Mitigating the impact of security incidents

Guidelines for trust services providers – Part 3

Version 1.0 – December 2013

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

About ENISA

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

Authors

Iñigo Barreira, Izenpe

Tomas Gustavsson, Primekey

Alexander Wiesmaier, AGT International

Clara Galan, Ministry of Defense, Spain [1]

Sławomir Górniak, ENISA

Contact

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

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

Acknowledgements

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

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

Legal notice

Copyright Notice

Executive summary

E-Government services have significant potential to make public services more efficient for the benefit of citizens and businesses in terms of time and money. And while these benefits are increasingly being felt nationally, e-Government services still face administrative and legal barriers on a cross-border level, although pan-European projects like STORK[2] have shown that technical issues of interoperability of electronic identifications can be overcome. In order to remove existing barriers for cross-border e-ID based services the European Commission has proposed in June 2012 a draft regulation on electronic identification and trust services for electronic transactions in the internal market [38], which will replace the existing Electronic Signature Directive 1999/93/EC [37]. The main goals of this action are to:

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

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

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

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

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

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

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

This document, Part 3: Mitigating security incidents, recommends measures to mitigate the impact of security incidents on trust service providers (TSP) by proposing suitable technical and organisational means to handle the security risks posed to the TSP. This is done using a certification service provider (CSP) as representative example. The document focuses on the concepts and entities of hierarchical public key infrastructures (PKI), leaving other concepts, such as web of trust, out of scope.

Understanding which entities and processes are involved in trust services and which possible impacts derive from security incidents is the first step of a proper risk management approach. The

[2] https://www.eid-stork.eu/

most important entities involved in trust services include: the certificate authority (CA), the registration authority (RA), the subject, the relying party, and others such as the time stamping authority (TSA) and the validation authority (VA). The major processes involved in trust services include: registration, certification, CA key management, subject key & certificate management, revocation and other processes such as validation or time-stamping. The main impacts of a TSP security incident include: Identity theft, eavesdropping, signature forgery, service unavailability, and repudiation damage.

In order to understand the possible security related situations the TSP might face it is important to develop an understanding of possible incident scenarios and attack vectors. The major incident scenarios include: the compromise of major TSP building blocks such as the CA, the RA, the revocation services, or the cryptographic modules, a repudiation claim, an impersonation, a personal data breach, the compromise of a subject key, and the loss of service availability. The ENISA survey[3] reveals that TSP providers see a CA compromise as the scenario with the biggest impact (8.7 of 10), while the compromise of a subject's key pair is seen as the scenario with the lowest impact (4.3 of 10) on the TSP. The same report also reveals that a compromise of the CA is deemed by the TSPs the least probable scenario, while the compromise of a subject's key pair is seen as the most probable scenario. The major attack vectors include: logical attacks, cryptographic attacks, insider attacks, and physical attacks. Following said surrey, most TSPs consider logical attacks the most likely (56% say highly likely or likely) while physical attacks are considered the most unlikely (89% say unlikely or very unlikely).

Preparing for possible incidents is one of the most important steps in impact mitigation as it allows the TSP to be able to respond quickly and effectively in case of an incident. Amongst the most important procedures and information gathering capabilities are: alert gathering capability, incident response capability, having staff and systems incident ready, established means of communication with stakeholders, and ready to go contingency plans.

In order to be able to actually react (in an appropriate way) to an incident, the TSP must be able to detect and assess incidents. Amongst the most important indicators for a security incident are: fraudulent certificate activities, abnormal activities in information systems, suspicious information in the certificate lifecycle management logs, unaccounted key media, loss of availability, and loss of custody of subject key.

Once an incident is detected, an effective and prompt response is critical for mitigating the impact of a breach in a TSP. In order to select an appropriate response, breaches are classified into the following two general types: breaches that compromise the integrity of the trust service and breaches that don't compromise the integrity of the trust service (availability is not taken into account in this classification). Depending on the type of breach, the focus of handling the incident differs. In the former case, 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. In the latter case, the priority in response depends on the type of incident: with personal data breaches, to protect the confidentiality of the data; with loss of availability, to recover the service; with repudiation claim, to ensure traceability and accountability of actions.

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

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

include: determine what facilitated the incident, analyse the existing security policies and procedures, conduct a risk assessment, and define and implement corrective measures.

