enisa

THE EU CYBER SECURITY AGENCY

SECURITY FRAMEWORK Fhw TRUST SERVICE PROVIDERS

Technical guidelines on trust services

DECEMBER 2017

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop 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.

Contact

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

Acknowledgements

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

ISBN: 978-92-9204-188-5
doi: 10.2824/16328 Catalogue number: TP-06-16-339-EN-N

Table of Contents

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. In order to overcome both administrative and legal barriers on a cross-border level, the eIDAS Regulation was created. The main goals of this Regulation 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 Service Provider systems
- enforce obligation of notifications about security incidents at Trust Service Providers

Article 19, which is the main focus of this document, of the eIDAS Regulation, states that Trust Service 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 or on the personal data maintained therein.

In this context, the European Union Agency for Network and Information Security (ENISA) has decided to develop these Guidelines on Security Requirements Applicable to Trust Service Providers, with the purpose of discussing the minimal security levels to be maintained by qualified and non-qualified Trust Service Providers.

1. Introduction

1.1 Purpose of this document

The Regulation (EU) No 910/2014 (hereafter the eIDAS Regulation[1]) repeals the Directive 1999/93/EC[2] for electronic signatures by providing a new legal framework for "electronic identification and trust services for electronic transactions in the internal market".

Whereas the former Directive focused on electronic signatures only, the eIDAS Regulation extends the concept of trust services to other services as electronic seals and time stamps, registered mail and website authentication. Furthermore, the eIDAS Regulation brings along new security requirements regarding the Trust Service Providers as well as the trust services they provide with the introduction of qualified Trust Service Providers and qualified trust services. In response to the eIDAS Regulation, ENISA has decided to support Trust Service Providers in fulfilling these new requirements set out in the Regulation by presenting, through a risk-based approach, the guidance to meet the minimum level of security.

The eIDAS Regulation also covers cross-border authentication and associated Levels Of Assurance for the electronic identification and authentication of identities and mutual recognition of these identities across Member States. Cross-border authentication and associated requirements defined by the eIDAS Regulation, is not in scope of this document.

The purpose of this document is to provide qualified and non-qualified Trust Service Providers with technical guidelines for implementing security measures based on risk, both from a technical and organizational perspective. By doing this, Trust Service Providers will be able to ensure the security of provided trust services and mitigate the impact of incidents to maintain appropriate security level, as required by Article 19.

The verbs “shall”, “should” and “may” in this document should be used in accondance with ETSI guide[3].

1.2 Concept of Trust Service Providers and Trust Services

A Trust Service Provider is a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified Trust Service Provider, where a qualified Trust Service Provider provides one or more qualified trust services. ***The qualified status is granted per Trust Service*** *by the supervisory body.*The eIDAS Regulation defines a trust service as an electronic service normally provided for remuneration which consists of:

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

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
[2] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999L0093&from=en
[3] https://portal.etsi.org/Portals/0/TBpages/edithelp/Docs/AGuideToWritingWorldClassStandards.pdf

As with Directive 1999/93/EC for electronic signatures, multiple types of trust services has been defined in the eIDAS Regulation to indicate the level of trust that can be given to a certain type of trust services and what the associated requirements are that to be fulfilled to comply with trust levels.

For trust services from the eIDAS Regulation, the following service types have been created and defined:

Electronic Signature

- '*electronic signature*' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
- '*advanced electronic signature*' means an electronic signature which meets the requirements set out in Article 26;
- '*qualified electronic signature*' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;

Electronic Seal

- '*electronic seal*' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;
- '*advanced electronic seal*' means an electronic seal, which meets the requirements set out in Article 36;
- '*qualified electronic seal*' means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;

Electronic Time Stamp

- '*electronic time stamp*' means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;
- '*qualified electronic time stamp*' means an electronic time stamp which meets the requirements laid down in Article 42;

Electronic Registered Delivery Service

- '*electronic registered delivery service*' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;
- '*qualified electronic registered delivery service*' means an electronic registered delivery service which meets the requirements laid down in Article 44;

(Certificate for) Website Authentication

- '*certificate for website authentication*' means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;
- '*qualified certificate for website authentication*' means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Article 45;

Each of the defined trust services and trust service types, relies on electronic certificates for their implementation, being the creation, verification, validation or preservation activities provided by a Trust Service Provider.

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, a public key certificate binds an identity (i.e. a person, a service or a device) to a public/private key pair. This certificate can then be used, amongst others, to verify the identity or signature of the certificate holder. Another example is an attribute certificate which for instance can bind an identity to certain attributes, such as profession or access rights.

These electronic certificates are provided by a (qualified) certification service provider and where the services implemented can be broken down into the following component services, which is also described in EN 319 411 (relevant parts):

- Registration service: verifies the identity and, if applicable, any specific attributes of a subject. The results of the verification process 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. Risk Assessment

2.1 Risk Assessments on Trust Service Providers

As stated in paragraph 1 of Article 19 of the eIDAS Regulation, qualified and non-qualified Trust Service Providers are required to take appropriate technical and organisational measures to manage the risks posed to the security of the trust service(s) they provide. Moreover, having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk.

In order to support Trust Service Providers in fulfilling these requirements, the following section will present the general approach regarding the conduction of a risk assessment. This section will not describe in detail the different existing methods, but will provide some guidance on how to conduct a risk assessment on Trust Service Providers.

As defined in ISO/IEC 27005:2011[4], the risk assessment process can be divided into the following phases:

- **Risk Identification**: Identifying the different factors (i.e. 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 likelihood of occurrence.
- **Risk Evaluation**: Producing a scored list of all the identified risks, based on the risk analysis results, business criteria, affected assets, their vulnerabilities and potential threats.

There are several methodologies for risk assessment and each of those must be specific to the Trust Service Provider depending on the trust service(s) it provides.

It is important to note that the risk assessment activities presented in this guideline are primarily focussed on Trust Service Providers providing certification services and time-stamping services. However, this approach can be used as a reference to implement a risk assessment on other trust services defined under the eIDAS Regulation, such as validation services, preservation services and registered electronic delivery services.

[4] http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56742

2.2 Trust Service Provider Infrastructure

The first step in the risk assessment process is to determine the scope included in the risk assessment and its boundaries. For this purpose, the Trust Service Provider 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 non-exhaustive list of common entities and processes involved in the operations of a Trust Service Provider providing certification services have been produced as example. This list can be found below and should only be used as a generic reference.

