Risk assessment

Guidelines for trust services providers – Part 2

Version 1.0 – December 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

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

Authors

Iñigo Barreira, Izenpe

Tomas Gustavsson, Primekey

Alexander Wiesmaier, AGT International

Clara Galan, Ministry of Defense, Spain[1]

Sławomir Górniak, ENISA

Contact

For contacting the authors please use sta@enisa.europa.eu

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

Acknowledgements

ENISA would like to thank the numerous experts who reviewed this paper for their contributions. We also thank the following organizations for voluntarily taking part in the survey on security aspects of trust service providers launched by ENISA. The survey was conducted during the months of June and July 2013, 46 respondents from different organisations completed the survey. The list of the organisations taking part in this exercise is available in Annex 4 of this document.

[1] Seconded National Expert at ENISA during the time of the study

Legal notice

Copyright Notice

Executive summary

E-Government services have significant potential to make public services more efficient for the benefit of citizens and businesses in terms of time and money. And while these benefits are increasingly being felt nationally, e-Government services still face administrative and legal barriers on a cross-border level, although pan-European projects like STORK have shown that technical issues of interoperability of electronic identifications can be overcome. In order to remove existing barriers for cross-border e-ID based services the European Commission has proposed in June 2012 a draft regulation on electronic identification and trust services for electronic transactions in the internal market [38], which will replace the existing Electronic Signature Directive 1999/93/EC [37]. The main goals of this action are to:

- ensure mutual recognition and acceptance of electronic identification across borders
- give legal effect and mutual recognition to trust services
- enhance current rules on e-signatures
- provide a legal framework for electronic seals, time stamping, electronic document acceptability, electronic delivery and website authentication.
- ensure minimal security level of trust services providers systems
- enforce obligation of notifications about security incidents at trust services providers

In Article 15 of the above mentioned draft regulation the EC proposes that trust services providers have to demonstrate due diligence, in relation to the identification of risks and adoption of appropriate security practices, and notify competent bodies of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein.

In this context, the European Union Agency for Network and Information Security (ENISA) developed in 2013 the *Guidelines for trust services providers*, discussing the minimal security levels to be maintained by the trust services providers. The study is split into three parts:

Security framework: describing the framework surrounding trust service providers (TPSs), focusing on EU standards, but taking into account others where relevant.

Risk assessment: discussing the principles and concepts of managing the risks applicaple to TSPs by defining and controlling threats and vulnerabilities.

Mitigating the impact of security incidents: recommending measures to mitigate the impact of security incidents on trust service providers (TSP) by proposing suitable technical and organisational means to handle the security risks posed to the TSP.

All three parts can also be used separately, as they address different issues and target different audience, so the introductory sections overlap.

This document, Part 2: Risk Assessement, covers the following aspects:

- Assets: identification, classification and evaluation
- Threats to assets: classification and evaluation
- Vulnerabilities present in the environment
- Probability or frequency of the threat
- The impact that the exposure can have on the organization
- Countermeasures that can reduce the impact
- The residual risk, risk acceptance, risk treatment plan, etc.

Table of Contents

1 The concept of Trust Service Providers

A trust service provider (TSP) is a supplier facilitating electronic security services to customers. The scope of such services includes, but is not limited to, electronic signatures and seals, electronic time stamps, and electronic authentication. Usually, these services rely on electronic certificates issued by certificate service providers (CSP) which is a type of TSP. For the sake of simplicity, we use the CSP as a running example for a TSP within the document at hand. All recommendations apply analogously to other types of TSP as well.

An electronic certificate (or certificate for short) is an electronic document that binds certain pieces of data together and is signed by a trusted third party that vows for the binding. For example, an attribute certificate binds an identity, such as a person, a service, or a device, to certain attributes, such as profession or access rights. Another example is a public key certificate that binds an identity to a public key. This certificate can then be used, amongst others, to verify the identity or signature of the certificate holder. In order to keep things understandable, we use public key certificates as running example throughout this document. All recommendations apply analogously to other types of certificates as well.

Electronic certificates rely on public key cryptography. In public key cryptography, two separate keys, mathematically linked, are provided to an entity. One of the keys is public and can be disseminated, while the other key is private and needs to be under the sole custody of the key pair owner. The private key cannot be derived by sole knowledge of the public key, but one key completes the other in terms of cryptographic operations. For example, a cipher text created using the public key can be decrypted using the private key; equally, the public key can be used to verify signatures that were created by the private key. Because of this property of public key cryptography, and by ensuring the secrecy of the private key and the authenticity of the public key, a relying party can verify that an entity presenting a certificate is who it claims to be or that a signature is valid.

However, a third party is needed to ensure that the information contained in the certificate, including the public key, is actually linked to the real identity of the entity. This is done by a TSP, which uses its so-called certificate authority (CA) signing keys to sign the entities' certificates. With this operation the TSP attests that the certificate was issued to the entity whose information is contained in it. Hence, we distinguish between two different types of certificates:

- Subject certificates, also called end entity certificates, that are used for day to day tasks such as authentication, signatures, or encryption. The holder of such a certificate is called the subject.
- CA signing certificates that are used to sign other certificates. Apart from signing subject certificates, CA certificates are often also used to sign other CA certificates to establish a trust relationship between CAs.

Electronic certificates can be used for a variety of purposes, some of the most common being to support electronic signatures, electronic seals or website authentication. Electronic signatures or seals are meant for natural persons (signatures) or legal entities (seals) to be able to produce digital signatures on documents or messages in order to ensure:

- The integrity of the document or message: attest that the document or message has not been altered.
- The authenticity and non-repudiation: attest that the document or message was produced by the certificate owner.

In the context of authentication, when an entity A presents itself to another entity B with its electronic certificate, entity B can verify that the entity A is actually who it claims to be by checking that entity A is in possession of the private key associated with the public key included in the certificate.

In the case of encryption, electronic certificates can also be used to provide confidentiality. The use of public key cryptography for the exchange of session keys ensures the confidentiality of the communication. Here, the session key is the entity that carries out the encryption of the messages.

The service of Certificate Service Providers can be broken down into the following component services

- Registration service: verifies the identity and, if applicable, any specific attributes of a subject. The results of this service are passed to the certificate generation service.
- Certificate generation service: creates and signs certificates based on the identity and other attributes verified by the registration service.
- Dissemination service: disseminates certificates to subjects, and if the subject consents, makes them available to relying parties. This service also makes available the CA's terms and conditions, and any published policy and practice information, to subscribers and relying parties.
- Revocation management service: processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the revocation status service.
- Revocation status service: provides certificate revocation status information to relying parties. This may be based upon certificate revocation lists or a real time service which provides status information on an individual basis. The status information may be updated on a regular basis and hence may not reflect the current status of the certificate.

and optionally:

- Subject device provision service: prepares and provides a signature-creation device to subjects.

2 Introduction to risk assessment

As the networked world continues to shape and impact every aspect of our lives, threats to the global industry continue in parallel.

Security management ensures that the risks are identified and an adequate control environment is established to mitigate these risks.

There is a need to manage the risks by defining and controlling threats and vulnerabilities. To achieve this, it is important to understand the principles behind the management of risk and the concepts underlying the risk management process. These principles and concepts will be discussed in this document. Interactions between them are depicted on Figure 1.

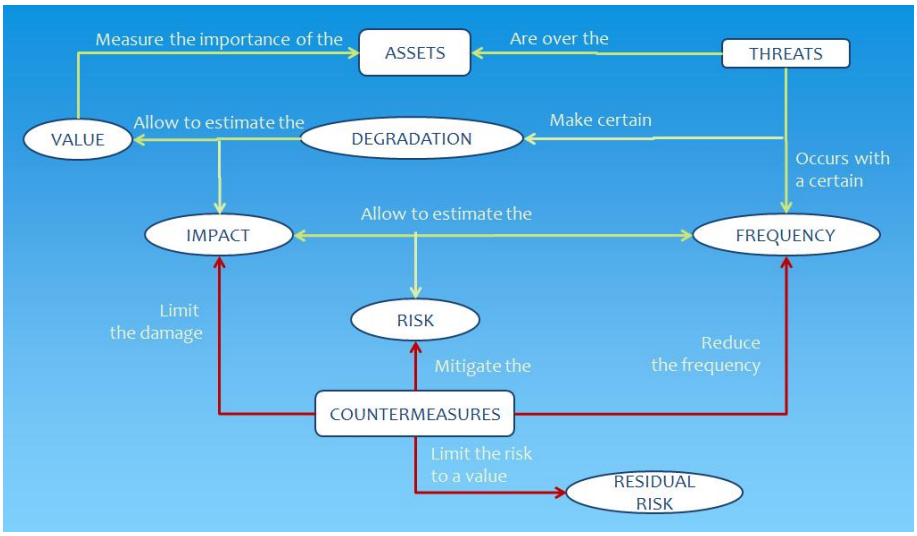

Figure 1 Concept of security risk management

Risk Assessment (also known as risk analysis) will evaluate:

- Assets: identification, classification and evaluation
- Threats to assets: classification and evaluation
- Vulnerabilities present in the environment
- Probability or frequency of the threat
- The impact that the exposure can have on the organization
- Countermeasures that can reduce the impact
- The residual risk, risk acceptance, risk treatment plan, etc.

Unlike risk assessments, vulnerability assessments tend to focus on technology aspects of an organization, such as networking or software applications. Through the use of different tools and methodologies, these assesments can provide information on the type and severity of vulnerability.

It´s also important to identify the risk avoidance, the risk transfer which is the ability to transfer the risk to another entity like an insurance company, the risk mitigation and the acceptance of the risk that can be based on a business decision.

3 Risk assessments on TSPs

In order to conduct a risk assessment, several methodologies exist. The goal of this report is not to describe in detail the different existing methods, but to provide a general overview of how a risk assessment is conducted and to identify risks specific to trust service providers that serve as a guide to assist providers when conducting an assessment.

For the purpose of the document, the risk assessment phases defined in ISO/IEC 27005:2008 (Information technology - Security techniques - Information security risk management) [2] are followed:

- Risk identification: Identifying the different factors (assets, threats, vulnerabilities, consequences and incident scenarios) that will identify and evaluate the risks:
    - System scope delimitation: Determining the scope included in the risk assessment and its boundaries
    - Asset identification: Identifying any type of item that has value to the organization and that could cause damage if it is involved in an incident.
    - Threat analysis: identifying all agents, either natural or human made, accidental or intentional, internal or external, that could pose a threat to the organization.
    - Vulnerability analysis: Identifying all potential weakness in the organization that could facilitate a successful attack and cause damage to the assets.
    - Consequence determination: Identifying the possible consequences that different events could have on the organization.
    - Incident scenario identification: Determining the possible events that could have an impact on the organization and that will serve as a base to identify the risks.
- Risk analysis: Determining the risk level based on the impact of each incident scenario and their probability of occurrence.
- Risk evaluation: Producing a scored list of all the identified risks, based on the risk analysis results; the business criteria; the affected assets and their vulnerabilities and the potential threats.

4 TSP infrastructure

The first step in the risk assessment process is to determine the scope included in the risk assessment and its boundaries. The TSP shall define the entities involved in the trust services it provides and the role of each entity.

To support the system scope delimitation process, a list of examples of common entities and processes involved in the operations of a TSP have been produced, which can be found below. This list is informative and should only be used as a generic reference.

4.1 The involved entities[2]

Certificate Authority: Certificate Authorities are entities that issue electronic certificates. TSPs issuing electronic certificates have one or several CAs. Certificate Authorities handle the whole certification lifecycle management process, with the exception of the registration process which is done by the Registration Authority. Commonly, Certificate Authorities generate and maintain their own key pair which they use to sign the certificates they issue. CAs act as a trust anchor: when a subject presents him/her certificate to a third party, it is the signature by a trusted CA in the subject certificate what ensures relying parties that the certificate is legitimated.