Learning from past incidents (own and at other TSPs) is crucial in IT security in general. Many TSP have already been affected by an incident during the course of their operations. Lessons can already be learned from a variety of real world incidents[4].

[4] Description and analysis can be found in Section 8.

Table of Contents

1 Introduction

This document provides recommendations on means of mitigating the impact of security incidents consisting of appropriate technical and organisational measures to manage the risks affecting the security of trust service provides (TSP). We use certificate service providers (CSP) as a representative case for all types of TSP. The document is geared to what is called hierarchical public key infrastructures (PKI) and the respective concepts and entities. Other concepts, such as web of trust, are out of scope of this document and are not considered.

The document starts with a high level introduction to TSPs, including involved entities, processes and impact analysis of security incidents. After that, the document covers the topics of identifying, preparing, detecting, responding, and eradicating incidents in more detail. The document closes with lessons learned from past real world incidents.

The general rule of security being a constant process of iteration, learning, and improvement also applies to the measures presented in this document.

The National Institute of Technology and Standards (NIST) is currently preparing a cybersecurity framework for critical infrastructures [35]. This framework is to a major extent applicable to manage cybersecurity-related risk to TSPs, and is recommended as complimentary reference to standards, guidelines, and best practices in the field.

2 Trust service provider entities, processes, and impact

2.1 Entities involved in trust services

Traditionally, the technology used by TSPs is public key encryption. 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 affects an entity or process in the trust service. Amongst the entities involved in trust services are:

2.1.1 Certificate Authority

Certificate Authorities (CAs) are the actual issuers of electronic certificates. TSPs providing electronic certificates have one or several CAs managing the whole certificate lifecycle, with the exception of the registration process which is done by the Registration Authority (see below). Root CAs usually generate and maintain their own key pair which they use to sign the certificates they issue (and usually provide certificates for other CAs). CAs act as a trust anchor: when an entity presents its certificate to a relying party (see below), it is the signature by a trusted CA in the certificate that provides assurance to the relying party that the certificate is legitimate and valid.

2.1.2 Registration Authority

The Registration Authority (RA) is the entity that verifies the certificate requester's identity to ensure that the certificate is issued to the legitimate subject. One RA may be connected with several CAs and one CA may be connected with several RAs. Once the identity is verified, the RA sends a certificate request to the CA, which will then produce an electronic certificate and deliver it to the subject. The RA can be part of the TSP or it may be an external entity with some type of contract or agreement with the TSP. As an example could serve a small TSP requiring physical presence of the subject for identification purposes. This TSP may delegate the registration activity to an existing external authority, as deploying physical offices may not be feasible for the TSP itself.

2.1.3 Subject

The subject is the entity whose identity is bound to some other data contained in the certificate issued by the TSP, e.g. the certificate binds this entity's identity to its public key. Subjects can be natural persons (e.g. electronic signature certificates) or legal entities (e.g. electronic seals or web authentication certificates). Subjects (or representatives) request from TSPs certificates which they use for many different purposes, such as electronic signatures, authentication or encryption. Subjects are bound to a certificate by the signature of the CA, which vows for their identity.

2.1.4 Relying party

The relying party is an entity that relies on the services and tokens (e.g. certificates) issued by the TSP. Relying parties can be persons, services, devices, or any other entity. Examples are email users, signature validation platforms, online services, browsers, etc.

2.1.5 Other entities

There are more possible entities involved in trust services. Examples include additional TSP authorities providing core services such as revocation services or validation services. Other examples are entities providing additional services such as time stamping services, authentication services, signature services, or long-term archiving. Although these and other entities are not in the focus of the document, the recommendations apply to them analogously.

2.2 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. Amongst the modules in a trust service are:

2.2.1 Registration process

The registration process comprises all procedures which are in place to register a subject with a TSP, such as:

- Subject applies at TSP
- Subject presents a proof of identity and maybe its eligibility (this step may be missing)
- TSP registers subject or refuses to do so

2.2.2 Certification process

The certification process comprises all procedures which are in place to provide a subject with a certificate, such as:

- Subject requests a certificate at the RA
- RA sends a certificate request to the CA
- CA issues certificate
- Certificate and keys delivery to subject

2.2.3 CA key management process

The CA key management process comprises all procedures which are in place to manage the CA key pair during its complete lifecycle, such as:

- CA key pair generation
- CA key pair storage
- CA key pair backup
- CA key pair recovery
- CA public key dissemination (e.g. by self-signed certificate)
- CA key pair decommissionning
- CA key pair archiving
- Subject key management process

This key certificate management process comprises all procedures which are in place to manage the subject keys, such as:

- Subject key pair generation
- Subject key pair provisioning (e.g. by device provisioning)
- Subject key pair storage
- CA key pair backup
- CA key pair recovery

Logically the revocation of subject key pair (subection 2.2.6) can be also considered as part of this process.