2.2.1 The involved entities[5]

Certification Authority: The Certification Authority (CA) is the entity that issues electronic certificates (e.g. for electronic signature, seal or website authentication). Trust Service Providers issuing electronic certificates have one or several CAs. These CAs handle the whole certification lifecycle management process, with the exception of the registration process which is done by the Registration Authority. Commonly, CAs generate and maintain their own key pair which they use to sign the certificates they issue. CAs act as a trust anchor, meaning when a subject presents its certificate to a third party, it is the signature from a trusted CA in the subject certificate that ensures relying parties that the certificate is legitimate.

Registration Authority: The Registration Authority (RA) 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 RA can be part of the Trust Service Provider or it may be an external entity with some type of contract or agreement with the Trust Service Provider. For example, a small Trust Service Provider requiring physical presence of the subject may delegate this activity to an external RA 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 Trust Service Provider. A subject can be natural persons or legal entities[6]. Subjects request certificates from Trust Service Providers which they use for many different purposes, such as electronic signatures, electronic seals or website authentication. 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 and signature validity. Relying parties can be signature validation platforms, online services that use the digital certificates for authenticating users, browsers that validate website 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 CAs. The VA shall guarantee the non-repudiation of its responses by digitally signed them and

---

[5] Further definitions can be found in ISO/IEC 13335 - http://www.iso.org/iso/catalogue_detail.htm?csnumber=39066, ISO/IEC 24760 – http://www.iso.org/iso/catalogue_detail.htm?csnumber=57916, ISO/IEC Guide 73 – http://www.iso.org/iso/catalogue_detail?csnumber=44651, RFC 3647 – https://www.ietf.org/rfc/rfc3647.txt, ETSI TS 102 158 – http://www.etsi.org/deliver/etsi_ts/102100_102199/102158/01.01.01_60/ts_102158v010101p.pdf, ETSI TS 102 042 – http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.04.01_60/ts_102042v020401p.pdf, eIDAS Regulation

[6] While certificates for electronic signature must only be issued to natural persons, certificates for electronic seals must only be issued to legal persons.

specifying the date and status (i.e. valid, revoked, cancelled or unknown) of a certificate. These results can be published via either 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 at the moment the corresponding certificate was valid. 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.

2.2.2 The involved processes

This is a list of the main processes involved in the most commonly used operations of Trust Service Providers providing certification services. 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 procedures 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 procedures 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 procedures 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 the procedures in place to revoke certificates, from the revocation request to the publication.

The validation process: The validation process comprises all procedures from users or Trust Service Providers on *confirming the validity of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services.*. 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 Trust Service Provider infrastructure.

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

2.2.3 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 of the Trust Service Provider 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 a Trust Service Provider providing certification services, a critical asset could be anything of value to the CA or any relying party or "subject". An example could be a CA private key, since an incident involving the confidentiality or integrity of a CA private key could have very damaging consequences for the Trust Service Provider. 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 Trust Service Provider as very high. Following this approach, the Trust Service Provider shall conduct an evaluation of the value of all the identified assets in order to have a list of assets and their value which corresponds to its actual business and operational environment.

To support the asset identification process, some examples of common assets owned by Trust Service Providers providing certification services, are listed below and should only be used as a generic reference. The list has been organized following the guidelines provided in the ISO/IEC 27005:2011[7], which divides assets into two categories:

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

[7] http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56742

2.2.3.1 Primary assets

Information assets: Information assets include all data that are handled by the Trust Service Provider, either produced by it or handled by third parties. In this category the Trust Service Provider should include at least all the information related to the certificates (e.g. public and private keys, certificate content, etc.) as well as all the logs of the system. Examples of information assets in a Trust Service Provider 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 Trust Service Provider 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 Trust Service Provider may have depending on the additional trust services it is offering. Examples of business processes in a Trust Service Provider 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 also be vulnerable and affect the business processes.

2.2.3.2 Supporting assets

Software, hardware and networks: The Trust Service Provider shall include in the asset inventory all software applications, all hardware infrastructures and all network infrastructures that are used in the Trust Service Provider. Examples of software, hardware and networks assets are:

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

Locations and sites: The Trust Service Provider 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:

- Trust Service Provider primary premises
- Trust Service Provider back up sites
- RA offices

Personnel: The Trust Service Provider shall include in this category all different roles involved in the Trust Service Provider processes and the access rights to the different assets. Examples of personnel assets are:

- Trust Service Provider trusted roles for CA, VA and TSA
- Other operational roles
- RA operators
- Different administrators at level of OS, DB, etc.

Other assets: The Trust Service Provider should identify all other assets not included in the above categories that have a value for the organization. Examples of other assets are:

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

2.2.4 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 likelihood of occurrence. Likelihood 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 likelihood 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 Trust Service Provider whose facilities are located on seismic activity area should rate the likelihood 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 Trust Service Providers may face, which can be found below, and should only be used as a generic reference. The Trust Service Provider shall have a list of potential threats and their likelihood of occurrence which corresponds to its actual business and operational environment.

Natural hazards: The Trust Service Provider 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 Trust Service Provider operation are:

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

Essential services: The Trust Service Provider 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 Trust Service Provider 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 Trust Service Provider should determine, based on the type of services it is providing, the possible human made threats. For example, whether the Trust Service Provider is operating in public networks or internal networks will have an impact on the likelihood of materialization of certain human threats. Some examples of human made hazards that can be a threat to the Trust Service Provider 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

2.2.5 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, in the case of a Trust Service Provider providing certification services, the 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 (e.g. subject device, subject private key), which could be exploited by a threat (e.g. tampering of equipment or data) and lead to an incident (e.g. compromise of the subject private key). Therefore, in order to determine potential vulnerabilities, the Trust Service Provider assets and the existing threats shall be taken into account.

To support the vulnerability identification process, we have produced examples of potential vulnerabilities of Trust Service Providers providing certification services. The list is informative and should only be used as a generic reference. The Trust Service Provider risk analysis shall include a list of potential vulnerabilities which corresponds to its actual business and operational environment (i.e. its trust services).

2.2.5.1 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

2.2.5.2 Vulnerabilities in the Trust Service Provider key management process

The Trust Service Provider key management process refers to the key generation, backup and recovery, storage, usage, destruction, etc. processes of the entities involved in the Trust Service Provider, like the CA, the VA and the 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, like insufficient random seed material) 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 Trust Service Provider 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, etc.)
- 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. Example of vulnerabilities in the certificate dissemination process:

- 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
- Insecure processes or applications may lead to sending fake data/certificates to be signed

2.2.5.3 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 Trust Service Provider 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 Trust Service Provider needed assurance level may lead to liability of the Trust

Service Provider 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 Trust Service Provider 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 Trust Service Provider 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

2.2.5.4 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.