Registration Authority: The Registration Authority is the entity that verifies the certificate requester's identity to ensure the certificate is issued to the legitimate subject. Once the identity is verified, the RA sends a certificate request to the CA, who will then produce an electronic certificate and deliver it back to subject. The Registration Authority can be part of the TSP or it may be an external entity with some type of contract or agreement with the TSP. For example, a small TSP requiring physical presence of the subject may delegate this activity to an external CA as deploying a whole set of physical offices may not be feasible.

Subject: The subject is the entity who owns an electronic certificate issued by the TSP. A subject can be natural persons or legal entities. Subjects request certificates from TSPs which they use for many different purposes, such as electronic signatures, authentication or encryption. Subjects are bound to a certificate by the signature of the CA, who vows for their identity.

Relying party: The relying party is an entity that relies on the certificates issued by the CA to verify the subject identity or signature validity. Relying parties can be signature validation platforms, online services that use the digital certificates for authenticating users, browsers that validate web authentication certificates, end users, etc.

Validation Authority: The Validation Authority (VA) is an entity that provides information on the status of certificates to verify whether certificates are valid or not. There can be one or more VAs connected to each CA in the PKI. The VA shall be capable of storing information on the status of the certificates generated by one or more Certification Authorities (CAs).

The VA shall guarantee the non-repudiation of its responses. These responses are digitally-signed by the Validation Authority and specify the date and status (valid, revoked, cancelled or unknown) of a certificate and these results can be published e.g. via CRLs or OCSP.

Time-stamping Authority: The Time-stamping Authority (TSA) is the entity that provides a proof of existence for a particular data set at a particular time. This is usually used to verify that a digital signature was applied to a message for example, before the corresponding certificate was revoked

[2] Further definitions can be found in ISO/IEC 13335 [1], ISO/IEC 24760 [3], ISO/IEC Guide 73 [4], RFC 3647 [23], ETSI TS 102158 [14], ETSI TS 102042 [16], Directive 1999/93/EC [37]

thus allowing a revoked public key certificate to be used for verifying signatures created prior to the time of revocation.

The TSA shall generate a digitally-signed time-stamp that includes the time of the request; the information that securely binds the stamp to the electronic document; and a unique registration number for auditing purposes.

4.2 The involved processes[3]

This is a list of the main processes involved in the most commonly used TSP operations. The list is informative and should only be used as a generic reference.

The registration process: The registration process is the initial process by which the subject goes to the registration authority to request a certificate. The subject presents a proof of identity and the RA sends a certificate request to the CA which upon production of the certificate delivers it back to the subject.

The key management process: The key management process comprises all the processes which are in place to manage the key pairs of the CAs, VAs and TSAs mainly during its complete lifecycle:

- The key pair generation
- The key pair storage, backup and recovery
- The certificate dissemination
- The key pair usage
- The key pair destruction
- The key renewal, rekey and update
- Key archive

The subject key management process: The subject key management process comprises all the processes that are in place to manage the keys of the subject during their lifetime:

- The subject key generation
- The subject key device provisioning
- The subject key storage, backup and recovery
- The subject key renewal, rekey and update
- The subject key dissemination
- The subject key destruction

The subject certificate management process: The subject certificate management process comprises all the processes that are in place to manage the subject certificate:

- The subject certificate generation
- The subject certificate delivery
- The subject certificate renewal, rekey and update
- The subject certificate dissemination

The revocation process: The revocation process comprises all actions from the revocation request to the revocation publication in the certificate revocation status service.

[3] Please also refer to the "Guidelines for trust service providers – Mitigating the impact of security incidents"

The validation process: The validation process comprises all actions from users or trust service providers on requesting / providing the status of the digital certificates. This can be done e.g. through:

- CRL (Certificate Revocation List)
- OCSP (Online Certificate Status Protocol)

The time stamping process: The time stamping process comprises all action from users and trust service providers that want to add time stamps to electronic documents or transactions.

The information and condition process: These processes comprise all actions to protect external and internally the TSP infrastructure.

The operational process: These operational processes comprise all actions related to procedures and policies established by the TSP to perform its activities.

4.3 Determine assets

In a risk assessment context, assets are what the organization needs to protect. Assets are not only physical, tangible items that the organization can easily classify in terms of monetary value. The information that the organization produces or gathers is an important asset as well as the trust relationships and reputation as examples of intangible assets.

All assets shall be identified and listed. Each asset shall be assigned an owner to determine who finally has the responsibility for the protection and maintenance of that asset.

The assets shall be categorized based on their type and characteristics.

Once assets have been identified, the next step is to determine their value, together with the asset owner. An asset's value can be determined based on the negative consequences an incident affecting them may have for the organization. This can be qualitative (recommended) and quantitative (money).

In the case of TSPs, an example of a critical asset would be the CA private key. An incident involving the confidentiality or integrity of the CA private key could have very damaging consequences for the TSP. For example, a malicious individual could impersonate the CA and generate fraudulent certificates. Therefore, the value of the CA private key would certainly be estimated by any TSP as very high. Following this approach, the TSP shall conduct an evaluation of the value of all the identified assets.

To support the asset identification process, some examples of common assets TSPs own, are listed below. The list is informative and should only be used as a generic reference. The TSP shall have a list of assets and their value which corresponds to its actual business and operational environment. The list has been organized following the guidelines provided in the ISO 27005 [2], which divides assets in two categories:

- Primary assets, which comprise the information assets and the business processes.
- Supporting assets, which comprise software, hardware, network, personnel and locations.

Primary assets

Information assets: Information assets include all data that are handled by the TSP, either produced by it or handled by third parties. In this category the TSP should include at least all the information related to the certificates (public and private keys, certificate content, etc.) as well as all the logs of the system (CA operation logs, OCSP logs, etc.). Examples of information assets in a TSP are:

- CA certificate
- CA private key
- RA certificate
- RA private key
- VA certificate
- VA private key
- TSA certificate
- TSA 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: The TSP should identify all the business processes that are conducted in the organization. The list should include all certificate lifecycle management processes, plus any additional processes the TSP may have depending on the additional services (validation, preservation, etc.) that the organization is offering. Examples of business processes in a TSP are:

- 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 VA key pair generation
- The VA key pair storage, backup and recovery
- The VA certificate dissemination
- The VA key pair usage
- The VA private key destruction
- The TSA key pair generation
- The TSA key pair storage, backup and recovery
- The TSA certificate dissemination
- The TSA key pair usage
- The TSA 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 validation management process
- The revocation management process
- The revocation status dissemination process

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

Supporting assets

Software, hardware and networks: The TSP shall include in the asset inventory all software applications; all hardware infrastructures (servers, user equipment, cryptographic modules, etc.) and all network infrastructures that are used in the TSP. Examples of software, hardware and networks assets are:

- Hardware
  - CA equipment: servers for CA root and subordinates CAs
  - Other CA necessary equipment, e.g. LDAP
  - RA equipment: PCs, printers, etc.
  - VA equipment
  - TSA equipment
  - Subject devices: smartcards, USB tokens, etc.
  - Hardware Security Modules (HSMs)
  - Web servers
- Software
  - CA key management applications
  - CA backup applications
  - Other CA applications
  - RA applications
  - VA management applications
  - TSA management applications
- Network Infrastructure
  - Communication lines

Locations and sites: The TSP shall 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

Personnel: The TSP shall 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 for CA, VA and TSA
- Other operational roles
- RA operators
- Different administrators at OS, DB, etc. level

Other assets: The TSP should identify all other assets not included in the above categories that have a value for the organization. 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

4.4 Identify threats

Following an identification of the assets and value assigned, a threat analysis should be conducted. Identification of threats is an important step in the risk assessment cycle because a threat is the potential for a particular threat-source to successfully exercise a particular vulnerability on an asset.

Once threats have been identified, the next step is to estimate the probability of occurrence. Probability of occurrence of each threat is one of the aspects that influence the overall risk score for each incident scenario. It shall be determined, in cooperation with other members in the organization, the probability of occurrence of each threat based on:

- Motivation of the threat agent behind each threat
- Exploited vulnerabilities by the threat and existing countermeasures
- Analysis of past events

For example, a TSP whose facilities are located on seismic activity area should rate the probability of occurrence of a seismic event higher than one that is located in a non-seismic area.

Threats can be accidental or intentional, human made or natural, internal or external, technical or physical. To support the threat identification process, we have produced examples of common threats TSPs may face, which can be found below. The list is informative and should only be used as a generic reference. The TSP shall have a list of potential threats and their probability of occurrence which corresponds to its actual business and operational environment.

Natural hazards: The TSP should identify natural hazards that are present in the area where its locations are set, and based on factors like statistical analysis of previous occurrence, determine their likelihood. Some examples of natural hazards that can be a threat to the TSP operation are:

- Seismic or hydrological events
- Fire
- Water damage or corrosion
- Electromagnetic phenomena
- Windstorms

Essential services: The TSP should examine the contracts with providers of essential services, such as electricity, communication lines, etc. to determine the service level agreements in terms of downtime. Past history of loss of essential services in the organization should be taken into account.

Some examples of essential service hazards that can be a threat to the TSP operation are:

- Disruption of essential services like electricity, communications or air conditioning.
- Disruption due to the impact of downtime of in-house services in the data centre

Human made threats: The TSP should determine, based on the type of services it is providing, the possible human made threats. For example, whether the provider is operating in public networks or internal networks will have an impact on the probability of materialization of certain human threats. Some examples of human made hazards that can be a threat to the TSP operation are:

- Theft or loss of equipment
- Theft or loss of data
- Accidental destruction of equipment
- Accidental destruction of data
- Tampering of equipment
- Tampering of data
- Malicious software

- Eavesdropping
- Cryptanalysis

Threat agents: Intentional threats are caused by threat agents. Human made threats are usually classified in terms of intentional or accidental, although in some cases natural hazards and loss of essential services can also be intentionally caused by a threat agent. Additionally to threats, threats agents are also important to be considered (especially their motivation and their opportunity). Some examples of threat agents are:

- Hackers
- Computer criminals
- Intelligence organizations
- Disgruntled employees
- Terrorists

4.5 Analyse vulnerabilities

Identifying possible vulnerabilities is a key step in risk management, as they constitute the possible weakness of an asset or group of assets that can be exploited by one or more threats.

For example, storage of the private key of the certificate subject in a non-tamper resistant device can be a potential vulnerability, which would affect a group of assets (subject device, subject private key) and that could be exploited by a threat (tampering of equipment or data) and lead to a consequence (compromise of the subject private key). Therefore, in order to determine potential vulnerabilities, the TSP assets and the existing threats shall be taken into account.

To support the vulnerability identification process, we have produced examples of potential vulnerabilities of TSPs. The list is informative and should only be used as a generic reference. The TSP risk analysis shall include a list of potential vulnerabilities which corresponds to its actual business and operational environment.

Vulnerabilities in the registration process

Subject registration: Vulnerabilities in the registration process may arise from the failure of a proper verification of the subject identity during the registration or from an inadequate policy (or lack or enforcement) for proof of identity, which could lead to the success of an impersonation attack.

