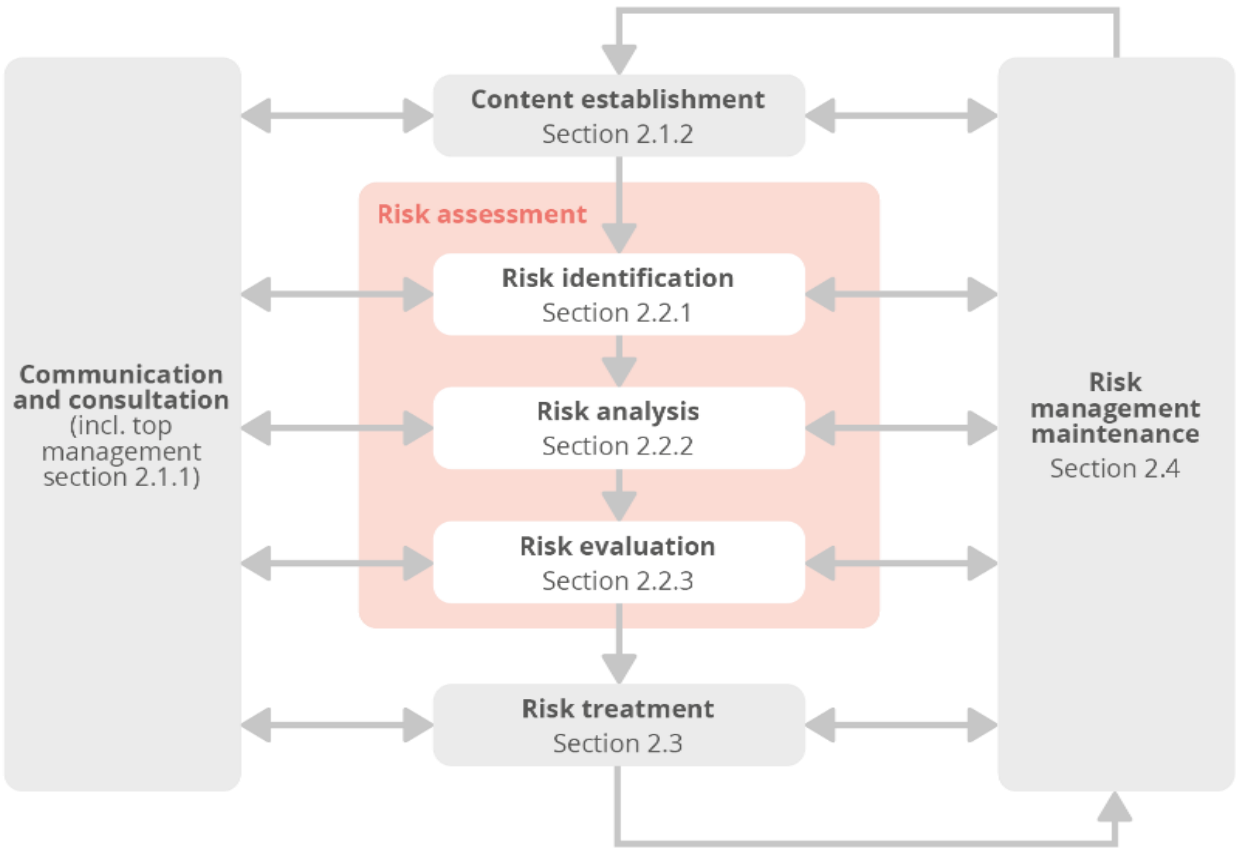
2. RISK MANAGEMENT

As mentioned in Section 1.2.3, the eIDAS Regulation requires that TSPs shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide and prevent the impact of security incidents. Having regard to the latest technological developments, those measures shall ensure that the level of security shall be 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 in particular the requirements of an information security management system (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, this document aims at presenting more specific and practical guidelines for TSP regarding the management of risks posed to the security of their trust services. The structure of this section is illustrated in Figure 7 and is driven by the structure of this standard. For more details on the different steps of this methodology, the TSP is suggested to consult [ISO/IEC 27005].

Figure 7: Risk management process (Source: [ISO/IEC 27005])



2.1 PREREQUISITES

Before diving into the risk assessment, it is important to establish the necessary framework for the management of risks. For this purpose, ENISA[5] recommends defining the basic assumptions for the organisation's external and internal environment and the overall objectives of the risk management process and activities. To perform such definitions, the involvement of the TSP's management is priorly required.

2.1.1 Management involvement

Standards and best practices state that:

- *"Top management shall demonstrate leadership and commitment with respect to the information security management system"* ([ISO/IEC 27001]).
- *"Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness*" ([ISO/IEC 27001]).
- "The TSP's *management shall approve the risk assessment and accept the residual risk identified*" ([EN 319 401]).

The involvement of top management is therefore highly recommended when assessing risks and should hence participate to all steps identified below, including the context establishment. These obligations aim to make risk management become part of the organisation's culture and philosophy.

2.1.2 Context establishment

An essential step recommended by ENISA[6] before performing the risk assessment, is to properly establish the context of the organisation. This includes:

- **Understanding the background** of the organisation and its risks (e.g. its core processes, valuable assets, competitive areas etc.) and in particular:
  - Defining the external and internal environment;
  - Identifying the scope and boundaries of the TSP, in particular the entities (e.g. certification authority, registration authority, validation authority, subjects, relying parties) and processes (e.g. registration, subject key management, revocation) involved in the provision of the trust services;
  - Clarifying and gaining common understanding of the organisation objectives.
- **Formulating the risk acceptance criteria** to evaluate the significance of a risk and to determine whether the risk is acceptable or tolerable. These criteria must be formulated in compliance with the background concluded above. Nevertheless, it should be noted that these criteria can be defined later during the risk management processes and can still be modified at any step of the process.

Article 19 requires the level of security underlying to the security measures taken by the TSP to be commensurate to the degree of risk. This degree of risk greatly varies depending on the context of the TSP (e.g. provided services and their criticality in terms of availability, integrity, and availability). In that respect, the result of risk assessment of two TSPs, e.g. two TSPs providing different services or two TSPs providing the same service but to different types of customers, tend to be different. The same applies to the result of the risk treatment and the selection of underlying security measures, as a direct consequence of the result of the risk assessment and the decided aforementioned risk acceptance criteria. In comparison with a QTSP, depending on the established context, a non-QTSP may require a similar, lower, or even

[5] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/crm-strategy/scope-framework
[6] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/crm-strategy/scope-framework

higher level of security (e.g. a TSP issues certificates used to sign major financial transactions). Regarding QTSPs, it shall however be noted that the burden of proof in case of claimed damages is on the QTSP (Article 13) and this may influence their security framework. [ENISA Security Framework for QTSPs] provides guidance and information in this regard.

More information on the context establishment can be found in clause 7 of [ISO/IEC 27005], clause 4 of [ISO/IEC 27001], and ENISA documentation on threat and risk management[7].

2.2 RISK ASSESSMENT

This section guides the reader on how to carry out a risk assessment to identify, estimate, and evaluate trust service risks taking into account business and technical issues. This section does not describe in detail the different existing methods but provides guidance on how to conduct a risk assessment on a TSP, based on [ISO/IEC 27005] methodology.

Following this methodology, the risk assessment process can be divided into the following phases:

1. **Risk identification:** Identifying the different factors, i.e. assets, threats, vulnerabilities, existing controls, and consequences, that will identify and evaluate the risks.
2. **Risk analysis:** Determining the risk level based on the impact of each incident scenario and their likelihood of occurrence.
3. **Risk evaluation:** Producing a scored list of all the identified risks, based on the risk analysis results, business criteria, affected assets, their vulnerabilities, and potential threats.

2.2.1 Risk identification

[ISO/IEC 27005] states that *"the purpose of risk identification is to determine what could happen to cause a potential loss, and to gain insight into how, where and why the loss might happen"*. This may be achieved with:

1. **Identification of assets**, i.e. valuable items to the TSP;
2. **Identification of threats**, i.e. all agents, either natural or human-made, accidental or intentional, internal or external, that could pose a threat to the organisation;
3. **Identification of vulnerabilities**, i.e. potential weaknesses in the organisation that could facilitate a successful attack and cause damage to the assets;
4. **Identification of existing security controls** implemented by the TSP to address the vulnerabilities;
5. **Identification of consequences** that different events could have on the organisation.

It is important to note that this process has to be systematic and comprehensive enough to ensure that no risk is unwittingly excluded. It is very important that during this stage all risks are identified and recorded, regardless of the fact that some of them may already be known and likely controlled by the organisation.

Good quality information and thorough knowledge of the organisation and its internal and external environment (identified in Section 2.1.2 "Context establishment") are very important in identifying risks. Historical information about this for similar organisations (competitors or not) may also prove to be very useful as they can lead to safe predictions about current and evolving issues that have not yet been faced by the organisation.

2.2.1.1 Identification of assets

An asset is defined in [ISO/IEC 27005] as *"anything that has value to the organization, and which therefore requires protection"*. Assets are not only physical or tangible items but can also

be information or business processes. In fact, [ISO/IEC 27005] suggests distinguishing two types of assets:

- **Primary assets** that can business processes (or activities) and information.
- **Secondary/supporting assets**, on which the primary assets rely. These secondary assets are usually physical and tangible assets such as: hardware, software, network, personnel, location and sites, or other assets (e.g. TSP reputation, trust relationship, customer base).

Examples of primary and secondary assets for a TSP issuing certificates can be found in Annex A. Annex D of [ENISA Article 19 incident reporting] also provides examples of assets for the eIDAS trust services.

It should be noted that the asset identification can be performed with different level of details. This level of detail greatly affects the amount of information that will be available for the risk assessment. Therefore, a primary asset can be as simple as the trust service provided (as a whole) by the TSP. The TSP may also decide to split the trust service in several primary assets comprising business processes (e.g. registration process, key pair generation, storage, backup, and recovery, private key destruction, revocation process) and information (Root CA certificate, subjects' private keys, registration archives, CRL).

Pursuant to Article 13 of eIDAS on liability, assets related to evidence (e.g. records, audits) are particularly important to demonstrate due diligence of (Q)TSP in case of damage or litigation. In particular, when a natural or legal person claims damage and blames a non-QTSP for it, the burden of proving intention or negligence of the non-QTSP lies with the person claiming the damage. But, in the case of a QTSP, its intention or negligence is presumed unless it proves that the damage occurred without intention or negligence. It is therefore highly recommended in this document to attach high importance on the **collection** and **protection** of the records and other elements that can be used as evidence in case of litigation.