2.2.5.5 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: Trust Service Providers disseminate the revocation status of their issued certificates periodically. The update frequency of the list of revoked certificates should be reflected in the Trust Service Provider 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
- Failure to produce and publish CRLs

2.2.5.6 Vulnerabilities in the validation process

Validation management process: The validation management process deals with all procedures from users or Trust Service Providers on confirming the validity of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services. 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

2.2.5.7 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

2.2.5.8 Vulnerabilities in the Trust Service Provider information and communication systems

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

- Lack of appropriate measures to protect Trust Service Provider operation from malicious software
- Lack of disaster recovery and business continuity plans
- Lack of a logical perimeter security to protect Trust Service Provider 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

Trust Service Provider hardware components: For a Trust Service Provider, 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 Trust Service Provider 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

Trust Service Provider communication networks: Communication networks are critical in several aspects of the Trust Service Provider 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 Trust Service Provider could lead to the inability to issue certificates or to publish revocation status. Examples of vulnerabilities in the Trust Service Provider 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

Trust Service Provider systems audit logs: Lack of audit logging procedures on operations conducted over the Trust Service Provider 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

2.2.5.9 Vulnerabilities affecting the Trust Service Provider operation

Trust Service Provider policies: Trust Service Provider 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 Trust Service Provider 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)

Trust Service Provider operational procedures: Trust Service Provider 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 Trust Service Provider operations
- Lack of Incident Response Procedures
- Lack of Business Continuity and Contingency Plans
- Lack of quality assurance plans for issued certificates

Trust Service Provider personnel: Trust Service Provider personnel, especially those whose work in the Trust Service Provider 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

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

2.2.6 Identify necessary/required controls

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

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

This section presents a set of minimum security measures (it can be used ETSI EN 319 412 family of standards control specific for Trust Service Providers issuing electronic certificates or more generic, the ISO 27000[8] family of standards controls) that can be used as a reference for Trust Service Providers.

2.2.6.1 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

2.2.6.2 Security measures in the Trust Service Provider 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 (and 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 and 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

[8] http://www.iso.org/iso/iso27001

- 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

2.2.6.3 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 (and other parameters) deemed appropriate for the Trust Service Provider 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 and 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 Trust Service Provider ensures the authenticity of the hardware before delivery to the subject
- The security characteristics of the subject signature device are verified by the Trust Service Provider and deemed appropriate for the Trust Service Provider and subject business requirements
- If the subject device is activated by a PIN or pass phrase, they are distributed through secure channels

2.2.6.4 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 Trust Service Provider supervises that the certificate is delivered to the legitimate subject and that it is under his/her sole control
- The Trust Service Provider 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.

2.2.6.5 Security measures in the revocation management process

Certificate revocation management service

- The Trust Service Provider 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 Trust Service Provider 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 the modification of CRLs are logged

2.2.6.6 Security measures in the validation process

Certificate validation management service

- The Trust Service Provider 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 Trust Service Provider is able to validate any certificate that it has issued

2.2.6.7 Security measures in the time stamping process

Time stamping management service

- The Trust Service Provider 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

2.2.6.8 Security measures in the Trust Service Provider information and communication systems

Trust Service Provider software

- The Trust Service Provider 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 or physically separated from other Trust Service Provider applications
- Trust Service Provider software applications are separated from public networks by the appropriate perimeter security mechanisms to restrict the visibility among internal and external hosts
- The Trust Service Provider 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 Trust Service Provider information systems and their actions shall be logged
- The Trust Service Provider conducts periodical vulnerability assessments to detect potential security flaws in its information systems
- The Trust Service Provider 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 logs
  - The roles authorized to delete logs after their minimum retention time
  - The retention time for logs
- The Trust Service Provider 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, etc.
- 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, etc.
- Trust Service Provider software is kept up to date with security fixes

Trust Service Provider hardware

- Equipment is protected from environmental threats

- Equipment is protected from theft and tampering by implementing the appropriate physical security measures
- The Trust Service Provider 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, FIPS, etc.)
- Any information with might remain on hardware to be disposed is securely destroyed (e.g. wiping and shredding of hard disks)

Trust Service Provider communication networks

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

2.2.6.9 Security measures in the Trust Service Provider operation

Trust Service Provider policies

- The Trust Service Provider has produced and approved a Certificate Policy and a Certification Practice Statement
- The Trust Service Provider has verified that the Certificate Policy and the Certification Practice Statement match business requirements and objectives
- The Trust Service Provider has produced and approved an Information Security Policy and a Business Continuity Plan
- Policies are enforced

Trust Service Provider operational procedures

- The Trust Service Provider has produced and regularly tests and reviews business continuity plans to ensure continuity of operations after incidents
- The Trust Service Provider 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 Trust Service Provider has produced and maintains an incident response plan which clearly states responsibilities in incident management
- The Trust Service Provider keeps a record of incidents and reviews this information periodically to ensure the implementation of corrective measures

Trust Service Provider personnel

- The Trust Service Provider 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)
- Trust Service Provider personnel receive the appropriate training regarding security procedures
- The Trust Service Provider 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

Trust Service Provider facilities

- Trust Service Provider facilities are protected from unauthorized access
- Trust Service Provider 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 Trust Service Provider has produced and maintains contingence plans to respond to essential services failure (electricity, air conditioning)

2.2.7 Determine consequences

A consequence is defined as the "outcome of an event affecting objectives"[9]. 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 Trust Service Provider.

The following list identifies some of the consequences that different incidents may have on the Trust Service Provider operations when providing services for the issuance of electronic certificates.

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 Trust Service Provider 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.

[9] https://www.iso.org/obp/ui/#iso:std:iso:31000

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 Trust Service Provider.

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 Trust Service Provider 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.

2.2.8 Identify incident scenarios[10]

Having the input from identified assets, threats, vulnerabilities and consequences, the next step is to identify the list of risks, formulated in the form of 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 regarding a Trust Service Providers providing certification services are (some incident scenarios are repeated as they may affect more than one entity):

Incidents affecting CAs

- Compromise of a CA
- 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

[10] Further information regarding the mitigation of security incidents can be found in section 4 of this document.