Registration Authority: Aside from an inadequate subject registration process, the RA can be a source of vulnerabilities that may lead to fraudulent certificate requests. Inadequate protection against malicious software could lead to intruders accessing the RA information systems in order to issue a fraudulent certificate request to the CA, or it could cause accidental malfunction of the systems, which would interrupt the issuance of certificates. A lack of protection of the RA key could also cause fraudulent certificate requests. Additionally, vulnerabilities in the communication channel between the CA and the RA can cause fraudulent requests of certificates, alteration of requests, etc. by malicious individuals. Examples of vulnerabilities in the registration process are:

- 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

Registration records: RAs shall keep adequate records of the registration documents, as deficiencies in the archival of registration records by the RA could lead to repudiation by the certificate subject. Examples of vulnerabilities in the accountability of the registration process are:

- Lack of appropriate procedures for registration documents archival
- Insufficient protection of registration records

Vulnerabilities in the TSP key management process

The TSP key management process refers to the key generation, backup and recovery, storage, usage, destruction, etc. processes of the entities involved in the TSP, like the Certification Authority (CA), the Validation Authority (VA) and the Time Stamping Authority (TSA) as the main actors involved in these processes.

Key pair generation: The key pair shall be generated in a highly secure way. From a cryptographic point of view, vulnerabilities in the key generation may exist if the chosen algorithm and key length (or other parameters) are not strong enough for the needed level of security. Cryptographic algorithms are under constant study by cryptographers who periodically discover possible attacks which lead to the algorithms being replaced. Additionally, generation of the key pair in an insecure physical or logical environment may lead to its loss or theft. Examples of vulnerabilities in the key pair generation:

- The signing key is generated with a weak key generation algorithm or insufficient key length (or other parameters) for the TSP business requirements
- Attack vectors that make the cryptographic algorithms used to generate the key pair insecure are discovered
- Key is generated in a non-secure physical or logical environment
- Usage of insecure random number generator
- Selection of weak algorithm (or parameters) the keys are generated for
- Key generation is not performed by trusted individuals

Key pair storage, backup and recovery: After its generation, the signing keys shall be protected during their whole life cycle to avoid their loss or theft. Vulnerabilities in the key lifecycle management come from a lack of physical or logical protection of the private key. Examples of vulnerabilities in the key pair storage, backup and recovery process:

- 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 (e.g. access protection, integrity, …)
- Private keys are disposed or archived in non-secure manner
- Private key restore can be performed in a non-secure manner

Certificate dissemination: Certificate is disseminated publicly in order for third parties to be able to validate the signature on subjects' certificates. Lack of appropriate security measures to guarantee the integrity and authenticity of the distributed public key may lead to an impersonation by a malicious individual, who could them generate fake certificates. Examples of vulnerabilities in the certificate dissemination process:

- Certificate is not disseminated in a way that can guarantee its integrity and authenticity
- Setting wrong attributes in the certificate, such as policy mapping or path length constraints

Key pair usage: Signing keys are used to sign subjects' certificates. In the signing process the private key is activated and therefore can be subject to attacks. Examples of vulnerabilities in the key 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 as CWA 14167-1 [26a] indicates.
- Insecure processes or applications may lead to sending fake data / certificates to be signed

Vulnerabilities in the subject key management process

Subject key pair generation: Key pairs can be generated in the subject device or by the CA that afterwards delivers it to the subject. If the key pair is generated by the CA and then delivered to the subject, either by electronic or physical means, any vulnerability in the delivery process could lead to a compromise of the subject private key. Another source of vulnerabilities in the subject key generation may exist if the chosen algorithm and key length (or other parameters) are not strong enough for the CA needed level of security. Examples of vulnerabilities in the subject's certificate generation process:

- Subject key is generated with a weak algorithm or insufficient key length (or other parameters) for the TSP or subject business requirements
- Attack vectors that make the cryptographic algorithms used to generate the subject key pair insecure are discovered
- Subject key is generated in a non-secure physical or logical environment
- Usage of insecure or weak random number generator
- Selection of weak algorithm (or parameters) the keys are generated for
- Subject key generation is not performed by trusted individuals
- Unsecure delivery of key pair to subject (Only if CA generates key pair)
- Failure to properly verify identity of subject when key pair is delivered (Only if CA generates key pair)
- Unsecure retraction of undeliverable keys

Subjects device provisioning: The subject device (or signature creation device, hardware or software) is where the subject private key is generated and the cryptographic operations with the certificates are performed. The security features of the subject device are important to guarantee confidentiality and integrity of the private key and the cryptographic operations. Inappropriate security characteristics of the subject's device for the TSP needed assurance level may lead to liability of the TSP in case of a breach. When the subject device is a cryptographic device, such as a token or a smart card, it is usually provisioned by the TSP from an external party, usually a manufacturer. A source of vulnerabilities would be the failure to verify the authenticity of the subject's device or its security features. Examples of vulnerabilities in the subject's device provisioning process:

- 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

Subject key pair usage: Subject key pair activation, both in software or hardware format, should be protected by PIN or password to ensure that it is not conducted fraudulently. The subject shall, as

well, handle diligently its key pair to avoid misuse. Examples of vulnerabilities in the subject's private key usage are:

- 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

Vulnerabilities in the subject certificate management process

Subject certificate generation and delivery to subject: Certificates are generated by the CA following standardized formats. The CA then signs the certificate and delivers it to the subject, either physically or electronically. The CA shall ensure that the certificate is delivered to the legitimate subject. Examples of vulnerabilities in the subject's certificate generation process:

- Unsecure delivery of certificate to subject
- Failure to properly verify identity of subject when certificate is delivered
- Tampering with the certificate before it reaches the subject, e.g. during transport
- Failure in retracting undeliverable certificate, e.g. revocation
- Failure to support subject's platform properly (i.e. Linux, Windows, Mac, Android, iOS, etc.), leads to loss of availability.
- Failure to generate certificate with correct contents according to policies.

Subject certificate dissemination: Subjects' certificates may be disseminated to relying parties after subject consent. Failure of consent may lead to a breach of personal data protection regulations. Additionally, if the certificate repository is not disseminated with the appropriate security levels, certificates could be fraudulently accessed. Examples of vulnerabilities in the subject's certificate dissemination:

- Subject consent is not obtained before disseminating the certificate
- Subject certificate repository is not secured
- Certificate repository is not up to date

Vulnerabilities in the revocation management process

Certificate revocation management process: The certificate revocation management process deals with the complete workflow from the request of a revocation by any party to the inclusion of the revocation in the certificate revocation status service. Vulnerabilities may arise from a lack of a clear policy that states who can request revocation and under which circumstances. Additionally, the absence of a policy on the procedure that should be followed may lead to delays in the revocation that could facilitate a fraudulent use of the certificate. Other vulnerabilities come from a lack of mechanisms to guarantee the integrity and authenticity of revocation requests which may lead to forging requests or repudiation of the request by the originator. Examples of vulnerabilities in the certificate revocation management process are:

- 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

Certificate revocation status dissemination: TSPs disseminate the revocation status of their issued certificates periodically. The update frequency of the list of revoked certificates should be reflected in the TSP policies. Failure to disseminate certificate revocation status in the agreed timeframe could

lead to revoked certificates being used in a fraudulent way. Lack of appropriate security measures to guarantee the integrity and authenticity of the distributed certificate revocation list may lead to forgery by a malicious individual. Examples of vulnerabilities in the certificate revocation status dissemination process are:

- 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
- Failure to update the status of the certificate
- Failure to check revocation status by relying parties
- Failure (e.g. downtime, DOS) of revocation dissemination service

Vulnerabilities in the validation process

Certificate validation management process: The certificate validation management process deals with the complete workflow from the request of a validation of a certificate by any party to the response with the status of the certificate to the requester. Vulnerabilities may arise from a lack of a clear policy and technical issues on the procedure that should be followed, that may produce delays or incorrect answers that could facilitate a fraudulent use of the certificate. Other vulnerabilities come from a lack of mechanisms to guarantee the non-repudiation of the answers. Examples of vulnerabilities in the certificate validation management process are:

- Lack of appropriate validation procedures
- Failure to produce and publish CRLs
- Differences between OCSP and CRLs responses
- Insecure request and response channels
- Lack of a logging system to monitor the system status

Vulnerabilities in the time stamping process

Time stamping management process: The time stamping management process deals with the complete workflow from the request to provide a time stamp token in order to indicate that a data set existed at a particular point in time. Vulnerabilities may arise from the use of a no trustworthy source of time or a lack of procedures and policies. Examples of vulnerabilities in the time stamping process are:

- Lack of use of a trustworthy source of time
- Insecure request and response channels
- Lack of a logging system to monitor the system status

Vulnerabilities in the TSP information and communication systems

TSP software applications: All TSP applications need to be trustworthy, updated and protected. Lack of protection of TSP applications from malicious software could be exploited by intruders to access TSP operation related systems, or it could cause accidental malfunction of the systems. Examples of vulnerabilities in the TSP software are:

- Lack of appropriate measures to protect TSP operation from malicious software
- Lack of disaster recovery and business continuity plans
- Lack of a logical perimeter security to protect TSP systems
- 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.

TSP hardware components: For a TSP, hardware vulnerabilities may arise from the lack of redundancy of hardware in case of a natural disaster, from accidental hardware malfunction or from hardware deterioration due to natural hazards. Examples of vulnerabilities in the TSP hardware are:

- Lack of appropriate measures to protect equipment from environmental threats
- Lack of appropriate measures to protect equipment from theft or tempering
- Lack of secure equipment storage facilities
- Lack of (automated) status testing
- Lack of incident response protocols/policies

TSP communication networks: Communication networks are critical in several aspects of the TSP operation, such as the communication with the RA or the dissemination of the certificate revocation status. A lack of proper dimensioning of the communication networks of the TSP could lead to the inability to issue certificates or to publish revocation status. Examples of vulnerabilities in the TSP communication networks:

- Inadequate dimensioning of the communication networks
- Lack of logical protection of communication networks
- Lack of (automated) status testing
- Lack of incident response protocols/policies

TSP systems audit logs: Lack of audit logging procedures on operations conducted over the TSP systems supporting all business processes could lead to a loss of accountability of users' actions in case of a security incident. Even if an appropriate logging policy exists and it is enforced, lack of protection of logs against accidental or intentional alteration or destruction can have the same consequences. Examples of vulnerabilities related to audit logs are:

- Lack of appropriate audit logging policies
- Insufficient protection of audit logs

Vulnerabilities affecting the TSP operation

TSP policies: TSP shall have clear policies regarding the whole certification management processes. They shall produce, enforce and make available to subjects, at least, a Certification Policy and a Certification Practice Statement which states their policies, procedures and operational controls. Examples of vulnerabilities affecting TSP policies are:

- Nonexistence of a Certification Policy or a Certification Practice Statement
- Certification Policy or Certification Practice Statement don't match business objectives
- Certification Policy or Certification Practice Statement don't address properly the level of risk
- Lack of an Information Security Policy
- Lack of appropriate contractual agreements with external RAs and third parties
- Bad policy enforcement
- Insufficient policy updates
- Policies not made available to concerned parties
- CP or CPS don't match 3rd party requirements (for example CA/B Forum requirements for web certificates)

TSP operational procedures: TSP policies shall be enforced through operational procedures followed on daily operations to avoid security incidents. Examples of vulnerabilities affecting CA operational procedures are:

- Lack of Standard Operational Procedures for TSP operations
- Lack of Incident Response Procedures
- Lack of Business Continuity and Contingency Plans
- Lack of quality assurance plans for issued certificates

TSP personnel: TSP personnel, especially those whose work in the TSP operations (trusted roles), shall have an appropriate level of training and experience in order to avoid potential errors that could cause compromise or malfunction of systems. A lack of separation of duties or incorrect audit procedures can lead to abuse of the system without detection by the organization. Examples of vulnerabilities affecting CA personnel are:

- 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

TSP facilities: Physical vulnerabilities derive from a lack of appropriate protection of the TSP facilities, especially those dealing with CA operations. Malicious activities in the perimeter or natural hazards can lead to a compromise or malfunction of TSP systems or assets. Examples of vulnerabilities affecting TSP facilities are:

- Physically insecure CA key generation environment
- Lack of a secure perimeter to protect CA operation areas
- Lack of protection measures from natural hazards
- Lack of contingency plans against loss of essential services

4.6 Identify existing controls

The list of potential vulnerabilities should be contrasted with the list of existing controls. Existing controls are the means of mitigating the probability of exploiting potential vulnerabilities as they decrease the level of exposure. The TSP shall conduct a gap analysis to determine for which vulnerabilities no sufficient controls are in place.