[ISO/IEC 27005] suggests associating an owner to the assets. This would enable to determine who has the final responsibility for the protection and maintenance of that asset.

Guiding example (on "CA key pair generation" asset)

In the case of a TSP issuing certificates, an example of a primary asset may be the CA key pair generation (taken from Annex A examples). If the confidentiality of the CA private key is compromised, a malicious individual could impersonate the CA and generate fraudulent certificates. This asset will be used throughout this document as the guiding example for the risk assessment examples.

Table 1: Example of asset "CA key pair generation"

Asset name	Asset owner
CA key pair generation	Security officer

2.2.1.2 Identification of threats

A threat is defined in [ISO/IEC 27005] as "*potential cause of an unwanted incident, which can result in harm to a system or organization*". In other words, a threat is a potentially harmful occurrence. It can be accidental or intentional, human-made or natural, internal or external, technical or physical.

It should be noted that some threats may affect more than one asset. A threat may cause different impacts depending on which assets are affected. This will be further covered in the next sections.

This identification of threats may be obtained from the asset owner, the different departments of the organisation (e.g. human resources, infrastructure, legal) that may already have experience incidents, or the national organisations (e.g. authorities, insurance companies, national government authorities).

The TSP may consult existing threat catalogues and statistics available from industry bodies, national governments, insurance companies, standardisation bodies. For instance, the French National Cybersecurity Agency (ANSSI) provides EBIOS which notably provides a study of threat sources. Another relevant source is the annual analysis report on the trust services security incidents (with regards to Article 19 of eIDAS)[8]. All trust services security incidents can also be visualized via the CIRAS visual tool[9] provided by ENISA.

Annex A of this document, providing potential threat for TSPs issuing certificates, can also be consulted for specific examples along with Annex C of [ISO/IEC 27005] providing more general examples of threats.

It is important to note that threats may change over time. It is hence suggested to regularly reconsider the past identified threats.

Guiding example (on "CA key pair generation" asset)

Using the example above with asset "CA key pair generation", one may associate to this asset two potential threats (taken from Annex A examples), as illustrated below. It has been decided here to associate the threat directly to the asset.

Table 2: Example of potential threat for "CA key pair generation" asset

Asset name	Potential threats
CA key pair generation	Cryptanalysis
	Theft or loss of data

[8] https://www.enisa.europa.eu/news/enisa-news/annual-report-on-trust-services-security-incidents-in-2019
[9] https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

2.2.1.3 Identification of vulnerabilities

A vulnerability is defined in [ISO/IEC 27005] as a "*weakness of an asset or control that can be exploited by one or more threats*". Identified vulnerabilities must have a corresponding threat. A vulnerability with no associated threat may not result in a risk.

Identifying possible vulnerabilities is a key step in risk management, as they constitute the possible weaknesses of an asset or group of assets (e.g. all assets related to personnel) that can be exploited by one or more threats.

Similarly to threats, the TSP may consult existing vulnerability catalogues and statistics available from industry bodies, national governments, insurance companies, standardisation bodies. Annex D of [ISO/IEC 27005] provides examples of typical vulnerabilities. Annex A of this document also proposed potential vulnerabilities for TSPs issuing certificates.

Guiding example (on "CA key pair generation" asset)

Using the "CA key pair generation" example, four vulnerabilities have been associated with the identified threats (taken from Annex A examples).

Table 3: Example of vulnerabilities for "CA key pair generation" asset

Asset name	Potential threats	Vulnerabilities
CA key pair generation	Cryptanalysis	Key is generated with a weak algorithm or insufficient key length
		Usage of insecure or weak random number generator
	Theft or loss of data	Key is generated in a non-secure physical or logical environment
		Key generation is not performed by trusted individuals

2.2.1.4 Identification of existing security controls

The list of potential vulnerabilities should be contrasted with the list of existing controls. Existing controls are the means of mitigating the likelihood of exploiting potential vulnerabilities as they decrease the level of exposure. The TSP should conduct a gap analysis regarding the trust service(s) it provides in order to determine for which vulnerabilities no sufficient controls are in place.

The controls that are planned to be implemented (as part of an already defined risk treatment plan) should be considered as existing controls.

The gap analysis should be an input to conduct the risk calculation. The likelihood of an incident scenario taking place is decreased by controls put in place to mitigate vulnerabilities.

It may be possible that, at the time of the first risk assessment performed by the TSP, no existing control currently exists for a given vulnerability. Defining which vulnerabilities require controls may be decided when evaluating the risk (see Section 2.2.3).

The identification of existing security controls can alternatively be performed before the identification of the vulnerability, as suggested by [ISO/IEC 27005].

Guiding example (on "CA key pair generation" asset)
Using the "CA key pair generation" example, existing controls (defined for illustration purposes in Table 4) have been associated with the identified vulnerabilities.

Table 4: Example of existing controls for "CA key pair generation" asset

Asset name	Potential threats	Vulnerabilities	Existing controls
CA key pair generation	Cryptanalysis	Key is generated with a weak algorithm or insufficient key length	Key pair is generated with RSA-768[10].
		Usage of insecure or weak random number generator	Key pair is generated with a self-made random number generator.
	Theft or loss of data	Key is generated in a non-secure physical or logical environment	Key pair is generated in restricted area on a workstation disconnected from the Internet.
		Key generation is not performed by trusted individuals	Key pair is generated by the security officer and a trustworthy person independent of the TSP's management as witness (i.e. Notary).

2.2.1.5 Identification of consequences

In this document, a consequence (or impact) is defined as the result of the exploitation of a vulnerability of an asset by a threat. In particular, the purpose of the identification of consequences is, according to [ISO/IEC 27005], to identify "*the consequences that losses of confidentiality, integrity, and availability may have on the assets*".

Before identifying the potential consequences that an incident scenario may have on a TSP and its assets, the TSP may beforehand establish a list of potential incident scenarios that may occur. Annex A provides examples of incident scenarios that may occur for a TSP issuing certificates. Examples of security incidents are also provided in Annex C of [ENISA Article 19 incident reporting].

For a TSP, loss of confidentiality, integrity, and availability on an asset may have operational consequences, legal consequences, financial consequences, reputational consequences, or human consequences. For each incident scenario that may affect an asset, the TSP may therefore think about the different consequences on each of the aforementioned categories.

Particular attention must be paid to legal consequences and in particular on assets related to personal data. The eIDAS Regulation requires in Article 5.1 that "*processing of personal data shall be carried out in accordance with Directive 95/46/EC*". Directive 95/46/EC is now replaced by the 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", known as the General Data Protection Regulation (GDPR). TSPs are hence subject to GDPR requirements. Compliance with GDPR (and associated guidance) is a subject on its own and is hence outside of the scope of this document. Further information on this topic may be found for instance in ENISA documents specific to this area[11]. More information on Article 5 can be found in [ENISA Recommendations for QTSPs based on standards].

[10] The choice of a weak algorithm is deliberate for the purpose of illustration in the risk analysis.
[11] https://www.enisa.europa.eu/topics/data-protection

Annex A of this document suggests potential consequences that can have an incident scenario on a TSP issuing certificates.

Guiding example (on "CA key pair generation" asset)
Using the "CA key pair generation" example, loss of confidentiality could lead to an issuance of fraudulent subjects' certificates, which could be used to impersonate these subjects. This impersonation could be used to intercept private communications or forge electronic signatures. Such an incident has in particular consequences on the operations (relying parties must be informed, CA certificates and all issued certificates must be revoked, new certificates must be issued…), finances (e.g. due to a loss of clients), and the reputation.

2.2.2 Risk analysis

The previous section provided guidelines on how to identify all parameters that influence the risk calculation, i.e. assets, threats, vulnerabilities and existing controls, and consequences. The TSP should now have enough information to start the risk analysis process.

A risk analysis is defined in [ISO/IEC 27005] as the "*process to comprehend the nature of risk and to determine the level of risk*".

This analysis must also take into account special circumstances under which assets may require additional protection, such as with regulatory compliance. During this phase of the risk assessment, the TSP will use all the identified sources to estimate the risk, in terms of impact and likelihood. Information used to estimate impact and likelihood usually comes from[12]:

- Past experience or data and records (e.g. incident reporting);
- Reliable practices, international standards, or guidelines;
- Market research and analysis;
- Experiments and prototypes;
- Economic, engineering, or other models;
- Specialist and expert advice.

This phase comprises:

1. **Estimation of the level of impacts** that identifies consequences may have on assets;
2. **Estimation of the likelihood of occurrence**, or the estimation of the likelihood of the exploitation of a vulnerability on an asset by a threat;
3. **Estimation of the level of risk**, based on the computed level of impacts and likelihood of occurrence.

These estimations may be performed in varying degrees of detail depending on the criticality of assets and the associated risks. Depending on the degree pursued by the TSP, estimations can be done using different methodologies: qualitative analysis, quantitative analysis, and semi-quantitative analysis[13].

2.2.2.1 Estimation of the level of impacts

Section 2.2.1.5 proposed a way to identify the consequences that losses of confidentiality, integrity, and availability may have on the assets, due to the exploitation of a vulnerability by a threat. This step estimates the level of impacts such consequences have on the TSP if this exploitation materializes.

[12] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/risk-assessment
[13] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/risk-assessment

This estimation can be done via qualitative, semi-quantitative, or quantitative analysis. If the TSP performs a qualitative analysis, it should beforehand define the scale of level of impacts. It can use digits (1 to 5) or levels (low, medium, high).

A level of impact can be estimated based on the analysis of different types of consequences. Section 2.2.1.5 proposed the following types of consequences: operational, legal, financial, reputational, and human.

Guiding example (on "CA key pair generation" asset)
Regarding the "CA key pair generation" example, we mentioned that loss of confidentiality may have:

- Operational consequences (relying parties must be informed, CA certificates and all issued certificates must be revoked, new certificates must be issued). Using qualitative methodology, the TSP may attribute a level of impact on the operations of 5/5, given that such incident has a disastrous impact on the continuity of the operations: the entire organisation and all certificates may be affected.
- Financial consequences (e.g. due to a loss of clients, operational costs). Using qualitative methodology, the TSP may attribute a level of impact on the operations of 4/5.
- Reputational consequences. Using qualitative methodology, the TSP may attribute a level of impact on the operations of 4/5.

After this analysis, the TSP may estimate the level of impact on the asset "CA key pair generation" to 5/5, because it is the highest attributed score (the TSP may decide to compute the level of impact differently). The TSP may also split the level of impact in terms of loss of confidentiality, integrity, and availability and attribute a different score for each of them.