- 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

2.3 Risk analysis

Once all the parameters that influence the risk calculation have been identified (i.e. assets, threats, vulnerabilities, existing controls, consequences, and incident scenarios) the Trust Service Provider has enough information to start the risk analysis process. According toISO 27005[11], risk analysis 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.

This analysis must also take into account special circumstances under which assets may require additional protection, such as with regulatory compliance. During this phase of the risk assessment, the Trust Service Provider will use all the identified sources to estimate the risk, in terms of impact and likelihood.

2.3.1 Assess the impact

An impact is defined as the result of an unwanted incident. It 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 Trust Service Provider needs to determine the possible consequences of each identified incident scenario and the impact it would have on the Trust Service Provider's 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

[11] http://www.iso27001security.com/html/27005.html

consequences. Based on the potential consequences, for each incident scenario the level of impact can be determined.

2.3.2 Assess the likelihood

In general, likelihood is defined as an estimation of the extent to which an event is likely to occur (ENISA[12]) and can be expressed discretely or on a continuous scale. To determine the likelihood 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 likelihood score.

2.3.3 Estimate the degree of risk

Risk estimation is defined as the process used to assign values to the likelihood and consequences of a risk. The degree 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.

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

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.

Impact: The result of an unwanted incident

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

The risk of compromising of a subject key pair and the claiming to repudiate the certificate subject shall be reduced by applying the correspondent countermeasures.

2.4 Evaluate risk

Risk evaluation is the process of comparing the estimated risk against given risk criteria to determine the significance of risk.

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 27005). Risk criteria are closely linked to the Trust Service Provider business environment and should be determined by the Trust Service Provider and specific to the trust service(s) it provides.

To support the risk evaluation process, we have produced examples of evaluations, based solely on the risk estimation, of the main risks Trust Service Providers face when providing trust services for the issuance of electronic certificates. This list is informative and should only be used as a reference. The Trust Service

[12] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

Provider 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 of the identified risks, 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 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.

The likelihood of the risks has not been evaluated, as this metric highly depends on the nature of potential incident.

Risk 1: Compromise of a Certification Authority

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

Related 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 Trust Service Provider 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

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 or Subject key is generated with a weak key generation algorithm or insufficient key length (or other parameters) for the Trust Service Provider business and legal requirements
- Attack vectors that make the cryptographic algorithms used to generate the CA key pair insecure are discovered
- 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
- Failure to fulfil legal requirements related to QSCDs
- Loss of accountability of actions
- Loss of reputation

Risk 3: Compromise of a Registration Authority

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

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

Impact **Medium**

Description: A personal data breach occurs when personal data provided to or produced by the Trust Service Provider are disclosed to unauthorized individuals. Personal data maintained by the Trust Service Provider 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 Trust Service Provider.

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

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

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 Trust Service Provider 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

Related 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
- Intentional or 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

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 Trust Service Provider cannot guarantee the security of the whole certificate management process. Repudiation can have liability consequences for the Trust Service Provider.

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 Trust Service Provider needed assurance level
- Subject key is generated with a weak algorithm or insufficient key length (or other parameters) for the Trust Service Provider 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

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 Trust Service Provider 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

Impact **Very high**

Description: A compromise of the Validation Authority (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 Trust Service Provider 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

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 Trust Service Provider 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

3. Mitigating Impact of Security Incidents

The previous section presented the general approach supporting Trust Service Providers in the implementation of the appropriate security measures through the conduction of a risk assessment, as required the eIDAS Regulation.

Furthermore, Article 19 of the eIDAS Regulation states that these security measures shall be taken to prevent and minimise the impact of security incidents as well as inform the stakeholders of the adverse effects of any such incidents.

This section will present some guidelines supporting Trust Service Providers in fulfilling these requirements by using the appropriate measures to efficiently prevent, detect, assess and respond to security incidents as well as mitigate their impact. The example taken in the following mainly regards Trust Service Providers providing trust services for the issuance of electronic certificates, but can be easily extended to other kinds of Trust Service Providers (e.g. providing creation, validation, verification or preservation services for electronic signatures or seals).

This section does not include guidelines regarding the reporting of incidents by Supervisory Bodies in case of breach of security or loss of integrity, as required by the eIDAS Regulation. For this matter, ENISA is creating a document which aims at supporting Supervisory Bodies responsible for the application and enforcement of the Article 19 of the eIDAS Regulation. This document describes a framework for security incident reporting which comply with requirements set out in paragraphs 2 and 3 of Article 19. [13]

3.1 Trust Service Provider entities, processes, and impact

3.1.1 Entities involved in trust services

Understanding the different entities involved in the trust service processes is important to be able to determine the different types of incidents that may take place in trust services. Each incident scenario can affect any entity or process involved in the provided trust service.

Section 3.2.1 of this document provides a non-exhaustive list of common entities involved in the operations of a Trust Service Provider providing certification services with their definition.

3.1.2 Processes involved in trust services

Understanding the processes that take place in providing trust services is important to determine which processes may be affected by an incident. Attackers will try to exploit vulnerabilities in any of the processes, and successful attacks on the different processes will have different consequences.

Section 3.2.2 of this document provides a non-exhaustive list of common processes involved in the operations of a Trust Service Provider providing certification services with their definition.

3.1.3 Impact of security incidents

It is important to understand the consequences of a security incident to comprehend why it is critical for Trust Service Providers to respond promptly and appropriately to it. Most operations in the Internet that require a high assurance of proof of identity rely nowadays on the use of electronic certificates.

[13] https://www.enisa.europa.eu/publications/technical-guideline-for-incident-reporting

3.1.3.1 Assuming the identity of another entity

Entities present digital certificates to relying parties in order to link their identity with the corresponding public key. Once verified, the relying party will accept the identity of the entity as correct. This process can be applied for any authentication purposes, for example, an entity accessing a system or a web page presenting itself to a user.

If a malicious entity manages to circumvent, break, or another unlawful operation on this process, e.g. by forging certificates, it is able to assume the subject's identity and act in its name.

3.1.3.2 Eavesdropping on private communications

On the Internet, sensitive communication between entities is often secured against eavesdropping and spoofing (e.g. websites by means of TLS). In these processes, electronic certificates play a major role in exchanging the respective keys. Once verified, the relying party will deem the communication confidential.

If a malicious entity managed to interfere with this (e.g. by mounting a man in the middle attack using fake certificates) it would be able to eavesdrop on the communication.