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

This section presents a set of minimum security measures (it can be used ETSI EN 319 412 [11] family of standards control specific for TSPs or more generic, the ISO 27000 [2] family of standards controls) that can be used as a reference for all TSPs issuing electronic certificates, regardless of their certification scope or qualification status.

Security measures in the registration process

Subject registration

- Proof of identity, as stated in the Certificate Practice Statement, is required during the registration phase.

- All registration records (supporting documents for the registration process) are kept under security measures to guarantee their confidentiality and integrity, and shall follow data protection regulations.
- The RA systems are protected against malicious software.
- The communication channel between RA and CA is secured to ensure the confidentiality, integrity and authenticity of certificate requests.
- RA systems are protected against unauthorized access
- RA logging, auditing and supervision procedures are in place and up to date
- Skilled/trained trustworthy personnel

Security measures in the TSP key management process

Key pair generation

- Signing key pair is generated in a secure physical and logical environment.
- Signing key pair is generated with key generation algorithm and key length (or other parameters) appropriate.
- Signing key pair generation is conducted only by trusted roles and under at least a dual person control.
- Signing key is generated in a secure cryptographic device.
- Signing key is kept secret and under sole control of CA
- Usage of secure and strong random number generator
- Selection of strong algorithm (or parameters) the keys are generated for

Key pair storage, backup and recovery

- The private signing key is stored in a secure device.
- All operations related to storage, backup and recovery of the private signing key are subject to the same security measures as the key generation.
- The private key is kept in a physically and logical secure environment.
- The private signing key should be backed up.
- Back-up copies of the private signing key are subject to the same security measures as the primary key.

Certificate dissemination

- Certificate is disseminated in a way that guarantees its integrity, authenticity and availability.

Key pair usage

- The signing key is used for subject certificate signing.
- The signing key is used for self-signing or cross-signing
- The signing key may be also used to sign other type of certificates
- The signing key is used to sign revocation status
- The signing keys are used to sign the CA, VA or TSA operations
- Key pair activation is performed only by trusted roles under at least dual control and shall only be used within physically secure premises

Security measures in the subject key management process

Subject key pair generation

- Subject key pair is generated with a key generation algorithm and key length (or other parameters) deemed appropriate for the TSP signing purposes and business requirements.

- The secrecy of the key is maintained (only if CA generates key pair).
- The key is destroyed (or kept under strict controls if the CA policy allows so) upon delivery to the subject (only if CA generates key pair).
- Delivery of key pair to subject is performed in a secure manner (only if CA generates key pair).
- The identity of the subject is verified upon delivery (only if CA generates key pair).
- The key pair is destroyed (or kept under strict controls if the CA policy allows so) if undeliverable
- Usage of secure and strong random number generator
- Selection of strong algorithm (or parameters) the keys are generated for

Subject's device provisioning process

- Subjects' devices are stored securely and delivered securely to the subject to avoid any kind of tampering.
- When the subject signature device is provisioned externally, the TSP ensures the authenticity of the hardware before delivery to the subject.
- The security characteristics of the subject signature device are verified by the TSP and deemed appropriate for the TSP and subject business requirements.
- If the subject device is activated by a PIN or pass phrase, they are distributed through secure channels.

Security measures in the subject certificate management process

Delivery of the certificate to the subject

- The certificate is delivered to the subject in a manner that guarantees its confidentiality.
- The TSP supervises that the certificate is delivered to the legitimate subject and that it is under his/her sole control.
- The TSP retracts the certificate if undeliverable

Subject certificate dissemination

- The subject certificate is accessible to third parties only upon the subject consent.
- The certificate repository is maintained securely.
- Subjects' certificates and terms and conditions are available to authorized parties on a 24x7 basis.

Subject certificate usage

- The subject is provided guidelines regarding the correct handling of the certificate and its usage

Security measures in the revocation management process

Certificate revocation management service

- The TSP has an enforced policy for revocation request that includes:
  - Who can request revocation
  - Under which circumstances
  - The maximum time frame between a revocation request and the publication in the certificate revocation dissemination service.
- The authenticity of certificate revocation requests is checked.

- If the certificate subject is not the source of the certificate revocation request, this shall be informed of the request.
- The channel established with the certificate revocation requester is secure.
- The TSP is able to revoke any certificate that it has issued, even after a disaster.
- All events related to a certificate revocation request are logged.

Certificate revocation status dissemination service

- Certificate revocation status is disseminated with the update frequency stated in the Certificate Practice Statement.
- When certificate revocation is disseminated through CRLs, the authenticity and integrity of the CRL is ensured, by, for example, an electronic signature of the list.
- Certificate revocation status service is available to relying parties on a 24x7 basis.
- The channel between the revocation management service and the certificate revocation status service is secured and the authenticity of the messages ensured.
- When certificate revocation status requests are made through an online service, the responses are signed by the CA to guarantee their integrity and contain the exact time.
- All events related to certificate revocation status requests or accesses to the CRLs are logged.

Security measures in the validation process

Certificate validation management service

- The TSP has a policy for validation requests
- To guarantee the non-repudiation of the response, responses shall be digitally signed by the VA
- The channel established with the certificate validation requester is secure.
- The TSP is able to validate any certificate that it has issued
- All events related to a certificate validation request are logged.

Security measures in the time stamping process

Time stamping management service

- The TSP has a policy for time stamping requests
- The time stamp token shall be digitally signed and include:
  - The time of the request
  - The information that securely binds the time stamp to the electronic document
  - A unique registration number for auditing purposes
- The channel established with the requester is secure
- To use a trustworthy source of time
- All events related to a certificate time stamp request are logged.

Security measures in the TSP information and communication systems

TSP software

- The TSP software applications implement appropriate measures against infection with malicious software.
- Software applications related to CA operation (CA key lifecycle management, subject certificate management and revocation management) are logically separated from other TSP applications.

- TSP software applications are separated from public networks by the appropriate perimeter security mechanisms to restrict the visibility among internal and external hosts.
- The TSP implements access right management procedures to ensure user accounts to access information systems are properly managed.
- All users are authenticated and shall possess adequate authorization before granted to access the TSP information systems and their actions shall be logged.
- The TSP conducts periodical vulnerability assessments to detect potential security flaws in its information systems.
- The TSP has an enforced audit logging policy. The policy shall state:
    - The events recorded
    - The security measures applied to protect them
    - The roles authorized to access and modify logs
    - The retention time for logs
- The TSP logs at least the following events:
    - All login events (successful and unsuccessful) to CA operation related systems (CA key lifecycle management, subject certificate generation and revocation management).
    - All changes to the audit function.
    - All key generation, key usage, cert generation, revocation, … (basically everything)
- All audit logs are protected from unauthorized modification and all changes to the audit functions should be recorded.
- Logs should contain at least who, when, what, where …
- TSP software is kept up to date with security fixes.

TSP hardware

- Equipment is protected from environmental threats.
- Equipment is protected from theft and tampering by implementing the appropriate physical security measures.
- The TSP maintains a hardware inventory.
- Equipment which is not in use shall be stored in locked facilities separated from public areas.
- Security sensitive hardware, such as HSMs, smartcards, etc., are certified with appropriate levels (CC [42], FIPS [36], …)
- Any information with might remain on hardware to be disposed is securely destroyed, e.g. wiping and shredding of hard disks.

TSP communication networks

- The TSP communication networks are protected to ensure confidentiality and integrity of the information transmitted.
- The TSP has taken the appropriate measures to ensure the communication networks are sufficient to handle the TSP traffic and are redundant in case of a disaster.

Security measures in the TSP operation

TSP policies

- The TSP has produced and approved a Certification Policy and a Certification Practice Statement.
- The TSP has verified that the Certification Policy and the Certification Practice Statement match business requirements and objectives.

- The TSP has produced and approved an Information Security Policy and a Business Continuity Plan
- Policies are enforced

TSP operational procedures

- The TSP has produced and regularly tests and reviews business continuity plans to ensure continuity of operations after incidents.
- The TSP has backup procedures.
- Backed up data are stored in an area physically separated from primary information processing facilities.
- Backed up data are logically and physically protected from unauthorized access.
- The TSP has produced and maintains an incident response plan which clearly states responsibilities in incident management.
- The TSP keeps a record of incidents and reviews this information periodically to ensure the implementation of corrective measures.

TSP personnel

- The TSP has produced documents that clearly state job descriptions, especially those related to trusted roles operating the CA operation related systems (CA key lifecycle management, subject certificate generation and revocation management).
- TSP personnel receive the appropriate training regarding security procedures.
- The TSP implements a policy of separation of duties among trusted roles.
- Background checking of personnel in security sensitive areas
- Adequate (technical and organizational) supervision of personnel

TSP facilities

- TSP facilities are protected from unauthorized access.
- TSP facilities are protected from natural hazards such as fire and flooding.
- CA operation related activities (CA key lifecycle management, subject certificate generation and revocation management) are conducted in physically protected areas with access only by authorized individuals.
- The TSP has produced and maintains contingence plans to respond to essential services failure (electricity, air conditioning).

4.7 Determine consequences

A consequence is defined as the "outcome of an event affecting objectives". Therefore, consequences don't need to be necessarily negative. Consequences are identified in order to be able to determine the risk rating. The impact of each incident scenario will be evaluated based on the consequences it may have for the TSP.

The following list identifies some of the consequences that different incidents may have on the TSP operation.

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 inability to check the validity of certificates. Compromises of the CA or RA can also lead to 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' willing 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.

Loss of qualification status: Lack of compliance with qualification requirements, failure to conduct the necessary audits or negligence in managing the security of the certificate lifecycle can lead to the loss of qualification status.

4.8 Identify incident scenarios[4]

Having the input from identified assets, threats, vulnerabilities and consequences, the next step is to identify the list of risks, formulated like possible incident scenarios. These incident scenarios are used in the risk assessment, and combined with likelihood and impact finally determine the risk scenarios.

Examples of incident scenarios are (some incident scenarios are repeated as they may affect more than one entity):

Incidents affecting CAs

- Compromise of a CA

[4] Please also refer to the "Guidelines for trust service providers – Mitigating the impact of security incidents"

- Compromise of the cryptographic algorithms or use of inadequate key lengths (or other parameters)
- Compromise of the revocation systems
- Repudiation claim by certificate subject
- Accidental loss of availability of the certification services
- Personal data breach

Incidents affecting RAs

- Compromise of a RA
- Impersonation
- Repudiation claim by certificate subject
- Personal data breach

Incidents affecting the subject certificate

- Compromise of the subject's key pair
- Compromise of the cryptographic algorithms or use of inadequate key lengths (or other parameters)
- Repudiation claim by certificate subject
- Personal data breach

Incidents affecting VAs

- Compromise of the VA
- Compromise of the cryptographic algorithms or use of inadequate key lengths (or other parameters)
- Accidental loss of availability of the validation services

Incidents affecting TSAs

- Compromise of the TSA
- Compromise of the cryptographic algorithms or use of inadequate key lengths (or other parameters)
- Accidental loss of availability of the time stamping services

5 Analyse risk

Once all the parameters that influence the risk calculation have been identified (assets, threats, vulnerabilities, existing controls, consequences, and incident scenarios) the TSP has enough information to start the risk analysis process. Risk analysis (the term risk analysis is sometimes interchanged with risk assessment) is defined as a systematic use of information to identify sources and to estimate the risk, where source is defined as an item or activity having a potential for a consequence (ISO/IEC Guide 73 [4]).