Table 5: Example of level of impact for "CA key pair generation" asset

Asset name	Impact (1-5)	Potential threats	Vulnerabilities
CA key pair generation	5	Cryptanalysis	Key is generated with a weak algorithm or insufficient key length
			Usage of insecure or weak random number generator
		Theft or loss of data	Key is generated in a non-secure physical or logical environment
			Key generation is not performed by trusted individuals

2.2.2.2 Estimation of the likelihood of occurrence

The estimation of the likelihood of occurrence can be seen as the likelihood of the exploitation of a vulnerability on an asset by a threat.

It is then suggested in this document to estimate, using the qualitative, semi-quantitative, or quantitative analysis:

- The probability of occurrence of identified threats;
- The vulnerability level of the identified vulnerabilities, depending on the identified existing controls (reducing the exposure to the vulnerabilities).

Taking into account all these parameters, each incident scenario should be assigned a likelihood score.

Guiding example (on "CA key pair generation" asset)

Using the "CA key pair generation" example:

- Threat "*Cryptanalysis*" has been assigned a 2/4 score because such a threat requires a high level of knowledge.
    - Vulnerability "*Key is generated with a weak algorithm or insufficient key length*" has a 4/5 score because the identification of existing control states that "*Key pair is generated with RSA-768*", that is not recommended at the time being as key length for a CA key pair generation.
    - Vulnerability "*Usage of insecure or weak random number generator*" has a 3/5 score because the identification of existing control states that "*Key pair is generated with a self-made random number generator*", that may have security flaws.
- Threat "*Theft or loss of data*" has been assigned a 3/4 score because theft does not require a high level of knowledge but still require access to the asset.
    - Vulnerability "*Key is generated in a non-secure physical or logical environment*" has a 3/5 score because the identification of existing control states that "*Key pair is generated in restricted area on a workstation disconnected from the Internet*" but may be accessed by external personnel (e.g. cleaning service).
    - Vulnerability "*Key generation is not performed by trusted individuals*" has a 1/5 score because the identification of existing control states that "*Key pair is generated by the security officer and a trustworthy person independent of the TSP's management as witness (i.e. Notary)*", that may be considered as a sufficient control.

Table 6: Example of likelihood of occurrence for "CA key pair generation" asset

Asset name	Impact (1-5)	Potential threats	Prob. (1-4)	Vulnerabilities	Vuln. level (0-5)
CA key pair generation	5	Cryptanalysis	2	Key is generated with a weak algorithm or insufficient key length	4
				Usage of insecure or weak random number generator	3
		Theft or loss of data	3	Key is generated in a non-secure physical or logical environment	3
				Key generation is not performed by trusted individuals	1

2.2.2.3 Estimation of the level of risk

Risk estimation is based on the estimated level of impacts and likelihood of occurrence.

In this document, the following formula will be used:

$$Risk = Threat \times Vulnerability \times Impact$$

Different weighting scores can be assigned to the assigned impact/likelihood pair of each incident scenario (e.g. *Threat* and *Vulnerability* can be summed up, instead of multiplied).

Guiding example (on "CA key pair generation" asset)

Using the "CA key pair generation" example, the following risk levels have been computed:

Table 7: Example of level of risk for "CA key pair generation" asset

Asset name	Impact (1-5)	Potential threats	Prob. (1-4)	Vulnerabilities	Vuln. level (0-5)	Risk level
CA key pair generation	5	Cryptanalysis	2	Key is generated with a weak algorithm or insufficient key length	4	40
				Usage of insecure or weak random number generator	3	30
		Theft or loss of data	3	Key is generated in a non-secure physical or logical environment	3	35
				Key generation is not performed by trusted individuals	1	15

2.2.3 Risk evaluation

During the risk evaluation phase, decisions have to be made concerning which risks need treatment and which do not, as well as concerning the treatment priorities. Such evaluation is based on the previously computed estimation of the level of risk.

In this phase, the TSP compares the level of risks against the risk acceptance criteria, in order to evaluate the significance of the risks and to determine whether they are acceptable or tolerable. These risk acceptance criteria may have been determined during the context establishment (see Section 2.1.2).

2.3 RISK TREATMENT

This section provides guidelines on how to select the appropriate risk treatment measures, taking account of the risk assessment results, while ensuring that the level of security is commensurate to the degree of risk.

According to its definition, the "risk treatment" phase is the process of selecting and implementing measures to modify risk. Risk treatment measures usually are:

- **Acceptance**: Some risks may be accepted, meaning that the asset will remain unprotected against a specific risk. The TSP may decide to not protect the asset to save effort and money.

[ISO/IEC 27005] suggests that the list of all accepted risk with the justification that they do not meet the TSP's normal risk acceptance criteria should be formally accepted by the TSP's top management.

- **Reduction** (or mitigation): The TSP decides to lower the risk to an acceptable level. Measures suggested to be implemented by a TSP are provided by ETSI standards. These measures are further detailed in Section 4.
  It should be noted that after the risk reduction, aiming at decreasing the previously computed vulnerability levels, there will still be a residual risk; The zero risk is hardly achievable.
- **Transfer**: The TSP may decide to transfer the risk to another entity facing the same risk (e.g. insurance company).
- **Avoidance**: Finally, the TSP may decide to avoid the risk by stopping, postponing, or cancelling the activity that may be the cause for that risk. Such kind of activity may be a non-mandatory but valuable feature to the trust service it already provides but with strong requirements or obligations.

Detailed information on the risk treatment and risk acceptance is provided by ENISA on its website[14]. More information can also be found in clauses 9 and 10 of [ISO/IEC 27005].

Guiding example (on "CA key pair generation" asset)

For instance, using the "CA key pair generation" example, the TSP decided to reduce the risk. It may refer to [EN 319 411-1] and in particular clause 6.5.1 on "Key pair generation and installation" to reduce the previously identified risks. After implementing these controls, the TSP may estimate the previously computed vulnerability levels to 1/5 and may thereby greatly decrease the previously computed levels of risk.

2.4 RISK MANAGEMENT MAINTENANCE

In order to ensure the efficiency and effectiveness of risk management, it is essential to establish an ongoing review and monitoring process. This way, the TSP can ensure the actions decided based on the risk treatment remain relevant and up-to-date. Such a process is particularly relevant in today's continuously changing business environment where factors affecting the likelihood and consequences of risks are very likely to change.

In this regard, [EN 319 401] states that "*the risk assessment shall be regularly reviewed and revised*". It is up to the TSP to decide when such a review and revision must be performed. It is however suggested in this document to do it:

- Every year, e.g. as part of an internal audit (e.g. internal audit as defined in [ISO/IEC 27001]);
- When a significative change occurs to the context of the TSP that has been previously established (see Section 2.1.2);
- When a breach of security occurs (further covered in Section 3).

More information on the risk management maintenance can be found in clause 12 of [ISO/IEC 27005] .

[14] Risk treatment: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment
Risk acceptance: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/risk-acceptance

3. SECURITY INCIDENT MANAGEMENT

The previous section presented, based on [ISO/IEC 27005], specific and practical guidelines for TSP regarding the management of risks posed to the security of their trust services, as required by the first part of Article 19.1 of eIDAS:

> **Article 19.1:** *Qualified and non-qualified TSPs shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents* […]

Managing the risk is not enough to fully comply with Article 19 of eIDAS as it also requires managing security incidents. Applicable requirements and obligations are laid down in the remainder of Article 19.1 and in Article 19.2 of eIDAS:

> **Article 19.1:** […] *In particular, measures shall be taken to* […] *inform stakeholders of the adverse effects of any such incidents.*
>
> **Article 19.2:** *Qualified and non-qualified TSPs shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.*
>
> *Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the TSP shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.*
>
> […]

In other words, in case of **security incident** (breach of security or loss of integrity – examples of incident scenario for a TSP issuing certificates are provided in Annex A) that has a **significant impact** on the trust service(s) provided or on the personal data maintained therein, the QTSP or non-QTSP shall without undue delay:

- In any event within 24 hours after having become aware of it:
  - Notify the supervisory body; and
  - Where applicable, notify other relevant bodies, such as the competent national body for information security or the data protection authority;
  - Notify the natural or legal person to whom the trusted service has been provided of the breach of security or loss of integrity, where this breach is likely to adversely affect this person.

This section presents guidelines supporting TSP in fulfilling the second part of Article 19.1 and Article 19.2 by using the appropriate measures to efficiently **detect**, **measure**, **respond**, **report**, and **recover** from security incidents.

Figure 8: Security incident management

NOTE**:** One of the most important phases for responding to an incident in any kind of ICT service is to prepare beforehand all the procedures and necessary information to be able to detect, respond, and recover quickly and effectively if an incident takes place. In particular, an appropriate policy is an instrument to prepare and to provide notice to service users and supervisory authorities. In this regard, this section provides, highlighted in the tables below, recommendations on security incident management for TSPs.

These recommendations can be read along requirements specified in clause 7.9 of [EN 319 401] on incident management for trust services providers. [TSP Technical Best Practices], developed by representatives of Apple, Google, Microsoft, and Mozilla, also provides guidelines on incident handling for TSP issuing SSL certificates and looking for their recognition by browsers.

3.1 DETECT INCIDENT

Detection of an incident may be triggered by different events and can be detected by staff in the internal systems or even by media and public sources. During the detection phase, the TSP first response line should determine whether an incident is actually taking place. Also, there should be a review process to assure that no incident slipped through due to a wrong assessment. If the TSP first response line assesses an incident is occurring, the next phase is the incident analysis, which will determine the type of incident (e.g. fraudulent certificate activities) and execute the appropriate response plan.

Before the security incident occurs, the TSP must be prepared to detect it. lists recommendations for that purpose.

Such recommendations will help the TSP to detect security incidents. In this regard, Annex A proposes examples on how a TSP issuing certificates may detect security incidents related to the nature of the service it provides. Requirements specified in clause 7.9 of [EN 319 401] on incident management can also be used as recommendations by the TSP.

Table 8: Recommendations for security incident detection

Rec. ID	Recommendations
REC-3.1-1	**Enable means to gather alerts**
	Enable outside parties to report incidents Incidents in TSPs may in many cases be detected by certificate holders, relying parties or any other outside party. They should be able to easily report suspicious activity associated to certificates issued by the TSP. The TSP should establish a support line or helpdesk where any information regarding suspicious activity can be received.
	Enable systems for staff to report abnormal events Not all incidents will arrive from outside the TSP, for example suspicious log activity will be detected by the TSP personnel. The TSP should provide means for them to register any incidence in a standardized format so that incident management personnel can respond more effectively.