3.1.3.3 Forging electronic signatures

Where the legal framework allows it (through appropriate legal acts, which is the case in most major jurisdictions), electronic signatures can be used for the same purpose as handwritten signatures; they can be used to make legal commitments, like signing a contract or submitting a tax declaration, etc. Certificates play a major role in the verification of signatures, establishing authenticity and non-repudiation.

Being able to forge an electronic signature (e.g. by gaining unauthorized access to the signature key) enables the attacker to sign arbitrary documents in the victim's name.

3.1.3.4 Unavailability of services

A Trust Service Provider provides services to other parties. These other parties rely on the Trust Service Provider for services such as key generation, certificate issuance, and revocation checking.

Being able to delay or even entirely stop the Trust Service Providers services (e.g. the OCSP server[14]), enables the attacker to interfere with the day-to-day operations of the parties relying on them.

3.1.3.5 Reputation damage

The business of a Trust Service Provider stands and falls with its reputation. As having a good reputation is a necessary condition for being trusted and chosen by clients, having a bad reputation is sufficient to not being trusted.

If an attacker manages to cause serious security incidents, not only the security is at stake but also the Trust Service Providers reputation and thereby its entire business.

3.2 Identifying incident scenarios and attack vectors

After identifying the entities, processes and possible impacts on Trust Service Providers, it is important to develop an understanding of possible incident scenarios and attack vectors to understand the possible situations the Trust Service Provider might face.

[14] Online Certificate Status Protocol, described in RFC 6960, https://tools.ietf.org/html/rfc6960

3.2.1 Incident scenarios

Incident scenarios define possible types of events that could affect an organization and cause negative consequences. The importance of identifying incident scenarios is that it helps the organization to make a classification of incidents when they occur, and to have a protocol for response based on the characteristics and possible consequences of the incident.

Section 3.4 of this document provides a group of incident scenarios identified by ENISA which classifies the identified type of events that could affect a Trust Service Provider. In the following paragraphs, a description of the identified incident scenarios is provided.

Although all descriptions given in the following focus on technical issues, similar incidents can be provoked by organizational means, such as social engineering or coercion. In addition, most of the incidents can also be provoked by accident or human error.

3.2.1.1 Compromise of a CA

Relying parties use the electronic signature of the CA in certificates as an attestation of the legitimacy of the certificate. If attackers control the CA private keys, they can generate fake certificates which relying parties will accept as valid because they are signed by the CA. To achieve this, the attacker would need either access to the CA private signing key, or access to the certificate signing applications of the CA which activate the key (avoidable in case where principles of segregation of duties and dual control are put in place).

3.2.1.2 Compromise of a Registration Authority

The role of the RA is to verify the subject identity and to subsequently send a certificate issuance request to the CA. Although the RA does not generate the certificates itself, compromises to its systems or keys could lead equally to fraudulent certificate issuance. The main objective of an attacker compromising a RA is the generation of fraudulent certificate requests that are accepted by the CA as legitimate. To compromise the RA, an attacker may obtain access to the RA key and manage to send fraudulent requests to the CA, or succeed to intrude its certificate request generation systems or intrude and tamper with the communication channel between the RA and the CA.

3.2.1.3 Compromise of the revocation services

It is important that the information regarding the status of certificates is correct, complete and available 24x7 so that no revoked certificates are accepted as valid. The goal of a revocation service compromise may be to modify the revocation services so that revoked certificates appear as valid, to erase a revocation request so that a compromised certificate is not revoked, to disrupt legitimate user operations by invalidating revocation status information, or to fraudulently revoke valid certificates.

3.2.1.4 Compromise of the cryptographic modules

A compromise of cryptographic modules occurs when the cryptographic algorithms, parameters, protocols, or implementations (i.e. software or hardware) become insecure. If, for example, the algorithm used to generate the CA or subject key pairs become insecure, an attacker could deduce or replicate the private key. Another possibility is that the actual signature or encryption algorithm is weak, enabling an attacker to generate fake signatures or decrypt messages without having access to the private key. Note that bad parameters or implementations can very well lead to weaknesses despite the fact that the algorithm or protocol being used is secure.

3.2.1.5 Repudiation claim by certificate subject

A repudiation claim occurs when a subject denies having performed the actions that are attributed to him/her by the certificate usage. A repudiation claim may be legitimate when it is the consequence of another type of breach, such as compromised subject keys, or may be fraudulent when the subject simply wants to deny actions actually performed by him/her by questioning the security of the Trust Service Provider.

3.2.1.6 Impersonation

An impersonation occurs when a malicious entity assumes the identity of another entity with the objective to commit a malicious act. In our case, this means an attacker assumes the identity of a subject (e.g. in order to gain access rights to confidential information, or fraudulently act otherwise in the victim's name).

3.2.1.7 Personal data breach

A personal data breach occurs when personal data provided to or produced by the Trust Service Provider are disclosed to unauthorized entities. Personal data maintained by the Trust Service Provider include information contained in the certificates (which is available to everyone), the registration records and the audit logs, aside from staff or business relation data. A personal data breach can imply legal and economic sanctions from supervisory authorities, and can seriously damage the reputation of the Trust Service Provider.

3.2.1.8 Compromise of a subject's private key

Subjects use their private keys to sign documents, authenticate to systems or decrypt messages or communications. Subject's private keys should be under their sole custody, or, when foreseen by the certificate policy, under the Trust Service Provider custody, always following strong security procedures to protect the confidentiality and integrity of the key. A compromise of a subject private key occurs when the subject (or the Trust Service Provider on its behalf) loses exclusive custody of its private key, effectively allowing an attacker to supplant its identity or access confidential information.

3.2.1.9 Loss of availability of services

An incident affecting the availability of the CA or RA systems can have negative effects for the reputation of the Trust Service Provider. If there is temporary unavailability of requesting a new certificate or renewing one this incident might not seriously affect the trust in the CA. But if the revocation management systems are unavailable, this is a serious issue, as proper certificate usage is impeded.

3.2.2 Attack vectors

An attack vector is a path or means by which an attack can be or is made[15]. Attack vectors help to identify which are the possible points of entry an attacker may use when trying to penetrate a system. Based on the characteristics of Trust Service Providers, we use four attack vectors that can be used to compromise a Trust Service Provider operation. In the following paragraphs, a description of these attack vectors is provided. Although all descriptions given here focus on technical issues, it is possible to open the same attack vectors by organizational means, such as social engineering or coercion. In addition, most of the attack vectors can also be opened by accident or human error.