Risk assessment also takes into account special circumstances under which assets may require additional protection, such as with regulatory compliance.

During the risk analysis phase the TSP will use all the identified sources (assets, vulnerabilities, threats) to estimate the risk, in terms of impact and probability.

5.1 Assess impact

Impact is defined as the result of an unwanted incident (ISO/IEC PDTR 13335-1). Impact can be measured by the consequences the incident has on the organization assets, for example:

- Loss of availability
- Loss of integrity
- Loss of confidentiality
- Loss of accountability
- Non legal compliance
- Financial loss
- Loss of reputation

During the next step of the risk assessment process, the TSP needs to determine the possible consequences of each identified incident scenario and the impact it would have on the TSP assets. For this purpose, a mapping between the identified incident scenarios and the consequences should be undertaken, in order to link each incident scenario with its possible consequences. Based on the potential consequences, for each incident scenario the level of impact can be determined.

In June and July 2013 ENISA conducted a questionnaire-based survey among trust services providers, in which 46 participants took part. It had for goal to identify security practices in force at these organisations[5].

The survey asked to rate the potential impact for the trust service providers of identified incident scenarios. Results are depicted in Figure 2. The values represent the average impact score (from 0 – “no impact” to 10 – “maximal impact”) assigned by the respondents.

[5] For the in-depth description of the study, please refer to the document “TSP services, standards and risk analysis report”, ENISA 2013. The participants are mentioned in the acknowledgements at the beginning of this document.

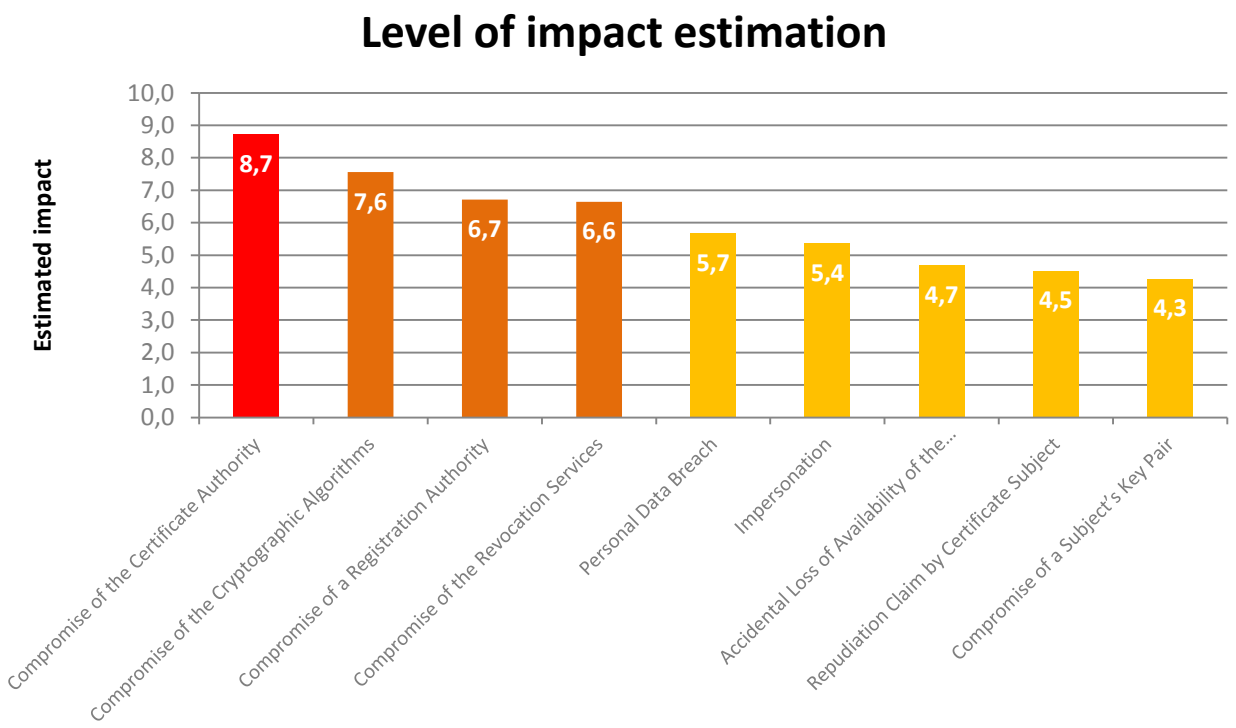

Figure 2: Estimated impact (based on survey results)

5.2 Assess probablility

Probability is defined as the extent to which an event is likely to occur (ENISA). To determine the probability of occurrence, each incident scenario should be mapped against:

- The possible threats that could cause the incident and their probability of occurrence
- The vulnerabilities that could be exploited for the incident to take occur
- The existing controls in place that mitigate and reduce the exposure to the vulnerabilities

Taking into account all these parameters, each incident scenario should be assigned a probability score. ENISA survey on security practices of trust services providers asked to rate the identified incident scenarios in terms of probability of occurrence for any certification service provider (0 – "no risk", 10 – "maximal probability"). Probability values in the Figure 3 represent the median impact score assigned by the trust service providers participating in the survey

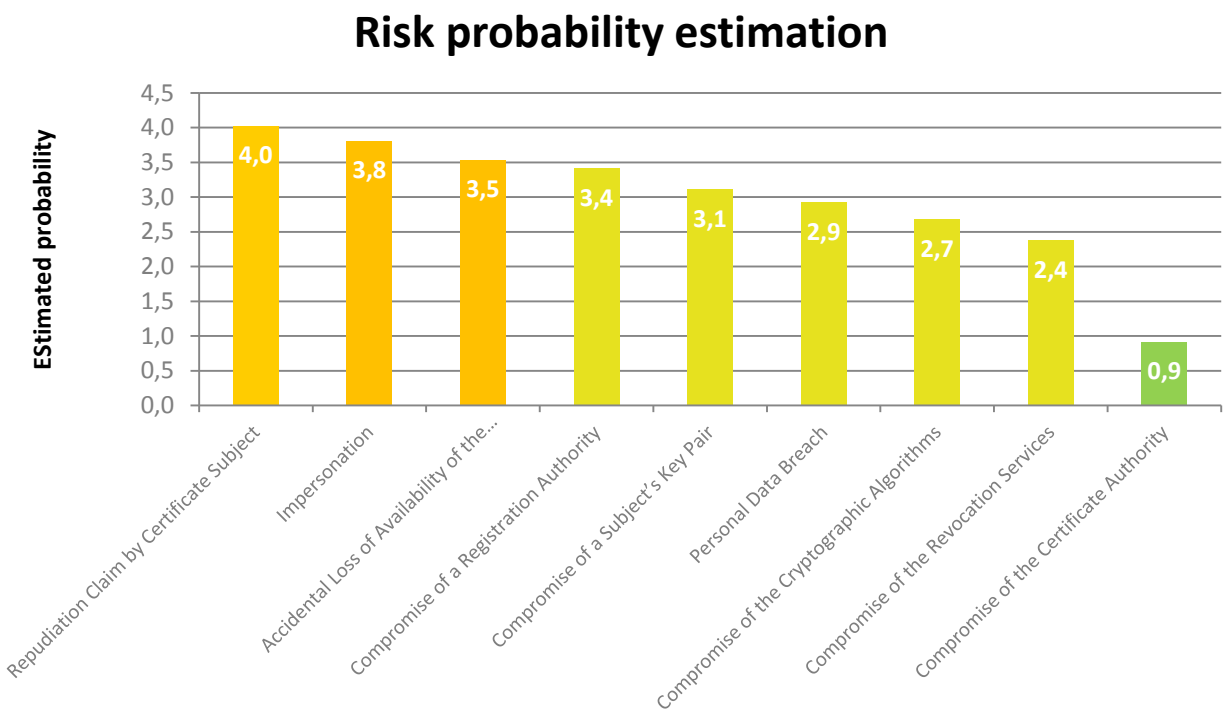

Figure 3: Estimated probability (based on survey results)

This figure shows that the probability of a compromise of a CA is quite small taking into account that this scenario is one of the worst that can happen to a TSP and according to the survey is indicated by the TSPs that one scenario which is likely to occur is the repudiation claim done by the certificate subject, mainly, claiming didn´t request for a certificate.

The answers of respondents (depicted by colours) show that the probability of these scenarios is judged being unlikely to occur.

5.3 Estimate level of risk

Risk estimation is defined as the process used to assign values to the probability and consequences of a risk (ENISA). The level of risk is determined as a combination of the expected impact of the incident and the likelihood of occurrence. Different weighting scores can be assigned to the assigned impact / likelihood pair of each incident scenario.

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

Based on the identified impact and probability scores on ENISA survey responses, the identified risks would have the level of risk depicted on the Figure 4 (values as on Figures 2 and 3).

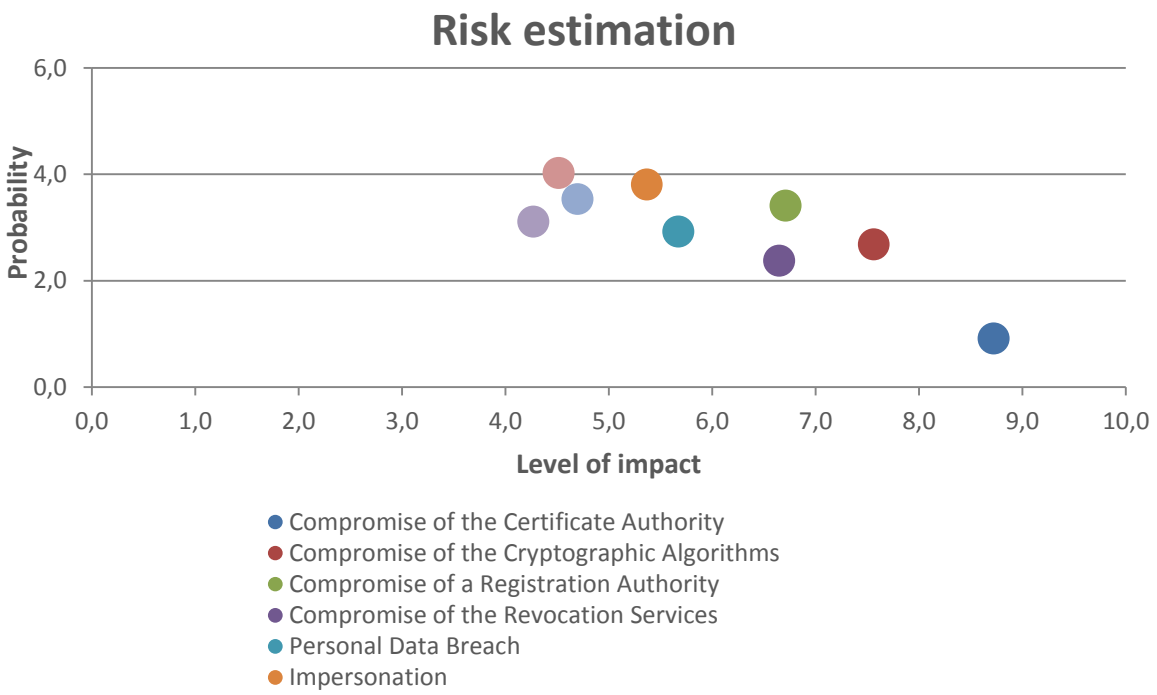

Figure 4 Risk level estimation (based on survey results)

This figure shows the level of impact caused by these possible scenarios and indicates that the compromise of a CA has the highest level of impact in the TSP business followed by a compromise of the cryptographic algorithms.