	Follow alert systems from external sources Suspicions of compromises of trust services or cryptographic algorithms, parameters, protocols, and implementations may be published (e.g. in the Internet) even before the TSP is aware. The TSP should follow security alert systems, forums, threat intelligence sources and be aware of the latest threats.
	Activate alerts in internal systems The TSP should establish an adequate level of logging in all information systems, revise logs periodically, and enable systems that alert personnel when suspicious activities appear in systems logs.
	Conduct continuous self-monitoring and self-testing The TSP should foster a culture of self-monitoring and self-testing. This includes actively trying to break their own systems by all available means such as vulnerability assessment, penetration testing, and red teaming. Whenever indicated, an alarm should be raised through the established channels.

3.2 MEASURE INCIDENT IMPACT

Once the incident has been detected, the TSP personnel should assess the circumstances of the breach, the information systems affected and all other relevant information to determine the type of breach and its impact.

The purpose of this section is to determine whether the security incident has a significant impact on the trust service and whether it has an adversely affect a natural or legal person to whom the trusted service has been provided. Based on this determination, the TSP may be able to decide if the security incident requires to be notified to the authorities mentioned in Article 19.

In order to determine the significance of a security incidents, a severity may be assigned to them. [ENISA Article 19 incident reporting] suggests the following scale:

1. **No impact**;
2. **Insignificant impact**: provider assets were affected but no impact on core services;
3. **Significant impact**: part of the customers/services is affected;
4. **Severe impact**: large part of the customers/services is affected;
5. **Disastrous**: the entire organisation, all services, all customers are affected.

[ENISA Article 19 incident reporting] further details this scale with numerous examples in Section 4.2.1.

3.3 RESPOND AND REPORT INCIDENT

An effective and prompt response is critical for mitigating the impact of a breach. Depending on the impact of the breach, mitigating the impact of a breach also requires reporting it to the appropriate authorities and to the public.

ENISA gathers all relevant documentation on incident reporting on their website, accessible via https://www.enisa.europa.eu/topics/incident-reporting. In particular, ENISA provides the Cybersecurity Incident Report and Analysis System (CIRAS) visual analysis tool[15] which proposes key statistics on incidents reported by competent authorities to ENISA and the Commission.

3.3.1 Before the incident

Before the security incident occurs, the TSP must be prepared to respond and report the incident. For this purpose, this document recommends the following:

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

Table 9: Recommendations for security incident response

Rec. ID	Recommendations
REC-3.1-2	**Create an incident response capability[16]**
	Create an incident response team TSPs should have an incident response team. Different configurations and capabilities of an incident response team exist, the TSP should define it according to its characteristics and their risk assessment. Amongst the questions to answer are: • Whether a 24x7 incident response capability is needed (which seems appropriate for revocation services at least). • The size of the team, whether they will be part-time or full time, and the required skills of the personnel. • Whether central incident management response or distributed incident response is applied.
	Create incident response procedures After determining different incident types that may occur, the TSP should define procedures for incident management. Having ready procedures will improve and speed up response when dealing with an incident. This should also include realistic response drills.
REC-3.1-3	**Prepare staff and systems for an incident**
	Assign roles and responsibilities Have an updated list of roles and responsibilities of staff in case of an incident. This applies not just to those directly involved in managing the incident, but for all personnel operating CA functions. All personnel should have clear instructions on how to proceed in case of an incident affecting their functions.
	Personnel training and awareness Conduct incident response awareness and exercises periodically in order for the involved staff to be able to handle incidents properly.
	Put redundancy or fail-safe mechanisms in place Have (cold or hot) standby systems in place to take over the duties of the main system in case of an incident. Consider applying fail-safe cryptographic modules, mechanisms such as forward secure signatures and/or utilizing fundamentally different crypto modules in parallel.
REC-3.1-4	**Have means of communication with all stakeholders**
	Create a repository of certificate holders contact information The TSP should establish, if appropriate according to local legislation and field of use, a database of issued certificates with the contact information of all the certificate holders and keep it updated. This will speed up the process of contacting them in case an incident takes place with their certificate.
	Create a repository of relying parties The TSP should establish a database with contact information regarding (known) relying parties (or their representatives) that use their certificates, such as government sites or trust stores for web browsers, in order to facilitate the process of contacting them if an incident takes place.
	Create a repository of supervisors and competent authorities The TSP should establish a database with contact information regarding supervisors and competent authorities and appropriate communication channels. As required by the eIDAS Regulation, qualified and non-qualified TSPs have to inform the supervisory authorities of any security incident affecting the service without undue delay. Additionally, the TSPs need to inform data protection authorities and under certain conditions data subjects when personal data are breached. It is also advisable to have contacts with competent CERTs. Knowing the appropriate channels for communication will facilitate the process if an incident occurs.

[16] https://www.enisa.europa.eu/topics/national-csirt-network

3.3.2 After the incident

When a security incident occurs, the TSP should carry on the incident response procedures previously defined (see REC-3.1-2). It is essential to note that, from the moment an event is classified as an incident, all evidence should be preserved in case it will be needed at a further stage.

Regarding the notification of the incident, Article 19.2 of the eIDAS Regulation states that TSP shall, within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any security incident that has a significant impact on the trust service provided or on the personal data maintained therein.

In the previous section, we determined a scale for the severity of the security incident. A security incident has been determined as "signification" if it obtained a score a 3 (on 5) or more. Only incidents of severity level 3 and beyond are reportable. Depending on the security incident, the TSP may have to notify:

- **National authorities:** Section 6.2 of [ENISA Article 19 incident reporting] proposes a notification template for that purpose.
- **Affected customers or the public**: Annex E of [ENISA Article 19 incident reporting] proposes guidelines for that purpose.

Particular attention must be paid to breach of personal data. The eIDAS Regulation requires in Article 5.1[17] that "*processing of personal data shall be carried out in accordance with Directive 95/46/EC*". Directive 95/46/EC is now replaced by GDPR. TSP is hence subject to GDPR requirements when personal data are compromised. Further information on this topic may be found for instance in ENISA documents specific to this area[18].

In order to illustrate this section, Annex A of this document proposes examples for security incident response for TSP issuing certificates and based on the examples of incident scenarios also provided in Annex A.

3.4 RECOVER FROM THE INCIDENT

3.4.1 Before the incident

Before the security incident occurs, the TSP must be prepared to recover from the incident or, in the worst-case scenario, discontinue its operations. For this purpose, this document recommends the following:

[17] More information on Article 5 can be found in [ENISA Recommendations for QTSPs based on standards].
[18] https://www.enisa.europa.eu/topics/data-protection

Table 10: Recommendations for security incident recovery

Rec. ID	Recommendations
REC-3.1-5	**Have contingency plans** The typical approach is to have backup sites (hot and/or cold) as well as business continuity plans (ETSI guidelines on business continuity management can be found in clause 7.10 of [EN 319 401]), but also the following.
	For TSP issuing certificates: **Have agreements with other TSPs to obtain substitute certificates** In the very critical situation where certificates need to be replaced, and none of the TSPs CAs, Ras, or revocation services can be trusted or are unavailable, the TSP may provide subjects with services from other TSPs until the operations can be resumed with their own systems. This will minimize the impact on subjects.
	Maintain updated information about your environment The TSP should have documented information regarding all data that can be helpful in case of an incident, such as: • lists of assets; • network diagrams; • applications and software versions; • disaster procedures; • recover and restore procedures; • contingency plans.
	Have a service termination plan In case the TSP decides for any reason or is forced to discontinue operations, there should be a plan in place to ensure that the services go down smoothly (e.g. make sure that issued certificates can be still verified or revoked from external sources). In some countries, the succession of service in case of termination is obligatory for QTSP. Such a termination plan is mandatory for QTSP following Article 24.2(i) of eIDAS. This is further covered in [ENISA Recommendations for QTSPs based on standards]. The reader is suggested to read the associated section of the latter document for more information. This document notably refers to clause 7.12 of [EN 319 401] and [ENISA Guidelines on Termination of Qualified Trust Services] for additional information.

3.4.2 After the incident

Once the source of the compromise has been determined and the appropriate response actions to mitigate the impact of the incident have been taken, the TSP should take the appropriate measures to minimize the possibility of the incident occurring again.

In the case that the security incident results in the decision of the TSP to discontinue operations, the TSP should carry on the termination plan defined in the previous section (see REC-3.1-5).

In the case that the TSP continues its activities, the following presents measures that a TSP should take in order to eradicate an incident:

1. **Determine what facilitated the incident**: Assess whether the incident was the consequence of vulnerabilities in any of the systems or processes of the TSP. Most incidents can be traced to some vulnerability. If the incident was due to a malicious insider, an associated vulnerability can be the lack of dual controls or mandatory rotation. In the case of a cryptographic attack, it might possible that the chosen algorithms, protocols, parameters, or implementations do not match the level of assurance needed for the TSP. In any case, it is of critical importance to trace what facilitated the incident in order to be able to eradicate it.
2. **Analyse the existing security policies and procedures**: Review the existing policies and procedures (including policy enforcement), especially those related to systems and processes related to the incident, to determine if they are sufficient for the expected

level of security. Especially important is to assess those policies and procedures related to the existing vulnerabilities.

3. **Re-conduct a risk assessment** (Section 2): Re-conduct a risk assessment to determine if the existing security controls match the level of risk accepted by the organisation. Based on the analysis results determine if security measures are to be incremented. Note that this should take place regularly anyway, even if no incident occurred.
4. **Define and implement corrective measures**: If the risk assessment results determine that any security levels need to be incremented, the last step in the eradication process is to define and implement the security measures needed. A parallel activity important during the eradication phase is to document all the actions taken during the incident. All this information should be used as input to improve the incident management procedures.

4. TRUST SERVICES SECURITY MEASURES

This section proposes a list of security measures to help 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 measures come from “technical” standards & best practices to address the risks both in general and in relevance with the specific trust services provided.

As mentioned in Section 1.4, to help TSP with further guidance and illustration on these policies, procedures, and processes, this document refers to ETSI and ISO/IEC standards. These standards are by no means made mandatory by the eIDAS Regulation. Regarding the ETSI standards in particular, it is however 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 TS and their components.

In that respect, the categories of security measures identified as subsections below correspond to ETSI standards structure and may be seen as “typical topics of concern” when operating a TSP offering a specific type of TS.