3.2.2.1 Logical attacks

Logical attacks consist of attempts to infiltrate the CA or RA systems in order to manipulate them with the goal of obtaining access to private keys, producing fraudulent certificates or tampering with revocation

[15] http://web.mit.edu/mitei/research/studies/documents/electric-grid-2011/Electric_Grid_Full_Report.pdf

information. Trust services rely to a high extent on cryptography, however the set of information systems build upon the cryptographic modules are also an important component of the trust service.

CA and RA information systems may be subject to attacks that can result in fraudulent certificate issuance without actual access to any private key. For example, intrusion in a RA system can lead to fraudulent certificate request. Note that it is also possible to attack the subject's system to gain access to fraudulent certificates or provoke or prevent revocations.

To protect themselves from logical attacks, Trust Service Providers should implement perimeter security measures and all kind of security tools on their networks. The Trust Service Provider should also apply secure personal security environments (PSE), such as smart cards, as end user devices and promote the usage of secure connectivity equipment, such as certified card readers with PIN pad and display, and stress the importance of secured and up-to-date end user equipment, such as antivirus software and correct patch level.

3.2.2.2 Cryptographic attacks

Cryptographic attacks have an important impact on trust services, as the core technological component sustaining trust services is public key cryptography. The security of public key infrastructures depends, amongst others, heavily on the strength of the cryptographic algorithms, parameters, protocols, and implementations (i.e. software or hardware) they use. Cryptographers study permanently the existing cryptographic modules to determine whether they are vulnerable to the different existing types of attacks.

Attackers will try to compromise the security of cryptographic modules using vulnerabilities in order to compromise the security of the system.

To protect themselves from cryptographic attacks, Trust Service Providers should update their cryptographic parameters (e.g. key length), implementations (e.g. HSMs), protocols (e.g. key exchange), and even algorithms (e.g. hash algorithm) whenever indicated.

3.2.2.3 Insider attacks

Trust services are operated by people, and the security of the process relies to a certain extent on them. Insider attacks are those conducted by the Trust Service Provider personnel. This type of attack is usually hard to detect.

Trust Service Providers should implement measures such as logging and auditing and double control for the critical operations to avoid relying on any single person.

3.2.2.4 Physical attacks

Trust services are conducted at some physical location, where the actual hardware, software and key material are installed.

Trust Service Providers may be subject to attacks that try to compromise their physical security in order to gain access to applications or key material or to interfere with Trust Service Provider processes.

Trust Service Providers should implement strict physical security controls, especially in all areas where keys are stored or activated, making this type of attack difficult to implement. Additionally, private Trust Service Provider keys should be stored in tamper resistant hardware media (originals and possible backups) and shouldn't be extracted from this media at any point, except for redundancy, backup, or recovery purposes.

3.3 Preparing for incidents

One of the most important phases for responding to an incident in any kind of ICT service is to prepare beforehand all the procedures and necessary information to be able to respond quickly and effectively if an incident takes place. Appropriate policy is an instrument to prepare and to provide notice to service users and supervisory authorities. This section provides recommendations on what kind of aspects a Trust Service Provider should prepare.

3.3.1 Enable means to gather alerts

3.3.1.1 Enable outside parties to report incidents

Incidents in Trust Service Providers may in many cases be detected by certificate holders, relying parties or any other outside party. They should be able to easily report suspicious activity associated to certificates issued by the Trust Service Provider. The Trust Service Provider should establish a support line or helpdesk where any information regarding suspicious activity can be received.

3.3.1.2 Enable systems for staff to report abnormal events

Not all incidents will arrive from outside the Trust Service Provider, for example suspicious log activity will be detected by the Trust Service Provider personnel. The Trust Service Provider should provide means for them to register any incidence in a standardized format so that incident management personnel can response more effectively.

3.3.1.3 Follow alert systems from external sources

Suspicions of compromises of trust services or cryptographic algorithms, parameters, protocols, and implementations may be published (e.g. in Internet) even before the Trust Service Provider is aware. The Trust Service Provider should follow security alert systems and forums and be aware of the latest threats.

3.3.1.4 Activate alerts in internal systems

The Trust Service Provider should establish an adequate level of logging in all information systems, revise logs periodically, and enable systems that alert personnel when suspicious activities appear in systems logs.

3.3.1.5 Conduct continuous self-monitoring and self-testing

The Trust Service Provider should foster a culture of self-monitoring and self-testing. This includes actively trying to break the own systems by all available means such as penetration and vulnerability testing. Whenever indicated, an alarm should be raised through the established channels.

3.3.2 Create an incident response capability[16]

3.3.2.1 Create an incident response team

Trust Service Providers should have an incident response team. Different configurations and capabilities of an incident response team exist, the Trust Service Provider should define it according to its characteristics and their risk assessment. Amongst the questions to answer are:

- Whether a 24x7 incident response capability is needed (which seems appropriate for at revocation services at least).
- The size of the team, whether they will part-time or full time, and the needed skills of the personnel.

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

- Whether central incident management response or distributed incident response is applied.

3.3.2.2 Create incident response procedures

After determining different incident types that may occur, the Trust Service Provider should define procedures for incident management. Having ready procedures will improve and speed up response when dealing with an incident. This should also include realistic response drills.

3.3.3 Prepare staff and systems for an incident

3.3.3.1 Assign roles and responsibilities

Have an updated list of roles and responsibilities of staff in case of an incident. This applies not just to those directly involved in managing the incident, but for all personnel operating CA functions. All personnel should have clear instructions on how to proceed in case of an incident affecting their functions.

3.3.3.2 Train personnel

Conduct incident response exercises periodically in order for the involved staff to be able to handle incidents properly.

3.3.3.3 Put redundancy or fail-safe mechanisms in place

Have (cold or hot) standby systems in place to take over the duties of the main system in case of an incident. Consider applying fail-safe cryptographic modules, mechanisms such as forward secure signatures and/or utilizing fundamentally different crypto modules in parallel.

3.3.4 Have means of communication with all stakeholders

3.3.4.1 Create a repository of certificate holders contact information

The Trust Service Provider should establish, if appropriate according to local legislation and field of use, a database of issued certificates with the contact information of all the certificate holders and keep it updated. This will speed up the process of contacting them in case an incident takes place with their certificate.