On the other hand, the compromise of a subject key pair and the claiming to repudiate the certificate subject has a low level of impact in the TSP business.

This level of risk shall be reduced by applying the correspondent countermeasures.

6 Evaluate risk

Risk evaluation is the process of comparing the estimated risk against given risk criteria to determine the significance of risk (ISO/IEC Guide 73 [4]).

Risk criteria can include associated cost and benefits, legal and statutory requirements, socio-economic aspects, the concerns of stakeholders, priorities and other inputs to the assessment (ISO/IEC Guide 73 [4]). Risk criteria are closely linked to the TSP business environment and should be determined by the TSP.

To support the risk evaluation process, we have produced examples of evaluations, based solely on the risk estimation, of the main risks TSPs face, which can be found below. The list is informative and should only be used as a reference. The TSP shall produce their own risk universe which corresponds to its actual business and operational environment, including the risk criteria of its own organization in the final evaluation.

For each identified risk, a description and a characterization has been made, in order to provide a better understanding of the factors the that can have any effect on the potential materialization of the risk. The following factors have been taken into account:

- Description: Brief description of the characteristics of the identified risk and its likelihood and impact score.
- Related assets: Examples of the assets that could be affected by the incident scenarios involved in the risk.
- Possible vulnerabilities: Examples of vulnerabilities that, if being exploited, could lead for a materialization of the risk.
- Potential threats: Examples of threats that could cause the materialization of the risk.
- Possible consequences: Examples of consequences that the materialization of the risk could have.

Risk 1: Compromise of a Certification Authority

Probability **Very unlikely**

Impact **Very high**

Description: A compromise of the CA consists on 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.

Related assets

- CA private key
- CA key generation process
- CA key management process
- Hardware Security Modules (HSMs)
- CA certificate management applications
- CA key management process
- CA trusted roles

Possible vulnerabilities

- CA key is generated in a non-secure physical or logical environment

- CA signing key is generated with a weak key generation algorithm or insufficient key length (or other parameters) for the TSP business requirements
- CA private signing key is not kept in a physically or logical secure environment
- CA private signing key is not backed up
- Back-up copies of the CA private signing key are not stored securely
- CA key generation is not performed by trusted individuals
- CA key is not generated in a secure device
- CA private keys are disposed or archived in non-secure manner
- CA private signing key is not kept in a physically or logical secure environment
- Lack of enforcement of the information security policy in the CA
- Lack of technical measures to protect the CA from malicious software
- Usage of insecure or weak random number generator
- Selection of weak algorithm (or parameters) the keys are generated for
- Lack of appropriate software to protect the CA operations from malicious software

Potential threats

- All intentional human made threats

Possible consequences

- Fraudulent issuance of subjects' certificates
- Inability to issue subject's certificates
- Inability to use valid certificates
- Liability
- Loss of reputation
- Loss of qualification status

Risk 2: Compromise of the cryptographic algorithms

Probability **Unlikely**

Impact **High**

Description: 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.

Related assets

- CA private key
- RA private key
- Subjects' private keys
- Subjects', CAs and RAs certificates

Related vulnerabilities

- CA signing key is generated with a weak key generation algorithm or insufficient key length (or other parameters) for the TSP business requirements
- Attack vectors that make the cryptographic algorithms used to generate the CA key pair insecure are discovered.
- Subject key is generated with a weak algorithm or insufficient key length (or other parameters) for the TSP business requirements

- Attack vectors that make the cryptographic algorithms used to generate the subject key pair insecure are discovered
- Attack vectors against certificate signature algorithms making it possible to forge certificates
- Usage of insecure or weak random number generator
- Selection of weak algorithm (or parameters) the keys are generated for

Potential threats

- All intentional human made threats

Possible consequences

- Fraudulent use of valid certificates
- Inability to issue subjects' certificates
- Inability to use valid certificates
- Repudiation by certificate subject
- Loss of accountability of actions
- Loss of reputation

Risk 3: Compromise of a Registration Authority

Probability	**Unlikely**
Impact	**High**

Description: A compromise of the RA consists on 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.

Related assets

- RA certificate
- RA private key
- The registration process
- RA applications
- RA equipment
- RA offices
- RA operators

Related vulnerabilities

- Lack of appropriate software to protect the RA operation from malicious software
- Lack of appropriate protection of the RA private key
- Lack of adequate protection of the RA private key
- Insecure communication channel between the RA and the CA

Potential threats

- All intentional human made threats

Possible consequences

- Fraudulent issuance of subjects' certificates
- Inability to issue subjects' certificates
- Inability to use valid certificates

- Repudiation by certificate subject
- Liability
- Loss of reputation
- Loss of qualification status

Risk 4: Compromise of the revocation services

Probability **Unlikely**

Impact **High**

Description: 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.

Related assets

- Certificate revocation status request logs
- RA applications
- Certificate revocation lists
- CA equipment
- The revocation management process
- Other CA operational roles
- The revocation status dissemination process
- RA operators
- CA revocation management applications
- Validation servers

Related vulnerabilities

- 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
- Insecure dissemination of the certificate revocation list
- Lack of appropriate measures to protect CA operation from malicious software
- Lack of a logical perimeter security to protect CA systems
- Lack of logical protection of communication networks
- Lack of enforcement of the information security policy
- Lack of proper patch management rendering servers vulnerable to intrusion.

Potential threats

- All intentional human made threats

Possible consequences

- Fraudulent use of revoked certificates
- Inability to use valid certificates
- Inability to revoke certificates
- Repudiation by certificate subject
- Liability
- Loss of reputation
- Loss of qualification status

Risk 5: Personal data breach

Probability **Unlikely**

Impact **Medium**

Description: 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.

Related assets

- Subjects' certificates
- Registration archives
- Other CA applications
- RA applications
- RA operators
- RA offices

Possible vulnerabilities

- Lack of appropriate software to protect the RA operation from malicious software
- Unsecure communication channel between RA and CA
- Unsecure delivery of certificate to subject
- Lack of appropriate procedures for registration documents archival
- Insufficient protection of registration records
- Lack of appropriate measures to protect CA operation from malicious software
- Lack of enforcement of the information security policy

Potential threats

- Unintentional or intentional human made threats

Possible consequences

- Legal sanctions
- Loss of reputation

Risk 6: Impersonation

Probability **Possible**

Impact **Medium**

Description: Impersonation occurs when a malicious individual attempts to supplant another individual personal identity or to fraudulently claim legal representation of an organization in order to obtain a rogue electronic certificate perform some fraudulent actions.

Related assets

- The registration process
- RA operators

Related vulnerabilities

- Lack of appropriate verification of subject's identity
- Lack of appropriate policy for subject's registration procedure

Potential threats

- All intentional human made threats

Consequences

- Fraudulent issuance of subjects' certificates
- Inability to use valid certificates
- Liability
- Loss of reputation

Risk 7: Loss of availability of the certification services

Probability **Possible**

Impact **Medium**

Description: 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 of the affected systems, different processes of the TSP will be interrupted, resulting in possible financial and reputational loss.

Affected assets

- The CA key pair storage, backup and recovery
- The CA key pair usage
- CA key management applications
- RA applications
- CA Backup applications
- CA equipment
- RA equipment
- Network Infrastructure
- CA primary premises
- CA back up sites
- RA offices

Possible vulnerabilities

- CA private signing key is not backed up
- Lack of appropriate measures to protect CA operation from malicious software
- Lack of disaster recovery and business continuity plans
- Lack of a logical perimeter security to protect CA systems
- Lack of appropriate measures to protect equipment from environmental threats
- Lack of appropriate measures to protect equipment from theft
- Inadequate dimensioning of the communication networks
- Lack of logical protection of communication networks
- Lack of Business Continuity and Contingency Plans
- Lack of protection measures from natural hazards
- Lack of contingency plans against loss of essential services

Potential threats

- Natural hazards
- Loss of essential services
- Unintentional human made threats

Possible consequences

- Inability to issue subjects' certificates
- Inability to use valid certificates
- Inability to revoke certificates
- Loss of reputation

Risk 8: Repudiation claim by certificate subject

Probability **Possible**

Impact **Medium**

Description: 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.

Related assets

- Registration archives
- The registration process
- The subject's certificate generation process
- Subject devices
- Audit logs

Related vulnerabilities

- Unsecure delivery of certificate to subject
- Failure to verify the authenticity of the subject's device
- Inappropriate security characteristics of the subject's device for the TSP needed assurance level
- Subject key is generated with a weak algorithm or insufficient key length (or other parameters) for the TSP business requirements
- Lack of appropriate policies for the revocation process
- Lack of appropriate procedures for registration documents archival
- Insufficient protection of registration records
- Usage of insecure or weak random number generator
- Selection of weak algorithm (or parameters) the keys are generated for

Potential threats

- Unintentional or intentional human made threats

Possible consequences

- Repudiation by certificate subject
- Liability
- Loss of reputation
- Loss of qualification status

Risk 9: Compromise of a subject's key pair

Probability **Unlikely**

Impact **Medium**

Description: A compromise of a subject key pair consists on 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.

Related assets

- Subjects' private keys
- The subject's key pair generation process
- The subject's device provisioning process
- The subject key pair usage

Related vulnerabilities

- Unsecure delivery of certificate to subject
- Failure to verify the authenticity of the subject's device
- Inappropriate security characteristics of the subject's device for the TSP needed assurance level
- Subjects' failure to submit revocation request

Potential threats

- All intentional human made threats

Possible consequences

- Fraudulent use of valid certificates
- Liability
- Loss of reputation
- Loss of qualification status

Risk 10: Compromise of a Validation Authority

Probability **Very unlikely**

Impact **Very high**

Description: A compromise of the VA consists of an unauthorized intrusion in the VA information systems or any type of unauthorized access to its private key. A VA compromise may lead to fraudulent validation of subjects' certificates, the impossibility to validate certificates, or to an interruption in the validation of certificates.

Related assets

- VA private key
- VA key management process
- Hardware Security Modules (HSMs)
- VA certificate management applications
- VA key management process
- VA trusted roles

Possible vulnerabilities

- VA key is generated in a non-secure physical or logical environment

- VA signing key is generated with a weak algorithm or insufficient key length (or other parameters) for the TSP business requirements
- VA private signing key is not kept in a physically or logical secure environment
- VA private signing key is not backed up
- Back-up copies of the VA private signing key are not stored securely
- VA key generation is not performed by trusted individuals
- VA key is not generated in a secure device
- VA private keys are disposed or archived in non-secure manner
- VA private signing key is not kept in a physically or logical secure environment
- Lack of enforcement of the information security policy in the VA
- Lack of technical measures to protect the VA from malicious software
- Lack of technical measures to protect the communication channel between the VA and the requester
- Differences between the CRL and the OCSP
- Usage of insecure or weak random number generator
- Selection of weak algorithm (or parameters) the keys are generated for
- Lack of appropriate software to protect the VA operations from malicious software

Potential threats

- All intentional human made threats

Possible consequences

- Fraudulent validation of subjects' certificates
- Inability to validate subject's certificates
- Inability to use valid certificates
- Liability
- Loss of reputation
- Loss of qualification status

Risk 11: Compromise of a Time Stamping Authority

Probability **Very unlikely**

Impact **High**

Description: A compromise of the TSA consists of an unauthorized intrusion in the TSA information systems or any type of unauthorized access to its private key. A TSA compromise may lead to fraudulent issuance of time stamping tokens.