Beyond tailoring generic risk management to eIDAS trust services, ETSI standards also provide requirements that answer directly to eIDAS requirements. That is why these standards are also referred in [ENISA Recommendations for QTSPs based on standards]. As explained above in this document, a QTSP is first of all a TSP and most of the security and policy requirements applicable to QTSP are obligations on TSPs. Unsurprisingly, the standards referred by [ENISA Recommendations for QTSPs based on standards] for QTSP are also applicable to TSP and are generally written for TSP, qualified or not. The content of this section will consequently, and logically, refer to elements of [ENISA Recommendations for QTSPs based on standards] for further guidance. It is also not straightforward to determine if a certain measure is necessary because directly required by eIDAS or indirectly, as a consequence of the risks analysis; most of the requirements directly issued from eIDAS exist because they were perceived by the legislator as necessary to ensure a safe trust service provisioning (thus circumventing certain risk).

> NOTE: not all the requirements of the referred standards relate to the security framework. E.g. one can find requirements that answer the TSP’s obligation to inform its customers. They are not mentioned in this document but remain applicable.

Finally, it is important to note that not all ETSI standards are technologically neutral. Some references provided in the following sections are technology agnostic, in general when addressing the general management of a trust service, but the standards specific to a certain service are usually bound to a certain technology. E.g. ETSI standards on signature creation are clearly referring to digital signature (i.e. PKI based). This is, at the time of writing, the most used technology for signature creation and this is the reason why these standards are referred. Less spread technologies, like blockchain-based services, will likely see similar standards be developed, covering similar topics of concern.

For the sake of illustrating the process to determine ad-hoc security measures, Annex A provides a practical example of how a TSP issuing certificates for electronic signatures can

follow the security framework presented in Sections 2 and 3 of this document. This is a concrete illustration of the method followed by the editors of standards like [EN 319 411-1] to derive the measures referred below, starting from the scope of the services and the assets identification.

4.1 GENERAL SECURITY MEASURES FOR ALL TSPs

This section addresses the most common security concepts, as defined in standards such as [ISO/IEC 27001], and points toward general security measures for all TSP, regardless of the provided trust service.

It refers to [EN 319 401] that is structured to reflect such general security measures as well as specific eIDAS TSP requirements not necessarily directly linked to the security framework (e.g. TSP termination plan). These general security measures are largely technologically neutral and applicable to TSP independently of the trust service(s) they provide and thus, independently of the underlying technologies.

Next sections (starting from Section 4.2) provide specific guidance on top of the generic security measures, depending on the specific type of TS.

4.1.1 Requirements on the TSP's policies and practices

As detailed in previous sections, eIDAS Article 19 requires that all TSPs assess risks. Relying on standard(s) regarding due diligence and risk management such as [ISO/IEC 27002] (that provides guidelines for information security practices), and [ISO/IEC 27005] (that provides guidance on information security risk management as part of an information security management system (ISMS) as defined by [ISO/IEC 27001]), [EN 319 401] provides detailed requirements to be implemented by TSP with regard to information security policy.

Detailed guidance on the measures to be implemented may be found in:

- **Clause 6.3** of [EN 319 401].

4.1.2 Requirements on the TSP's management and operation

Article 24.2 of eIDAS imposes a series of obligations on QTSP. As mentioned above, although stated as applicable to QTSP only, these requirements underline the importance of security of the TSP management and operations and are expected also from a non-QTSPs.

In particular, Article 24.2(e) addresses trustworthy systems, Article 24.2(f) data protection, and Article 21.2(g) measures against forgery and theft of data. Implementing a security framework to address these obligations typically result in a series on requirements on (more details on the rationales can be found in [ENISA Recommendations for QTSPs based on standards]):

- Human resources;
- Asset protection;
- Access control;
- Cryptographic controls;
- Physical and environmental security;
- Operation security;
- Network security;
- Protection of collected evidence.

Detailed guidance on the measures to be implemented may be found in [EN 319 401]:

- **Clause 7.2** on human resources;
- **Clause 7.3 on** asset management;

- **Clause 7.4** on the limitation of TSP's system access to authorized individuals (and in particular REQ-7.4-02, REQ-7.4-03, and REQ-7.4-10 in the context of Article 24.2(e));
- **Clause 7.5** on cryptographic control, in case the TSP makes use of cryptographic keys or devices;
- **Clause 7.6** on physical and environmental security, and in particular for components whose security is critical to the provision of the trust service(s) and minimize risks related to physical security;
- **Clause 7.7 on** operation security;
- **Clause 7.8** on the network and related systems security;
- **Clause 7.10** on the collection of evidence (particularly important to demonstrate due diligence of the TSP in case of litigation, pursuant to Article 13 of eIDAS on liability) but also the protection of their confidentiality and integrity.

Concerning the monitoring of security events that might be relevant for notification and remediation as requested by eIDAS Article 19.2, detailed guidance on the measures to be implemented may be found in [EN 319 401]:

- **Clause 7.9** on incident management.

4.2 SECURITY MEASURES FOR PROVISION OF SPECIFIC TRUST SERVICES

On top of the general security measures presented in Section 4.1, the security framework needs to foresee additional measures specific to the trust service(s) provided. Typically, for trust services that make use of a signing key to sign evidence, ad-hoc measures with regard to the protection of that key will be required.

Such additional measures can be expressed as **complementary** measures one the topics covered by Section 4.1 or they may relate to **ad-hoc** topics specific to the operations of the trust service.

4.2.1 Certification service

Security and policy requirements for the issuance of certificates are specified in ETSI EN 319 411 parts 1 and 2 “Policy requirements for TSP issuing certificates”.

> NOTE: [EN 319 411-2] provides additional requirements to part 1 for the issuance of qualified certificates (see [ENISA Security Framework for QTSPs] that complements this document, and [ENISA Recommendations for QTSPs based on standards] for more details).

Clauses 6.4 and 6.5 of [EN 319 411-1] “Facility, management, and operational controls” and “Technical security controls”, complete [EN 319 401] clauses 7.2 to 7.4 and 7.6 to 7.8 by providing additional requirements on the following topics :

- **Clause 6.4.2** Physical security controls (complements [EN 319 401] clause 7.6);
- **Clause 6.4.3** Procedural controls (complements [EN 319 401] clause 7.4);
- **Clause 6.4.4** Personnel controls (complements [EN 319 401] clause 7.2);
- **Clause 6.4.8** Compromise and disaster recovery (complements [EN 319 401] clause 7.9);
- **Clause 6.5.7** Network security controls (complements [EN 319 401] clause 7.8);
- **Clause 6.5.6** Life cycle security controls (complements [EN 319 401] clause 7.7).

Clauses 6.5 “Technical security controls” of [EN 319 411-1] completes [EN 319 401] clauses 7.5 with detailed requirements on key pair generation and installation (**Clause 6.5.1).**

Clauses 6.2, 6.5 and 6.6 provide **ad-hoc requirements** on the TSP issuing certificate assets (i.e. mainly the signing keys) and procedures (i.e. mainly the identification of the subject to be certified) linked to the issuance of certificates as follows:

- **Clause 6.2** Identification and authentication states important requirements with regard to the security of the subject identity proofing process:
  - **Clause 6.2.2** Initial identity validation;
  - **Clause 6.2.3** Identification and authentication for re-key requests;
  - **Clause 6.2.4** Identification and authentication for revocation requests.
- **Clause 6.5.2, 6.5.3 and 6.5.4** indicates the requirements with regards to private key protection, cryptographic module engineering controls and activation data respectively;
- **Clause 6.6.3.-03** requires monitoring of non-issued certificates**.**

4.2.2 AdES creation service

One usually distinguishes two important components in the signature creation process:

1. The signature creation device that handles the signature creation data (e.g. private key); and
2. The signature creation application that packages the signature into a certain format (usually depending on the original format of the data to be signed) and a certain level (e.g. with elements that ensure the long-term validity of the signature).

A signature can be entirely performed by the signatory (i.e. with a signature creation application and a signature creation device (s)he holds), in which case no TSP is involved. Otherwise, a signature can be created on behalf of the signatory, in which case the TSP either:

1. Manages the signature creation data (on a signature creation device) on behalf of the signatory (this is often called a *signing server service*), while the signature is created by an application in the hand of the signatory or another TSP (see below). Security measures that are relevant for such a service are proposed in Section 4.2.3.2;
2. Offers the signature creation application, while the signature creation device is in the hand of the signatory or another TSP (this is often called a *signature creation application service*). Security measures that are relevant for such a service are proposed in Section 4.2.3.1.

NOTE: both activities may be offered by the same TSP, which offers the signature creation application and the management of the signature creation data all together on behalf of the signatory. This is often called a *remote signature service*.

4.2.2.1 Signature creation application service management and operation

Security and policy requirements for this service are specified in [TS 119 431-2] “TSP service components supporting AdES digital signature creation”.

Clause 6.3 of [TS 119 431-2] completes [EN 319 401] clause 6.3. as follows, with specific attention to the fact that the TSP creating signatures may have access to the signed data (considered as personal data):

- **Clause 6.3** Information security policy.

Clause 7 of [TS 119 431-2] “Signature creation application service management and operation”, completes [EN 319 401] clause 7, considering amongst other the fact that the communication channel to collect and transfer information from the customer, third parties TSP and the TSP offering the signature creation service needs to be protected, as follows:

- **Clause 7.6** Physical and environmental security (complements [EN 319 401] clause 7.6);

- **Clause 7.7** Operation security (complements [EN 319 401] clause 7.7).

Clause 8 of [TS 119 431-2] "Signature creation application service component technical requirements" provides **ad-hoc requirements** on the TSP offering signature creation services assets and related process (e.g. preserving the integrity of the data to be signed, conform to what the customer requests to sign) as follows:

- **Clause 8.1** Interfaces;
- **Clause 8.2** AdES digital signature creation.

4.2.2.2 Signing server service management and operation

CEN [EN 419 241-1] specifies the security requirements and recommendations for Trustworthy Systems Supporting Server Signing (TW4S) that generate digital signatures and relies on [EN 319 401]. Security requirements are provided in clause 6.

Further security and policy requirements for signing server service are specified in [TS 119 431-1] "TSP service components operating a remote QSCD / SCDev". **This document endorses requirements specified in CEN [EN 419 241-1]** specifying security requirements and recommendations for Trustworthy Systems Supporting Server Signing (TW4S) that generate digital signatures and relies on [EN 319 401] as well as the **requirements specified in [EN 319 401]** and completes them further as described below.

> NOTE: when the Signature Creation Device (SCDev) is a QSCD, the TSP must be qualified and additional obligations apply. See [ENISA Recommendations for QTSPs based on standards] for more details.