3.3.4.2 Create a repository of relying parties

The Trust Service Provider should establish a database with contact information regarding (known) relying parties (or their representatives) that use their certificates, such as government sites or trust stores for web browsers, in order to facilitate the process of contacting them if an incident takes place.

3.3.5 Create a repository of supervisors and competent authorities

The Trust Service Provider should establish a database with contact information regarding supervisors and competent authorities. As required by the eIDAS Regulation, qualified and non-qualified Trust Service Providers have to inform the supervisory authorities of any security incident affecting the service without undue delay. Additionally, the Trust Service Providers need to inform data protection authorities and under certain conditions data subjects when personal data are breached. It is also recommendable to have contacts with competent CERTs. Knowing the appropriate channels for communication will facilitate the process if an incident occurs.

3.3.6 Have contingency plans

The typical approach is to have backup sites (hot and/or cold) as well as business continuity plans, but also the following.

3.3.6.1 Have agreements with other Trust Service Providers to obtain substitute certificates

In the very critical situation where certificates need to be replaced, and none of the Trust Service Providers CAs, RAs or revocation services can be trusted or are unavailable, the Trust Service Provider should be able to provide subjects with services from other Trust Service Providers until the operations can be resumed with their own systems. This will minimize the impact on subjects.

3.3.6.2 Maintain updated information of your environment

The Trust Service Provider should have documented information regarding all data that can be helpful in case of an incident, such as:

- lists of assets
- network diagrams
- applications and software versions
- disaster procedures
- recover and restore procedures
- contingency plans

3.3.6.3 Have a service termination plan

In case the Trust Service Provider decides for any reason or is forced to discontinue operations, there should be a plan in place to ensure that the services go down smoothly (e.g. make sure that issued certificates can be still verified or revoked from external sources). In some countries the succession of service in case of termination is obligatory for accredited CAs.

3.4 Detecting and assessing the incident

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

From the moment an event is classified as an incident, all evidence should be preserved in case it will be needed at a further stage[17]. Furthermore, as stated in Article 19 paragraph 2 of the eIDAS Regulation, Trust Service Providers are required to notify the responsible Supervisory Body within 24 hours after having become aware of any data breach of security or loss of integrity that has a significant impact on the Trust Service Provider or on the personal data maintained therin.

The following will help Trust Service Providers fulfil the requirements set out in Article 19 of the eIDAS Regulation by providing some guidelines in order to efficiently detect and assess incidents that may take place at a Trust Service Provider when providing trust services for the issuance of electronic certificates.

3.4.1 Fraudulent certificate activities

An indicator that some kind of certificate compromise might be taking place is reported; for example:

[17] https://www.enisa.europa.eu/topics/csirt-cert-services

- Certificates associated with man in the middle attacks
- Certificates associated to known malware sites
- Malware signed with certificates
- Subjects reporting that certificates associated with their name do not belong to them
- Subjects that report usage of their certificates that they didn't do themselves.
- Attempts to use invalid or revoked certificates
- Fraudulent certificate activity may indicate different types of compromises. In order to determine what part of the trust service is compromised, at least the following steps should be followed:
- Analyse the potential fraudulent activity to determine the certificates' origin and verify that they are linked to a CA of the Trust Service Provider
- Contact the certificate subjects' to assess whether fraudulent activities are taking place
- Assess the circumstances under which the certificate was issued:
    - Contact the RA to check registration logs and records
    - Check certificate request and generation logs at CA

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

3.4.2 Abnormal activities in information systems

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

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

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

3.4.3 Suspicious information in the certificate lifecycle management logs

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

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

- Inconsistencies in the registration, certificate generation or revocation logs
- Inconsistencies in the information associated to any certificate
- Registration requests lacking associated registration records

- Certificate generation or revocation lacking any request
- Unusual behaviour (e.g. physical registration outside business hours)
- Inconsistencies in revocation service logs (e.g. OCSP queries for not issued certificates)

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

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

3.4.4 Unaccounted key media

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

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

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

3.4.5 Loss of availability

Loss of availability of the Trust Service Provider systems can be the consequence of an intrusion attempt or be due to accidental events. In any case it should be treated as an incident and its source should be investigated. In the event of a loss of availability, the Trust Service Provider should immediately restore the availability of critical systems, such as revocation services, e.g. by switching to standby systems. The Trust Service Provider should also assess whether there any accidental causes that could explain a disruption, such as loss of essential services, natural hazards, etc. but also investigate other potential causes.

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

3.4.6 Loss of custody of subject key

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

3.5 Responding to the incident

An effective and prompt response is critical for mitigating the impact of a breach in a Trust Service Provider issuing electronic certificates.

3.5.1 Types of breaches

Incidents at Trust Service Providers can be divided into two general types, and this classification plays an important role in selecting the appropriate response.

3.5.1.1 Breaches that compromise the integrity of the trust service

These incidents, or compromises, imply access to private keys, ability to infiltrate systems that activate these keys or any kind of illegitimate access to any process involved in the certificate generation. Such incidents can have as a consequence the fraudulent generation, use, or revocation of certificates, and therefore require immediate revocation of all fake certificates generated or appropriate handling of fake revocations. In some cases, even the revocation of all certificates issued by a certain CA, including the root certificate may be indicated. Among these incidents are:

- Compromise of a CA
- Compromise of a Registration Authority
- Compromise of the revocation services
- Compromise of the cryptographic modules
- Impersonation of a valid subject
- Loss of availability of revocation services

In incidents that compromise the integrity of the trust service, the priority in response is always to limit the damage, even if this has as a consequence the temporal unavailability of the service for legitimate users.

3.5.1.2 Breaches that don't compromise the integrity of the trust service

These types of incidents do not require revocation of certificates; therefore the response protocol is different. In any case, they may have very negative consequences for the Trust Service Provider. Among these incidents are:

- Personal data breach
- Loss of availability of the trust services other than revocation
- Repudiation claim
- Inability to validate the certificate

With incidents that do not compromise the integrity of the trust service, the priority in response depends on the type of incident: personal data breaches (i.e. to protect the confidentiality of the data), loss of availability (i.e. to recover the service) and repudiation claim (i.e. to ensure traceability and accountability of actions).

3.5.2 Response guidance

The following sections provide guidance to support the Trust Service Provider in responding to different incident scenarios.