Related assets

- TSA private key
- TSA key management process
- Hardware Security Modules (HSMs)
- TSA certificate management applications
- TSA key management process
- TSA trusted roles

Possible vulnerabilities

- TSA key is generated in a non-secure physical or logical environment

- TSA signing key is generated with a weak algorithm or insufficient key length (or other parameters) for the TSP business requirements
- TSA private signing key is not kept in a physically or logical secure environment
- TSA private signing key is not backed up
- Back-up copies of the TSA private signing key are not stored securely
- TSA key generation is not performed by trusted individuals
- TSA key is not generated in a secure device
- TSA private keys are disposed or archived in non-secure manner
- TSA private signing key is not kept in a physically or logical secure environment
- Lack of enforcement of the information security policy in the TSA
- Lack of technical measures to protect the TSA from malicious software
- Lack of technical measures to protect the communication channel between the TSA and the requester
- Lack of use of a trustworthy source of time
- Usage of insecure or weak random number generator
- Selection of weak algorithm (or parameters) the keys are generated for
- Lack of appropriate software to protect the TSA operations from malicious software

Potential threats

- All intentional human made threats

Possible consequences

- Fraudulent issuance of time stamp tokens
- Liability
- Loss of reputation
- Loss of qualification status

7 Conclusions

In this document we discussed the principles and concepts of managing the risks applicaple to TSPs by defining and controlling threats and vulnerabilities.

Security management ensures that the risks are identified and an adequate control environment is established to mitigate these risks. There is a need to manage the risks by defining and controlling threats and vulnerabilities. To achieve this, it is important to understand the principles behind the management of risk and the concepts underlying the risk management process.

The choice of the appropriate methodology to perform the risk assessment should be made by the organisation itself. This study has provided a general overview of how a risk assessment can be conducted and how to identify risks specific to trust service providers. It can serve as a guide to assist providers when conducting an assessment.

Annex 1 – Definitions

Asset: any person, facility, material, information or activity that has value to the organization, its business operations and their continuity, including Information resources that support the organization's mission.

Authentication: process that allows the validation of the electronic identification of a natural or legal person; or of the origin and integrity of an electronic data;

Certificate: Electronic attestation which links electronic signature or seal validation data of a natural or a legal person respectively to the certificate and confirms those data of that person;

Certification Authority: An entity trusted to issue certificates. A certification service provider may have one or several Certificate Authorities. It is generally a trusted party or trusted third party that accepts the responsibility of managing the certificate process by issuing, distributing and verifying certificates.

Certification Service Provider: An entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.

Contingency Plan: A plan for emergency response, backup operations, and post-disaster recovery in a system, as part of a security program, to ensure availability of critical system resources and facilitate continuity of operations in a crisis.

Cryptographic module: An umbrella term covering:

- cryptographic algorithms (e.g. encryption, hashing, key generation, ...)
- cryptographic parameters (e.g. key length, elliptic curve, ...)
- cryptographic protocols (e.g. key exchange, ...)
- cryptographic implementations (e.g. software libraries, HSMs, …)

Data Availability: The fact that data is accessible and services are operational. It can be described as the property of being accessible and useable upon demand by an authorized entity. In the context of service level agreements, availability generally refers to the degree to which a system may suffer degradation or interruption in its service to the customer as a consequence of failures of one or more of its parts.

Data Confidentiality: The protection of communications or stored data against interception and reading by unauthorized persons. Confidentiality means keeping the content of information secret from all entities except those that are authorized to access it.

Data Integrity: The confirmation that data which has been sent, received, or stored are complete and unchanged, which implies that the items of interest (facts, data, attributes etc.) have not been subject to manipulation by unauthorized entities.

Electronic seal: Data in electronic form which are attached to or logically associated with other electronic data to ensure the origin and the integrity of the associated data; (Proposal eSignatures)

Electronic Signature: Data in electronic form which is attached to or logically associated to other electronic data and serves as a method of authentication.

From a legal perspective, an electronic signature is not necessarily considered equivalent to a handwritten signature. When it meets a number of conditions, it can be put on par with a handwritten one.

Event: Occurrence of a particular set of circumstances

Evidence: Information that either by itself or when used in conjunction with other information is used to establish proof about an event or action. Evidence does not necessarily prove truth or existence of something but contributes to establish proof.

Hash Function: A mathematical function which maps values from a large (possibly very large) domain into a smaller range. A "good" hash function is such that the results of applying the function to a set of values in the domain will be evenly distributed and apparently at random over the range.

Impact: The result of an incident.

Incident: An event that has been assessed as having an actual or potentially adverse effect on the security or performance of a system.

Mitigation: Limitation of any negative consequence of a particular event

Probability: Extent to which an event is likely to occur.

Private Key: In a public key cryptosystem, that key of a user's key pair which is known only by that user

Public Key: In a public key cryptosystem, that key of a user's key pair which is publicly known.

Public Key Infrastructure (PKI): The infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.

Relying Party: A user or agent that relies on the data in a certificate in making decisions.

Risk: The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.

Risk Analysis: A process that examines an organization´s information resources, its existing controls, and its remaining organization and computer system vulnerabilities.

Risk Assessment: A process used to identify and evaluate risk and their potential effects

Risk Management: The discipline of identifying and measuring security risks associated with an information system, and controlling and reducing those risks to an acceptable level. The goal of risk management is to invest organizational resources to mitigate security risks in a cost-effective manner, while enabling timely and effective mission accomplishment.

Signature Creation Data: Unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature

Signature Creation Device: Configured software or hardware used to create an electronic signature

Subject: Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate.

Threat: Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Trust Service: Any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals

Vulnerability: The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.

Annex 2 – Abbreviations

CA Certification Authority

CABF CA/Browser Forum

CC Common Criteria

CEN European Committee for Standardization (Comité Européen de Normalisation)

CIMC Certificate Issuance and Management Components

CP Certificate Policy

CPS Certification Practice Statement

CRL Certificate Revocation List

CSP Certification Service Provider

CWA CEN Workshop Agreement

EAL Evaluation Assurance Level

ECC Elliptic Curve Cryptography

ECDSA Elliptic Curve Digital Signature Algorithm

EN European Standard

ETSI European Telecommunications Standards Institute

FIPS Federal Information Processing Standards

GCD Greatest Common Divider

HSM Hardware Security Module

HTTP Hypertext Transfer Protocol

HTTPS HTTP Secure

HW Hardware

ISO International Organization for Standardization

NIST National Institute of Standards and Technology

OCSP Online Certificate Status Protocol

PDS PKI Disclosure Statement

PIN Personal Identification Number

PKI Public Key Infrastructure

PP Protection Profile

PSE Personal Security Environment

QCP Qualified Certificate Policy

RA Registration Authority

RFC Requests For Comments

RSA Rivest, Shamir and Adleman, the persons who first described the algorithm

SHA Secure Hash Algorithm

SSCD Secure Signature Creation Device

SW Software

TLS/SSL Transport Layer Security/Secure Socket Layer protocol

TS (ETSI) Technical Specification

TSA Time Stamping Authority

TSP Trust Service Providers

TR (ETSI) Technical Report

VA Validation Authority

Annex 3 – Bibliography

ISO

[1] ISO/IEC 13335-1:2004 Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management
[2] ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management
[3] ISO/IEC 24760:2011 Information technology - Security techniques - A framework for identity management
[4] ISO/IEC Guide 73 Risk management – Vocabulary – Guidelines for use in standards
[5] ISO/IEC 9594-8:2008 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks
[6] ISO/IEC 27000:2009 Information technology – Security techniques – Information security management systems – Overview and vocabulary
[7] ISO/IEC 17021 Conformity assessment -- requirements for bodies providing audit and certification of management systems
[8] ISO/IEC 10118-3:2004 Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions
[9] ISO/IEC 15408 Series: Information technology -- Security techniques -- Evaluation criteria for IT security. It consists of three parts:
- [9a] ISO/IEC 15408-1:2009 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408.
- [9b] ISO/IEC 15408-2:2008 defines the content and presentation of the security functional requirements to be assessed in a security evaluation using ISO/IEC 15408
- [9c] ISO/IEC 15408-3:2008 defines the assurance requirements of the evaluation criteria.

ETSI

[10] ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting electronic signatures - http://www.etsi.org/deliver/etsi_en/319400_319499/319401/01.01.01_20/en_319401v010101c.pdf
[11] ETSI EN 319 412 Profiles for TSPs issuing Certificates
- [11a] 319 412-1: Overview and common data structures
- [11b] 319 412-2: Certificate profile for certificates issued to natural persons
- [11c] 319 412-3: Certificate profile for certificates issued to legal persons
- [11d] 319 412-4: Certificate profile for web site certificates issued to organisations
- [11e] 319 412-5: Qualified certificate statements for qualified certificate profiles

[12] ETSI TS 101 456 Policy requirements for certification authorities issuing qualified certificates: http://www.etsi.org/deliver/etsi_ts/101400_101499/101456/01.04.03_60/ts_101456v010403p.pdf
[13] TR 102 437 Guidance on TS 101 456 (Policy Requirements for certification authorities issuing qualified certificates) http://www.etsi.org/deliver/etsi_ts/101800_101899/101862/01.03.03_60/ts_101862v010303p.pdf

[14]TS 102 158 Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates http://www.etsi.org/deliver/etsi_ts/102100_102199/102158/01.01.01_60/ts_102158v010101p.pdf
[15]TR 102 040 International Harmonization of Policy Requirements for CAs issuing Certificates http://www.etsi.org/deliver/etsi_tr/102000_102099/102040/01.03.01_60/tr_102040v010301p.pdf
[16]ETSI TS 102 042 Policy requirements for certification authorities issuing public key certificates: http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/01.01.01_60/ts_102042v010101p.pdf
[17]ETSI TS 101 862 Qualified Certificate profile: http://www.etsi.org/deliver/etsi_ts/101800_101899/101862/01.03.03_60/ts_101862v010303p.pdf
[18]ETSI TS 102 176-1 Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms http://www.etsi.org/deliver/etsi_ts/102100_102199/10217601/02.00.00_60/ts_10217601v020000p.pdf
[19]TR 119 300 Business Driven Guidance for Cryptographic Suites
[20]TS 119 312 Cryptographic Suites for Secure Electronic Signatures
[21]EN 319 403 Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

IETF

[22]RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile http://www.ietf.org/rfc/rfc5280.txt
[23]RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework http://www.ietf.org/rfc/rfc3647.txt
[24]RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP http://www.ietf.org/rfc/rfc2560.txt
[25]RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP http://www.rfc-editor.org/rfc/rfc6960.txt

CEN

[26]CWA 14167 Security requirements for trustworthy systems managing certificates for electronic signatures:
[26a] CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14167-01-2003-Jun.pdf
[26b] CWA 14167-2 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP) ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14167-02-2004-May.pdf
[26c] CWA 14167-3 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)

ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14167-03-2004-May.pdf

[26d] CWA 14167-4 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14167-04-2004-May.pdf

NOTE: CEN Workshop Agreement 14167 is currently under revision to become the basis of a European Norm in CEN TC 224.