Clauses 6.4 and 6.5 of [TS 119 431-1] "Facility, management, and operational controls" and "Technical security controls", complete [EN 319 401] clause 7, considering that maintaining the control on the signing keys by their owner is a crucial security objective, as follows:

- **Clause 6.4.2** Physical security controls (completes [EN 319 401] clause 7.6)
- **Clause 6.5.3** Computer security controls (completes [EN 319 401] clause 7.4)

Clauses 6.2 and 6.3 of [TS 119 431-1] further complete CEN [EN 419 241-1] with additional requirements relating to the control the signing keys by their owner (i.e. ensuring that the right person access to the right key and can protect it from the use by third parties, through identity proofing and authentication measures) as follows:

- Signing key initialization:
  - 6.2.1 Signing key generation;
  - 6.2.2 eID means linking;
  - 6.2.3 Certificate linking;
  - 6.2.4 eID means provision.
- Signing key lifecycle operational requirements:
  - 6.3.1 Signature activation;
  - 6.3.2 Signing key deletion;
  - 6.3.3 Signing key backup and recovery.

4.2.3 Signature validation service

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

Clause 6.3 of [TS 119 441] completes [EN 319 401] clause 6.3. as follows:

- **Clause 6.3** Information security policy, with specific attention to the fact that the TSP validating signatures may have access to the signed data (considered as personal data).

Clause 7 of [TS 119 441] "Signature Validation Service management and operation" completes [EN 319 401] clause 7 by providing requirements on the following topics, considering amongst other the fact that the communication channel to collect and transfer information from the customer, third parties TSP and the TSP offering the validation service needs to be protected:

- **Clause 7.5** Cryptographic controls (complements [EN 319 401] clause 7.5);
- **Clause 7.6** Physical and environmental security (complements [EN 319 401] clause 7.6);
- **Clause 7.7** Operation security (complements [EN 319 401] clause 7.7);
- **Clause 7.8** Network security (complements [EN 319 401] clause 7.8);
- **Clause 7.9** Incident management (complements [EN 319 401] clause 7.9).

Clause 8 "Signature validation service technical requirements" provides **ad-hoc requirements** on the TSP offering validation services assets (e.g. the validation report signing keys) and related process as follows:

- **Clause 8.1** states requirements on the signature validation process;
- **Clause 8.2** states requirements on the signature validation protocol;
- **Clause 8.3** states requirements on the service interfaces.

4.2.4 Preservation service

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".

Clause 7 of [TS 119 511] "PSP management and operation" completes [EN 319 401] clause 7, considering amongst other issues the fact that the communication channel to collect and transfer information from the customer, third parties TSP and the TSP offering the preservation service, needs to be protected as follows:

- **Clause 7.5 and 7.14** Cryptographic controls (complements [EN 319 401] clause 7.5);
- **Clause 7.8** Network security (complements [EN 319 401] clause 7.8);
- **Clause 7.9** Incident management (complements [EN 319 401] clause 7.9).

The additional measures below cover the security of specific assets of TSP offering preservations services, amongst others the need to protect evidence in availability and integrity:

- **Clause 7.15** "Augmentation of preservation evidences" provides ad-hoc requirements on the TSP offering preservation services related process (i.e. augmentation of signatures);
- **Clause 8.1** "Preservation protocol" provides **ad-hoc requirements** on the protocol;
- **Clause 9** "Preservation process" provides **ad-hoc requirements** on the process in the following way:
    - **Clause 9.1** Storage of preserved data and evidences;
    - **Clause 9.2** Preservation evidences;
    - **Clause 9.3** Preservation of digital signatures.

4.2.5 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".

Clause 7 of [EN 319 421] "TSA management and operation" completes [EN 319 401] clause 7, considering that an essential aspect of the time-stamping resides in the security of the underlying cryptographic algorithms, the hash functions in particular, as follows:

- **Clause 7.6** Cryptographic controls (complements [EN 319 401] clause 7.5) with specific measures with regards to the TSP key:
  - 7.6.2 TSU key generation;
  - 7.6.3 TSU private key protection;
  - 7.6.4 TSU public key certificate;
  - 7.6.5 Rekeying TSU's key;
  - 7.6.6 Life cycle management of signing cryptographic hardware;
  - 7.6.7 End of TSU key life cycle.
- **Clause 7.8** Physical and environmental security (complements [EN 319 401] clause 7.6);
- **Clause 7.9** Operation security (complements [EN 319 401] clause 7.7);
- **Clause 7.10** Network security (complements [EN 319 401] clause 7.8).

Clause 7.7 « Time-stamping » provides **ad-hoc measures** for time-stamping, considering amongst others the accuracy of the time sources as a crucial asset.

NOTE: [EN 319 421] also provides specific requirements for QTSP issuing qualified time-stamps (see [ENISA Security Framework for QTSPs] that complements this document and [ENISA Recommendations for QTSPs based on standards] for more details).

4.2.6 Electronic registered delivery service and registered electronic mail 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 further covered in [ENISA Security framework for QTSPs]. The content of this section covers security measures that may apply to non-qualified electronic registered delivery services (non-QERDS) and non-qualified registered electronic mail services (non-QREMS).

Clause 7 of [EN 319 521] "ERDSP management and operation" (no additional requirements are defined in clause 7 of [EN 319 531]) completes [EN 319 401] clause 7 on the following topics:

- **Clause 7.5** Cryptographic controls (complements [EN 319 401] clause 7.5) and mostly targets the ERDS signing key;
- **Clause 7.6** Physical and environmental security (complements [EN 319 401] clause 7.6);
- **Clause 7.8** Network security (complements [EN 319 401] clause 7.8).

Clauses 5 "General provision on ERDS" in [EN 319 521] and "General provision on REMS" in [EN 319 531] provide **ad-hoc requirements** on the TSP offering ERDS and REMS. In particular, the following clauses (excluding sections "Provisions for EU QREMS/QERDS") provides measures relating to:

- **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.

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 QTSPs	Security Framework for Qualified Trust Providers https://www.enisa.europa.eu/publications/security-framework-for-qualified-trust-providers
ENISA Guidelines on Termination of Qualified Trust Services	Guidelines on Termination of Qualified Trust Services - Technical guidelines on trust services https://www.enisa.europa.eu/publications/tsp-termination

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
TSP Technical Best Practices	Trust Service Provider Technical Best Practices considering the EU eIDAS Regulation (910/2014) https://www.ccadb.org/documents/TSP_Technical_Best_Practices_eIDAS.pdf
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 419 241-1	CEN EN 419 241-1: “Trustworthy Systems Supporting Server Signing Part 1: General System Security Requirements”
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 119 431-2	ETSI TS 119 431-2 (v1.1.1): “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation”
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 (v1.1.1): "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".

A ANNEX: PRACTICAL EXAMPLES FOR TSPS ISSUING CERTIFICATES

Disclaimer: The following examples are provided for TSPs issuing certificates using PKI-based technology. The examples were chosen because the issuance of certificates is one of the most frequent types of trust services provided and PKI-based technology is by far the most frequent technology used for implementing this trust service.

The examples of assets, threats, etc. may constitute a basis for transposing to other types of trust services or other types of technologies.

A.1 EXAMPLES OF ASSETS

The following list of examples aim to illustrate guidelines provided in Section 2.2.1.1 of this document and is targeted to a TSP issuing electronic certificates. This list is not exhaustive and should only be used as a generic reference.

A.1.1 Primary assets

Information assets may be:

- CA certificate;
- CA private key;
- RA certificate;
- RA private key;
- Subjects' certificates;
- Subjects' private keys;
- Registration archives;
- Audit logs of the different involved entities;
- Certificate revocation status request logs;
- Certificate revocation lists.

Business processes may be:

- The registration process;
- The CA key pair generation;
- The CA key pair storage, backup, and recovery;
- The CA certificate dissemination;
- The CA key pair usage;
- The CA private key destruction;
- The subject device provisioning
- The subject certificate generation and delivery to subject
- The subject key pair generation
- The subject certificate renewal, rekey and update
- The subject certificate dissemination
- The revocation management process
- The revocation status dissemination process

These business processes have support processes that can perform additional activities that can also be vulnerable and affect the business processes.

A.1.2 Supporting assets

A.1.3 Software, hardware, and network

The TSP may include in the asset inventory all software applications, all hardware infrastructures and all network infrastructures that are used in the TSP. Examples of software, hardware and networks assets are:

- Hardware:
  - CA equipment (e.g. servers for CA root and subordinates CAs);
  - Other CA necessary equipment (e.g. LDAP);
  - RA equipment (e.g. PCs, printers, etc.);
  - Subject devices (e.g. smartcards, USB tokens, etc.);
  - Hardware Security Modules (HSMs);
  - Web servers.
- Software:
  - CA key management applications;
  - CA backup applications;
  - Other CA applications;
  - RA applications.
- Network Infrastructure:
  - Communication lines, routers, bridges, firewalls, etc (further covered in [ISO/IEC 27005].

A.1.4 Locations and sites

The TSP may include in this category all facilities where the CA operation is conducted, where other non-CA related operations are performed, as well as RA offices. Examples of location assets are:

- TSP primary premises;
- TSP back up sites;
- RA offices.

A.1.5 Personnel

The TSP may include in this category all different roles involved in the TSP processes and the access rights to the different assets. Examples of personnel assets are:

- TSP trusted roles;
- Other operational roles;
- RA operators;
- Different administrators at level of OS, DB, etc.

A.1.6 Other assets

The TSP may identify all other assets not included in the above categories that have a value for the organisation. Examples of other assets are:

- TSP reputation;
- TSP legal compliance;
- TSP trust relationships (e.g. to business partners, providers and suppliers or relying parties like governments, software application vendors);
- TSP customer base.

A.2 EXAMPLES OF THREATS

The following list of examples aim to illustrate guidelines provided in Section 2.2.1.2 of this document and is targeted to a TSP issuing electronic certificates. This list is non-exhaustive and should only be used as a generic reference.

Examples of threats
Theft or loss of equipment or data
Accidental destruction of equipment or data
Retrieval of recycled media
Tampering of equipment or data
Malicious software
Eavesdropping
Disclosure
Forging of rights
Abuse of rights
Cryptanalysis
Overload with traffic
Hardware failure
Software bug
Faulty hardware change/update
Faulty software change/update
Policy or procedure flaw
Security shutdown
Power cut of the power grid
Error in use
Fire
Water damage or corrosion
Environmental disaster (seismic or hydrological events, windstorms…)

These threats can be categorized by root cause and associated to an origin. [ENISA Article 19 incident reporting] proposes five root cause categories that may apply to TSPs:

- **Human error**: includes incidents caused by human error during the operation of equipment or facilities, the use of tools, the execution of procedures, etc.
- **System failures**: includes incidents caused by failures of a system, for example, hardware failures, software failures or errors in procedures or policies.
- **Natural disaster**: includes incidents caused by severe weather, earthquakes, floods, wildfires, and so on.
- **Malicious actions**: includes incidents caused by a deliberate act by someone or some organisation.
- **Third party failures**: includes incidents where the cause was not under the direct control of the provider, but some third-party.