3.5.2.1 Responding to a CA compromise

When a CA compromise is detected[18], it is critical for the Trust Service Provider to take prompt and appropriate measures to mitigate the impact of the breach. The goal is to prevent any further usage of fraudulent certificates. At least, the following actions should be undertaken:

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

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

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

3.5.2.2 Responding to a RA compromise

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

If all fraudulent certificates can be detected, revoking those certificates can be sufficient. But when not all fraudulent certificates can be detected with certainty, it is recommended for the CA to revoke all certificates based on registration data from the compromised RA, because there is no guarantee as to whether fake certificates are being used. At least, the following actions are recommended:

If all fraudulent certificates can be identified:

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

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

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

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

3.5.2.3 Responding to a compromise of the revocation services

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

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

3.5.2.4 Responding to a compromise of the cryptographic modules

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

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

Note that here are proactive measures which prevent Trust Service Providers from being compromised even if (a single) cryptographic module becomes insecure (e.g. forward secure cryptography or utilizing fundamentally different crypto modules in parallel). In this case, the immediate revocation is not necessary.

3.5.2.5 Responding to a repudiation claim by a certificate subject

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

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

3.5.2.6 Responding to impersonation

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

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

3.5.2.7 Responding to a personal data breach

The objective in the response to a personal data breach is to minimize the disclosure of personal information. However, depending on the nature of the breach, this will not always be possible for the Trust Service Provider. At least, the following actions are recommended:

- Determine if the incident is on-going and take contention measures. For example, in the case of a hacked system, disable the system until the vulnerabilities facilitating the incident have been found and corrective actions taken
- Notify competent authorities about the breach
- Inform affected entities regarding which personal information has been compromised and what is the extent of the disclosure

3.5.2.8 Responding to a compromise of a subject's key pair

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

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

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

- Determine the common cause
- Determine all affected subjects

3.5.2.9 Responding to a loss of availability of services

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

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

3.6 Eradicating and resolving the incident

Once the source of the compromise has been determined and the appropriate response actions to mitigate the impact of the incident have been taken, the Trust Service Provider should take the appropriate measures to minimize the possibility of the incident occurring again. The following present measures that a Trust Service Provider should take in order to eradicate an incident.

3.6.1 Determine what facilitated the incident

Assess whether the incident was the consequence of vulnerabilities in any of the systems or processes of the Trust Service Provider. Most incidents can be traced to some vulnerability. If the incident was due to a malicious insider, an associated vulnerability can be the lack of dual controls or mandatory rotation. In the case of a cryptographic attack, it might possible that the chosen algorithms, protocols, parameters or implementations do not match the level of assurance needed for the Trust Service Provider. In any case, it is of critical importance to trace what facilitated the incident in order to be able to eradicate it.

3.6.2 Analyse the existing security policies and procedures

Review the existing policies and procedures (including policy enforcement), especially those related to systems and processes related to the incident, to determine if they are sufficient for the expected level of security. Especially important is to assess those policies and procedures related to the exiting vulnerabilities.

3.6.3 Re-conduct a risk assessment

Re-conduct a risk assessment to determine if the existing security controls match the level of risk accepted by the organization. Based on the analysis results determine if security measures are to be incremented. Note that this should take place regularly anyway, even if no incident occurred.

3.6.4 Define and implement corrective measures

If the risk assessment results determine that any security levels need to be incremented, the last step in the eradication process is to define and implement the security measures needed.

A parallel activity important during the eradication phase is to document all the actions taken during the incident. All this information should be used as input to improve the incident management procedures.

Conclusions

As part of the eIDAS Regulation qualified and non-qualified Trust Service Providers are required to comply with the requirements set out in Article 19. Section 2 presented the context of the Regulation and described how Trust Service Providers can adapt in order to comply with the requirements. It also provided a set of guidelines and standards on how to comply with the different aspects of the Regulation and guidance to provide qualified services. It should however be noted that at the time of writing, many standards have yet to be written but should become available in the near future.

Some of the new requirements for Trust Service Providers, both qualified and non-qualified, concern the conduction of risk assessment and the mitigation of security incidents. Section 3 discussed the principles and concepts of managing the risks applicable to all Trust Service Providers by defining the controls to manage threats and vulnerabilities. Section 4 introduced the general process of incident mitigation and how this should be handled by Trust Service Providers. The methodology presented in both section 3 and 4 to be chosen by the Trust Service Providers, this document provided a general overview of how a risk assessment can be conducted, in order to identify, analyze and evaluate the risks specific to Trust Service Providers as well as recommendations regarding the approach for incident mitigation.

Definitions

For the purpose of this report, definitions of the Art.3 of the eIDAS Regulation apply. In particular, in this text the following definitions are used:

advanced electronic signature – an electronic signature which meets the requirements set out in Article 26 of the eIDAS Regulation;

authentication – an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;

certificate for electronic signature – an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;

certificate for website authentication – an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;

conformity assessment body – a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides;

eIDAS – is the Regulation being covered in this document. It has come into effect starting the 1st of July 2016. It reappeals Directive 1999/93/EC;

electronic document – any content stored in electronic form, in particular text or sound, visual or audiovisual recording;

electronic identification – the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;

electronic identification means – a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;

electronic identification scheme – a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;

electronic signature – data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

electronic signature creation data – unique data which is used by the signatory to create an electronic signature;

electronic signature creation device – configured software or hardware used to create an electronic signature;

electronic time stamp – data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;

qualified certificate for electronic signature – a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of the eIDAS Regulation;

qualified certificate for website authentication – a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;

qualified electronic signature – an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;

qualified electronic signature creation device – an electronic signature creation device that meets the requirements laid down in Annex II of the eIDAS Regulation;

qualified electronic time stamp – an electronic time stamp which meets the requirements laid down in Article 42 of the eIDAS Regulation;

qualified trust service – a trust service that meets the applicable requirements laid down in eIDAS Regulation;

qualified trust service provider – a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;

person identification data – a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;

product – hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services;

public sector body – a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;

relying party – a natural or legal person that relies upon an electronic identification or a trust service;

signatory – a natural person who creates an electronic signature;

trust service – an electronic service normally provided for remuneration which consists of:

- the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
- the creation, verification and validation of certificates for website authentication; or
- the preservation of electronic signatures, seals or certificates related to those services;

trust service provider – a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;

validation data – data that is used to validate an electronic signature or an electronic seal;

validation – the process of verifying and confirming that an electronic signature or a seal is valid.

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 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Catalogue Number TP-06-16-339-EN-N

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

ISBN: 978-92-9204-188-5
DOI: 10.2824/16328