[27] CWA 14169 Secure Signature-creation devices 'EAL 4+' ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14169-00-2004-Mar.pdf

[28] CWA 14355 Guidelines for the implementation of Secure Signature-Creation Devices Description ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14355-00-2004-Mar.pdf

[29] CWA 14170 Security requirements for signature creation applications ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14170-00-2004-May.pdf

[30] CWA 14890 Application Interface for smart cards used as Secure Signature Creation Devices

[30a] CWA 14890-1: Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements

[30b] CWA 14890-2: Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services

[31] CWA 14172 European Electronic Signature Standardisation Initiative (EESSI) Conformity Assessment Guidance. It is divided in 8 parts:

[31a] CWA 14172-1: EESSI Conformity Assessment Guidance - Part 1: General introduction ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-01-2004-Mar.pdf

[31b] CWA 14172-2: EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-02-2004-Mar.pdf

[31c] CWA 14172-3: EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-03-2004-Mar.pdf

[31d] CWA 14172-4: EESSI Conformity Assessment Guidance - Part 4: Signature-creation applications and general guidelines for electronic signature verification ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-04-2004-Mar.pdf

[31e] CWA 14172-5: EESSI Conformity Assessment Guidance - Part 5: Secure signature-creation devices ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-05-2004-Mar.pdf

[31f] CWA 14172-6: EESSI Conformity Assessment Guidance - Part 6: Signature-creation device supporting signatures other than qualified ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-06-2004-Mar.pdf

[31g] CWA 14172-7: EESSI Conformity Assessment Guidance - Part 7: Cryptographic modules used by Certification Service Providers for signing operations and key generation services ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-07-2004-Mar.pdf

[31h] CWA 14172-8: EESSI Conformity Assessment Guidance - Part 8: Time-stamping Authority services and processes ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-08-2004-Mar.pdf

CA/B Forum

[32] Baseline requirements for the issuance and management of publicly-trusted certificates version 1.1.6 https://www.cabforum.org/Baseline_Requirements_V1_1_6.pdf

[33] EV SSL certificate guidelines version 1.4.3 https://www.cabforum.org/Guidelines_v1_4_3.pdf

NIST

[34] Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths: http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

[35] NIST: Discussion Draft of the Preliminary Cybersecurity Framework, August 28, 2013. http://www.nist.gov/itl/cyberframework.cfm

[36] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules". http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexd.pdf

Legislation

[37] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:PDF

[38] Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:EN:PDF

[39] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data: http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm

Others

[40] EU Trusted Lists of Certification Service Providers: https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers

[41] Trust Service Principles and Criteria for Certification Authorities Version 2.0: http://www.cica.ca/resources-and-member-benefits/growing-your-firm/trust-services/item10797.pdf

[42] The common criteria framework: http://www.commoncriteriaportal.org/

[43]Notification with regard to electronic signatures in accordance with the Electronic Signatures Act and the Electronic Signatures Ordinance http://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/Areas/ElectronicSignature/PublicationsNotifications/SuitableAlgorithms/2012_algokatpdf.pdf?__blob=publicationFile
[44]PKCS #1: RSA Cryptography Standard: http://www.rsa.com/rsalabs/node.asp?id=2125
[45]ECRYPT II European Network of Excellence in Cryptology II: http://www.ecrypt.eu.org/documents/D.SPA.20.pdf
[46]RIPEMD (RACE Integrity Primitives Evaluation Message Digest): http://homes.esat.kuleuven.be/~bosselae/ripemd160.html
[47]Fox-IT – RSA-512 Certificates abused in the wild. https://www.fox-it.com/en/blog/rsa-512-certificates-abused-in-the-wild/
[48]Smartfacts – Factoring RSA keys from certified smart cards: Coppersmith in the wild. http://smartfacts.cr.yp.to/smartfacts-20130916.pdf
[49]ANSI X9.79 Public Key Infrastructure (PKI) - Practices and Policy Framework
[50]CIMC Protection Profile: http://www.commoncriteriaportal.org/files/ppfiles/cert-issu-v15-sec-eng.pdf
[51]EIFv2: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

European Commission standardisation mandate

[1] Standardisation mandate to the European standardisation organisations CEN, CENELEC and ETSI in the field of information and communication technologies applied to electronic signatures: http://www.etsi.org/images/files/ECMandates/m460.pdf

Under this mandate, the following standards are being developed at the moment of publication of this document:

- TR 1 19 000 Rationalised structure for electronic signature standardisation
- TR 4 19 010 Extended rationalised structure including IAS
- SR 0 19 020 Rationalised Framework of Standards for Advanced Electronic Signatures in Mobile Environment
- TR 4 19 030 Rationalised structure for electronic signature standardisation - Best practices for SMEs
- TR 4 19 040 Rationalised structure for electronic signature standardisation - Guidelines for citizens
- TR 1 19 100 Business driven guidance for signature creation and validation
- TS 1 19 101, EN 3 19 101 Policy and security requirements for signature creation and validation
- EN 3 19 102 Procedures for signature creation and validation
- EN 4 19 103 Conformity assessment for signature creation and validation applications (and procedures)
- TS 1 19 104 General requirements on testing compliance and interoperability of signature creation and validation
- EN 4 19 111 Protection profiles for signature creation and validation application
- EN 3 19 122 CAdES - CMS advanced electronic signatures
- TS 1 19 124 CAdES testing compliance conformance & interoperability
- EN 3 19 132 XAdES - XML advanced electronic signatures
- TS 1 19 134 XAdES testing compliance conformance & interoperability
- EN 3 19 142 PAdES - PDF advanced electronic signatures
- TS 1 19 144 PAdES testing compliance conformance & interoperability

- TS/EN 13 19 152 Architecture for Advanced electronic signatures in mobile environments
- TS 1 19 154 Testing compliance conformance and interoperability of AdES in mobile environments
- EN 3 19 162 ASiC - Associated signature containers
- TS 1 19 164 ASiC testing compliance conformance and Interoperability
- EN 3 19 172 Signature policies
- TS 1 19 174 Testing compliance and interoperability of signature policies
- TR 4 19 200 Business driven guidance for signature creation and other related devices
- EN 4 19 203 Conformity assessment of secure devices and trustworthy systems
- EN 4 19 211 Protection profiles for secure signature creation devices
- EN 4 19 212 Application interfaces for secure signature creation devices
- EN 4 19 221 Security requirements for trustworthy systems managing certificates for electronic signatures
- EN 4 19 231 Security requirements for trustworthy systems supporting time-stamping
- EN 4 19 241 Security requirements for trustworthy systems supporting server signing (signature generation services
- EN 4 19 251 Protection profiles for authentication device
- EN 4 19 261 Security requirements for trustworthy systems managing certificates for electronic signatures
- TR 1 19 300 Business driven guidance for cryptographic suites
- TS 1 19 312 Cryptographic suites for secure electronic signatures
- TR 1 19 400 Business driven guidance for TSPs supporting electronic signatures
- EN 3 19 401 General policy requirements for TSPs supporting electronic signatures
- EN 3 19 403 Requirements for conformity assessment bodies assessing Trust Service ProvidersGeneral requirements and guidance for conformity assessment of TSPs supporting e-signatures
- EN 3 19 411 Policy and security requirements for TSPs issuing certificates
- EN 3 19 412 Profiles for TSPs issuing certificates
- EN 3 19 413 Conformity assessment for TSPs issuing certificates
- EN 3 19 421 Policy and security requirements for TSPs providing time-stamping services
- EN 3 19 422 Profiles for TSPs providing time-stamping services
- EN 3 19 423 Conformity assessment for TSP providing time-stamping services
- EN 3 19 431 Policy and security requirements for TSPs providing signature generation services
- EN 3 19 432 Profiles for TSPs providing signature generation services
- EN 3 19 433 Conformity assessment for TSPs providing signature generation services
- EN 3 19 441 Policy and security requirements for TSPs providing signature validation services
- EN 3 19 442 Profiles for TSPs providing signature validation services
- EN 3 19 443 Conformity assessment for TSPs providing signature validation services
- TR 1 19 500 Business driven guidance for trust application service providers
- EN 3 19 503 General requirements and guidance for conformity assessment of trust application service providers
- TS 1 19 504 General requirements for testing compliance and interoperability of trust application service providers
- EN 3 19 511 Policy and security requirements for registered electronic mail (REM) service providers
- EN 3 19 512 Registered electronic mail (REM) services
- EN 3 19 513 Conformity assessment for REM service providers

- TS 1 19 514 Testing compliance and interoperability of REM service providers
- EN 3 19 521 Policy and security requirements for data preservation service providers
- EN 3 19 522 Data preservation services through signing
- EN 3 19 523 Conformity assessment of data preservation service providers
- SR 0 19 530 Study on standardisation requirements for e-delivery services applying e-signatures
- TR 1 19 600 Business driven guidance for trust service status lists providers
- EN 3 19 601 General policy and security requirements for trust service status lists providers
- EN 3 19 602 Trust service status lists format
- EN 3 19 603 General requirements and guidance for conformity assessment of trust service status lists providers
- TS 1 19 604 General requirements for testing compliance and interoperability of trust service status lists providers
- EN 3 19 611 Policy and security requirements for trusted lists providers
- EN 3 19 612 Trusted lists format
- EN 3 19 613 Conformity assessment of trusted list providers
- TS 1 19 614 Testing compliance and interoperability of trusted lists

NOTE:

For the purpose of the document, the risk assessment phases defined in [2]are followed:

- Risk identification: Identifying the different factors (assets, threats, vulnerabilities, consequences and incident scenarios) that will identify and evaluate the risks:
    - System scope delimitation: Determining the scope included in the risk assessment and its boundaries
    - Asset identification: Identifying any type of item that has value to the organization and that could cause damage if it is involved in an incident.
    - Threat analysis: identifying all agents, either natural or human made, accidental or intentional, internal or external, that could pose a threat to the organization.
    - Vulnerability analysis: Identifying all potential weakness in the organization that could facilitate a successful attack and cause damage to the assets.
    - Consequence determination: Identifying the possible consequences that different events could have on the organization.
    - Incident scenario identification: Determining the possible events that could have an impact on the organization and that will serve as a base to identify the risks.
- Risk analysis: Determining the risk level based on the impact of each incident scenario and their probability of occurrence.
- Risk evaluation: Producing a scored list of all the identified risks, based on the risk analysis results; the business criteria; the affected assets and their vulnerabilities and the potential threats.

Annex 4 – List of organisations taking part in the survey

ENISA gratefuly acknowledges the organisations that contributed to the study conducted in 2013. Mentioned are only these that expressed their consent to be acknowledged in the report.

Organization	**Country**
AC Camerfirma S.A.	Spain
AS Sertifitseerimiskeskus	Estonia
Banco de Espana	Spain
Borica - Bankservice AD	Bulgaria
British Telecom PLC	United Kingdom
Bundesnetzagentur	Germany
Commfides Norge AS	Norway
Consejo General de la Abogacia Espanola	Spain
DATEV eG	Germany
Direccion General de la Policia	Spain
DHIMYOTIS	France
Digidentity	Netherlands
DigiSign SA	Romania
DigitalSign - Certificadora Digital, SA	Portugal
Disig, a.s.	Slovakia
D-TRUST GmbH	Germany
EADTrust	Spain
e-commerce monitoring GmbH	Austria
EDICOM	Spain
ESG de electronische signatuur B.V.	Netherlands
Fabrica Nacional de Moneda y Timbre	Spain
Firmaprofesional	Spain
Halcom d.d.	Slovenia
Health and Social Care Information Centre	United Kingdom
I.CA	Czech Republic
InfoNotary Plc.	Bulgaria
Information Services Plc.	Bulgaria
Izenpe	Spain
Ministry of Finance and Public Administrations	Spain
Ministry of Defense	Spain

Ministry of Interior	Czech Republic
Multicert S.A.	Portugal
National Security Authority	Slovakia
OpenCA Labs	Italy
Population Register Centre	Finland
Post.Trust	Ireland
QuoVadis Trustlink B.V.	Netherlands
Science and Technology Facilities Council	United Kingdom
Spektar JSC	Bulgaria
Viafirma S.L.	Spain

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

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

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