Annex C of [ISO/IEC 27005] also proposes categories of threats and origins.

A.3 EXAMPLES OF VULNERABILITIES

The following list of examples aim to illustrate guidelines provided in Section 2.2.1.3 of this document and is targeted to a TSP issuing electronic certificates. This list is non-exhaustive and should only be used as a generic reference.

The TSP risk analysis must include a list of potential vulnerabilities which corresponds to its actual business and operational environment (i.e. its trust services).

Cat. ID	Examples of vulnerabilities
VUL-1	**Key pair generation** (can be divided for CA key pairs and subjects' key pairs)
	Key is generated with a weak algorithm or insufficient key length (or other parameters)
	Key is generated in a non-secure physical or logical environment
	Usage of insecure or weak random number generator
	Key generation is not performed by trusted individuals
VUL-2	**Key pair storage, backup, and recovery**
	Private signing key is not kept in a physically or logical secure environment
	Private signing key is not backed up
	Back-up copies of the private signing key are not stored securely
	Private keys are disposed or archived in non-secure manner
	Private key restore can be performed in a non-secure manner
VUL-3	**CA key pair usage**
	Lack of security procedures for signing key activation
	Security of cryptographic hardware used to sign certificates is not properly verified or maintained
	Signing key pair is used for other purposes than subject certificate signing, except for those that can be used optionally
	Insecure processes or applications may lead to sending fake data/certificates to be signed
VUL-4	**Subject key pair usage**
	Lack of protection measures for the subject key pair activation
	Negligent handling of private key by subject
	Lack of guidelines to train subject on subject key pair custody
VUL-5	**Certificate dissemination** (can be divided for CA key pairs and subjects' key pairs)
	Setting wrong attributes in the certificate, such as policy mapping or path length constraints
	Certificate repository is not secured
	Certificate repository is not up to date
VUL-6	**Delivery of subject key** (or certificate)
	Unsecure delivery of key pair to subject
	Failure to properly verify identity of subject when key pair is delivered
	Unsecure retraction of undeliverable keys
	Tampering with the key pair before it reaches the subject (e.g. during transport)
	Failure to support subject's platform properly (i.e. Linux, Windows, Android, iOS, mobile vs. desktop, etc.)
VUL-7	**Provisioning of subject device**
	Failure to verify the authenticity of the source of the subject's device
	Inappropriate security characteristics of the subject's device for the TSP needed assurance level
	Tampering with the subject´s device before it reaches the subject (e.g. during transportation)

	Failure to properly verify identity of subject when device is delivered
	Failure in retracting undeliverable subject´s device
	Failure in reusing subject´s device (e.g. improper removal of keys of former subject)
VUL-8	**Revocation management process**
	Lack of appropriate revocation policies and procedures
	Lack of proper enforcement of policies and procedures
	Failure to submit revocation request
	Insecure certificate revocation request channels
	Lack of proper verification of subject identity during revocation request
	Lack of measures to guarantee integrity and authenticity of revocation requests
VUL-9	**Certificate revocation status dissemination**
	Lack of an appropriate revocation list update policy
	Lack of enforcement of the revocation list update policy (including frequency)
	Insecure dissemination of the certificate revocation list
VUL-10	***Information and communication systems*: Software applications**
	Lack of disaster recovery and business continuity plans
	Lack of regular bug fixes and updates
	Lack of (automated) status testing
	Lack of incident response protocols/policies
	Lack of understanding of software security certification, leading to unpatched software due to certification (Common Criteria) status
VUL-11	***Information and communication systems*: Hardware components**
	Lack of secure equipment storage facilities
	Lack of (automated) status testing
	Lack of incident response protocols/policies
VUL-12	***Information and communication systems*: Audit logs**
	Lack of appropriate audit logging policies
	Insufficient protection of audit logs
VUL-13	**Personnel**
	Lack of appropriate training of personnel operating CA related activities
	Lack of separation of duties among trusted roles
	Lack of enforcement of the information security policy
	Lack of clear job descriptions for CA roles
	Lack of employment screening of personnel performing trusted roles
	Lack of adequate supervision
VUL-14	**Registration process**
	Inadequate policy for proof identity
	RA software inadequate
	Lack of appropriate software to protect the RA operation from malicious software
	Lack of appropriate protection of the RA private key
	Insecure communication channel between the RA and the CA
	Lack of technical expertise of the RA operator
	Lack of appropriate procedures for registration documents archival
	Insufficient protection of registration records

A.4 EXAMPLES OF INCIDENT SCENARIOS

In order to help identifying consequences of incident scenarios, this section provides examples of typical incident scenarios that may occur for a TSP issuing certificates.

Ways to respond to each incident scenario are described in the following sections.

Examples of incident scenario	Description of incident scenario
Incidents affecting CAs or the subject certificate	
Compromise of a CA	A compromise of the CA consists of an unauthorized intrusion in the CA information systems or any type of unauthorized access to its private key. A CA compromise may lead to fraudulent issuance of subjects' certificates, to the impossibility of using certificates issued by the CA, or to an interruption in the issuance of certificates.
Compromise of the subject's key pair	A compromise of a subject key pair consists of an unauthorized access to its private key. The objective of a subject key pair compromise is to make a fraudulent use of the subject certificate.
Compromise of the cryptographic algorithms or use of inadequate key lengths (or other parameters)	A compromise of the cryptographic algorithms occurs when the algorithms used to generate the CA or subject key pairs become insecure, and an individual could deduce or replicate the private key, effectively being able to supplant the CA or subject, or to access confidential information.
Compromise of the cryptographic modules	A compromise of cryptographic modules occurs when the cryptographic algorithms, parameters, protocols, or implementations (i.e. software or hardware) become insecure. If, for example, the algorithm used to generate the CA or subject key pairs become insecure, an attacker could deduce or replicate the private key. Another possibility is that the actual signature or encryption algorithm is weak, enabling an attacker to generate fake signatures or decrypt messages without having access to the private key. Note that bad parameters or implementations can very well lead to weaknesses despite the fact that the algorithm or protocol being used is secure.
Compromise of the revocation services	A compromise of the revocation services occurs when a malicious individual manages to breach the integrity of the certificate revocation systems, either by tampering a certificate revocation request or by altering the certificate revocation status service. The objective of this breach is to make a fraudulent use of a certificate that is revoked or in the process of being revoked.
Repudiation claim by certificate subject	A repudiation claim occurs when a subject declares not having performed the actions with his certificate. A repudiation claim can lead to actual repudiation when there is lack of audit logs and procedures or the TSP cannot guarantee the security of the whole certificate management process. Repudiation can have liability consequences for the TSP.
Accidental loss of availability of the certification services	Loss of availability of the certification services occurs when any of the systems involved in the certification management lifecycle (registration, certificate request, certificate generation, delivery to subject, revocation) becomes unavailable due to accidental system malfunctions or failures. Depending on the affected systems, different processes of the TSP will be interrupted, resulting in possible financial and reputational loss.
Personal data breach	A personal data breach occurs when personal data provided to or produced by the TSP are disclosed to unauthorized individuals. Personal data maintained by the TSP includes the information contained in the certificates, the registration records, and the audit logs, apart from staff or business relations data. A breach can occur due to theft or loss of devices containing personal data, hacking of the information systems or inadequate disposal. A personal data breach can imply legal and economic sanctions from supervisory authorities, and can damage the reputation of the TSP.

Incidents affecting RAs	
Compromise of a RA	A compromise of the RA consists of an unauthorized intrusion in the RA information systems, any type of unauthorized access to its private key, or its communication channel with the CA. The objective of a RA compromise is to generate fraudulent certificate requests to be sent to the CA in order to obtain rogue certificates.
Impersonation	Impersonation occurs when a malicious individual attempts to supplant another individual personal identity or to fraudulently claim legal representation of an organisation in order to obtain a rogue electronic certificate perform some fraudulent actions.

A.5 EXAMPLES OF CONSEQUENCES

The following list of examples aim to illustrate guidelines provided in Section 2.2.1.5 of this document and is targeted to a TSP issuing electronic certificates. This list is non-exhaustive and should only be used as a generic reference.

Fraudulent issuance of subjects' certificates: Incidents involving a breach of trust of the CA or the RA could lead to an issuance of fraudulent subjects' certificates, which could be used to impersonate these subjects. This breach, for example, can be due to a compromise in the CA or RA information system or gaining access to their private keys. This impersonation could be used to intercept private communications or forge electronic signatures.

Fraudulent use of valid certificates: Incidents related to the subject's custody of legitimate issued certificates or vulnerabilities in the subject device or keys can lead to a malicious individual use in order to impersonate the data subject. This impersonation could be used to intercept private communications, to forge electronic signatures or to decipher previously encrypted messages.

Fraudulent use of revoked certificates: Incidents affecting the revocation management system could lead to the inability to process certificate revocation requests, to disseminate their status, etc.

Inability to issue subjects' certificates: Incidents affecting availability or integrity of the RA or the CA information systems can lead the TSP not being able to issue new certificates.

Inability to use valid certificates: Some scenarios like the loss of availability of the certificate revocation status may lead to the inability to check the validity of certificates. Compromises of the CA or RA can also lead to the inability to use valid certificates due to the loss of trust or possibility of compromise.

Inability to revoke certificates: A failure or compromise of the revocation management systems could lead to subjects' willingness to revoke certificates not being able to do so, which could facilitate fraudulent use.

Repudiation by certificate subject: Lack of proper registration policies and record preservation can lead to a subject claiming repudiation of the actions performed with its certificate. Other integrity compromises in the certification chain may lead to the same repudiation claim.

Loss of accountability of actions: In case of an incident, existing logs, as well as their protection again manipulation, are an important tool to be able to determine the nature and source of the incident. Lack of an appropriate level of logging, loss of existing logs or lack of protection of logs can lead to the impossibility to determine user actions.

Liability: Any security incident or breach of the certification policies that carries a negative effect on subjects can lead to legal and financial liability for the TSP.

Loss of reputation: Any security incident, especially those affecting the integrity of the CA operations and the confidentiality of private keys, could cause a loss of reputation of the TSP that would negatively affect subject trust.

A.6 EXAMPLES OF SECURITY INCIDENT DETECTION

The following list of examples aim to illustrate guidelines provided in Section 3.1 of this document and is targeted to a TSP issuing electronic certificates. This list is non-exhaustive and should only be used as a generic reference.

A.6.1 Fraudulent certificate activities

Indicators that some kind of certificates are involved in fraudulent activities include for example:

- Certificates associated with man in the middle attacks.
- Certificates associated to known malware sites.
- Malware signed with certificates.
- Subjects reporting that certificates associated with their name do not belong to them.
- Subjects that report usage of their certificates that they did not do themselves.
- Attempts to use invalid or revoked certificates.

Fraudulent certificate activity may indicate different types of compromises. In order to determine what part of the trust service is compromised, at least the following steps should be followed:

- Analyse the potentially fraudulent activity to determine the certificates' origin and verify that they are linked to a CA of the TSP;
- Contact the certificate subjects' to assess whether fraudulent activities are taking place;
- Assess the circumstances under which the certificate was issued:
    - Contact the RA to check registration logs and records;
    - Check certificate request and generation logs at CA.

If any of the above investigations lead to a suspicion that there is a bogus certificate, the TSP should proceed to analyse suspicious activities in the certificate lifecycle management and abnormal logs in the information systems and finally come to a decision whether there is a breach or not and react accordingly.

A.6.2 Abnormal activities in information systems

Another incident indicator is any event in the TSPs systems that could indicate an intrusion attempt, for example:

- Unsuccessful login requests
- Unusual network traffic flows
- Unusual event detection in antivirus, IPS, perimeter systems etc.
- Appearance of filenames not known to the administrators
- Changes in audit functions in information systems

Abnormal log entries in information systems may come as a triggering event themselves, or they may be detected upon revision of systems when other suspicious activities are taking place. The TSP should analyse whether the logs point to an intrusion being successful. If that is case, the TSP should check for suspicious activities in the certificate lifecycle management to determine whether the intruder actually managed to create fraudulent certificates. Be aware that an intruder, once in the system, may be able to cover its tracks.

A.6.3 Suspicious information in the certificate lifecycle management logs

Suspicious information in the certificate lifecycle management logs may come as a triggering event itself, when personnel operating CA or RA functions detect strange certificate requests, issuances or revocations; or it may be detected upon checking of systems when other suspicious activities are taking place; or during standard auditing activities.

In any case, the TSP should inspect the system and check for any indication a fake certificate or revocation was requested or generated. Amongst the indicator are:

- Inconsistencies in the registration, certificate generation or revocation logs;
- Inconsistencies in the information associated to any certificate;
- Registration requests lacking associated registration records;
- Certificate generation or revocation lacking any request;
- Unusual behaviour (e.g. physical registration outside business hours); and
- Inconsistencies in revocation service logs (e.g. OCSP queries for not issued certificates).

If there is an indication of an incident, the TSP should assess the type of incident taking place by checking the different logs and correlating information from the different systems involved in the certification process. For example:

- Certificate requests logs with no associated registration records can be indicators of an RA compromise.
- Logs in the CA certificate generation systems that are not associated to any matching certificate requests from an RA could be an indication of a CA compromise.
- Suspicious certificates that have no associated certificate generation logs in the CA systems can indicate a CA compromise or a compromise of the cryptographic modules.
- Registration records that seem inconsistent may indicate an impersonation incident.
- Frequent revocation status requests (e.g. OCSP) for certificates that have no corresponding certificate issued may indicate a CA compromise incident.

A.6.4 Unaccounted key media

The TSP should maintain an inventory of all physical media storing key material and periodically verify that all media is accounted for. Any key media handling or storage device unaccounted for should be considered an indication of a compromise:

- CA key storage devices
- CA operators' keys
- RA key storage devices
- RA operators' keys
- Subjects' keys
- Key backup media

The TSP should assess the circumstances under which the key handling material was lost to determine whether it was due to accidental or intentional events, and whether fraudulent certificate or revocation issuance could have occurred. In any case the suitable measures should be taken to deal with the unaccounted media.

A.6.5 Loss of availability

Loss of availability of the TSP systems can be the consequence of an intrusion attempt or be due to accidental events. In any case it should be treated as an incident and its source should be investigated. In the event of a loss of availability, the TSP should immediately restore the

availability of critical systems, such as revocation services, e.g. by switching to standby systems. The TSP should also assess whether there any accidental causes that could explain a disruption, such as loss of essential services, natural hazards, etc. but also investigate other potential causes.

If no external event seems to be the cause of the disruption, the TSP should determine the origin of the system malfunction by checking information systems logs. When the source of the system malfunction is established, the next step is to check whether it was the consequence of any intentional action.

A.6.6 Loss of custody of subject key

Reports by a subject of loss of sole custody of its private key can point to an accidental loss or to an attempt of compromising a subject key. The TSP should assist the subject in determining whether any fraudulent activity is taking place.

A.7 EXAMPLES OF INCIDENT SCENARIO RESPONSE

The following list of examples aim to illustrate guidelines provided in Section 3.3 of this document and is targeted to a TSP issuing electronic certificates. This list is non-exhaustive and should only be used as a generic reference.

These examples are based on the “Examples of incident scenario” provided above.

A.7.1 Responding to a CA comprise

When a CA compromise is detected[19], it is critical for the TSP to take prompt and appropriate measures to mitigate the impact of the breach. The goal is to prevent any further usage of fraudulent certificates. At least, the following actions should be undertaken:

- Discontinue any new certificate issuance from the affected CA.
- Revoke the CA certificate (which automatically revokes all certificates issued by the CA).
- Update the revocation status information.
- Notify relying parties and urge them to update all revocation information.
- Inform affected subjects of the revocation of their certificates.
- Notify competent authorities about the breach.
- Provide affected subjects with substitute certificates from another CA (e.g. from a standby system or another TSP).

If the affected CA is a root CA, follow at least these additional steps:

- Revoke trust in the root CA in all trust repositories where it is included.
- Provide affected subjects with substitute certificates from another CA (e.g. from a standby system or another TSP).

A.7.2 Responding to a RA compromise

Both RA compromises and CA compromises can lead to fraudulent certificates being issued. The response will depend on whether it can be determined which certificate requests sent by the RA were illegitimate.

If all fraudulent certificates can be detected, revoking those certificates can be sufficient. But when not all fraudulent certificates can be detected with certainty, it is recommended for the CA to revoke all certificates based on registration data from the compromised RA, because there is

[19] RFC 6489 – Certification Authority (CA) Key Rollover in the Resource Public Key Infrastructure (RPKI) can be consulted as reference – https://tools.ietf.org/html/rfc6489

no guarantee as to whether fake certificates are being used. At least, the following actions are recommended:

If all fraudulent certificates can be identified:

- Discontinue any new certificate issuance requests from the affected RA.
- Revoke the RA certificate.
- Revoke all fraudulent certificates.
- Update the revocation status information.
- Notify relying parties and urge them to update all revocation information.
- Notify competent authorities about the breach.

If not all fraudulent certificates can be identified, follow at least these additionally steps:

- Revoke all certificates based on registration data from the compromised RA.
- Identify affected legitimate subjects and provide them with certificates from another RA (e.g. from a standby system or another TSP).

A.7.3 Responding to a compromise of the revocation services

The goal of responding to a compromise of the revocation services is to avoid the usage of revoked certificates and to re-establish the correctness of the revocation status information. Until revocation information can be trusted, relying parties should not accept certificates. With this objective, at least the following actions are recommended:

- Notify relying parties and urge them not to accept any certificates from the CA until revocation information can be trusted.
- If the revocation status site seems to be compromised, set up a stand-in site for revocation information checking, e.g. activate the standby system.
- Identify the last trustable revocation status information.
- Add the legitimate revocations occurred since then to this revocation status information.
- Disseminate this revocation status information.
- Notify competent authorities about the breach.

A.7.4 Responding to a compromise of the cryptographic modules

Compromise of the cryptographic modules is a different event from other compromises in TSPs, as the detection may come from external sources rather than an attack to the TSP itself. However, the TSP should take action like in any other compromise by revoking the corresponding certificates. At least, the following actions are recommended:

- Discontinue any new certificate issuance using the compromised cryptographic modules.
- Revoke all certificates issued with the compromised cryptographic modules.
- Update the revocation status information.
- Notify relying parties and urge them to update all revocation information.
- Inform affected certificate subjects of the revocation of their certificates.
- Notify competent authorities about the breach.
- Provide affected certificate subjects with certificates with stronger cryptographic modules.

Note that here are proactive measures that prevent TSPs from being compromised even if (a single) cryptographic module becomes insecure (e.g. forward secure cryptography or utilizing

fundamentally different crypto modules in parallel). In this case, the immediate revocation is not necessary.

A.7.5 Responding to a repudiation claim by a certificate subject

Although a repudiation claim does not imply necessarily a compromise of a certificate, it is advised in this event to revoke the certificate, to ensure no further actions are performed with the certificate. At least, the following actions are recommended:

- Revoke the certificate to prevent any further usage.
- Update the revocation status information.
- Assess whether a compromise has taken place.
- Gather all logs related to registration, certificate issuance and certificate usage (e.g. for evidence purposes).

A.7.6 Responding to impersonation

An impersonation attack implies the revocation of the affected certificates. Although this attack is of a smaller scale than other compromises, in many cases it is a directed attack and can have very damaging consequences; therefore a prompt response is needed. At least, the following actions are recommended:

- Revoke the attacked certificate(s).
- Update the revocation status information.
- Notify relying parties and urge them to update revocation information.
- If the impersonated subject is not yet aware, inform the subject.
- Notify competent authorities about the breach.

A.7.7 Responding to a compromise of a subject's key pair

A compromise in a subject key pair implies as an immediate action the revocation of the affected certificate. If the compromise may affect other subjects, for example when it derives from vulnerabilities in the subject device, further actions may be needed. At least, the following actions are recommended:

- Revoke the affected certificate(s).
- Update the revocation status service.
- If the certificate subject is not yet aware, inform the subject.
- Notify competent authorities about the breach.
- Issue new certificates for the subject(s).

In case the compromise affects other subjects, for example when it derives from vulnerabilities in the subject key pair algorithm, At least the following additional actions are recommended:

- Determine the common cause.
- Determine all affected subjects.

A.7.8 Responding to a loss of availability of services

The goal in the response to a loss of availability is to minimize the downtime of the service and the impact on the trust service.

- Activate contingency plans and business continuity plans (such as standby systems).
- If the disruption affects revocation status information systems, notify relying parties and urge them not to accept any certificates until revocation information is available to prevent the use of revoked certificates.

TP-02-20-995-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: 978-92-9204-440-4
DOI: 10.2824/36142