2.2.4 Subject certificate management process

The subject certificate management process comprises all procedures which are in place to manage subject certificates, such as:

- Subject certificate generation
- Subject certificate delivery
- Subject certificate renewal, rekey and update
- Subject certificate dissemination
- Subject certificate suspension

2.2.5 Revocation process

The revocation process comprises all procedures which are in place to revoke certificates, such as:

- Certificate revocation request
- Certificate revocation
- Certificate revocation publishing (e.g. CRL, OCSP).

2.2.6 Other processes and services

There are more processes involved in trust services. Examples include:

- Validation services (core to certificate management)
- Time stamping services
- Authentication services
- Signature services
- Long-term archiving

Although these and other processes are not in the focus of the document, the recommendations can apply to them by analogy, taking into account they differences in nature.

2.3 Impact of security incidents

It is important to understand the consequences of a security incident to comprehend why it is critical for TSPs to respond promptly and appropriately to incidents. Most operations in the Internet that require a high assurance of proof of identity rely nowadays on the use of electronic certificates. Amongst the main consequences of a compromise of a TSP are:

2.3.1 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.

2.3.2 Eavesdropping on private communications

On the Internet, sensitive communication between entities is often secured against eavesdropping and spoofing, e.g. Web sites 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.

2.3.3 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.

2.3.4 Unavailability of services

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

Being able to delay or even entirely stop the TSPs services, e.g. the OCSP server[5], enables the attacker to interfere with the day-to-day operations of the parties relying on them.

2.3.5 Reputation damage

The business of a TSP 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 TSPs reputation and thereby its entire business.

[5] Online Certificate Status Protocol, described in RFC 6960 [25]

3 Identifying incident scenarios and attack vectors

After identifying the entities, processes and possible impacts on TSPs, it is important to develop an understanding of possible incident scenarios and attack vectors to understand the possible situations the trust service provider (TSP) might face.

3.1 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.

ENISA identified a group of incident scenarios[6] that classifies the identified type of events that could affect a (TSP) and that can be used by TSPs as a reference. In the following paragraphs, a description of the identified incident scenarios is provided. Although all descriptions given here focus on technical issues, it is possible to provoke the same incidents by organizational means, such as social engineering or coercion. In addition, most of the incidents can also be provoked by accident or human error.

3.1.1 Compromise of a Certificate Authority

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).

3.1.2 Compromise of a Registration Authority

The role of the Registration Authority is to verify the subject identity and to subsequently send a certificate issuance request to the Certificate Authority. Although the RA doesn't 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.

3.1.3 Compromise of the revocation services

It is important that the information regarding the status of certificates is correct, complete and available 24x7 so that e.g. 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.

[6] Please refer to "Guidelines for trust service providers, part 2 – Risk assessment"

3.1.4 Compromise of the cryptographic modules

A compromise of cryptographic modules occurs when the cryptographic algorithms, parameters, protocols, or implementations (SW or HW) 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 /encryption algorithm is weak, enabling an attacker to generate fake signatures / decrypt messages without having access to the private key. Note that bad parameters or implementations (SW or HW) can very well lead to weaknesses despite the fact that the algorithm or protocol being used is secure.

3.1.5 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 provider.

3.1.6 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 name of the victim.

3.1.7 Personal data breach

A personal data breach occurs when personal data provided to or produced by the TSP are disclosed to unauthorized entities. Personal data maintained by the TSP 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 TSP.

3.1.8 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 TSP 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 TSP on its behalf) loses exclusive custody of its private key, effectively allowing an attacker to supplant his/her identity or access confidential information.

3.1.9 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 TSP. 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.

3.1.10 Impact and probability of incident scenarios

In June and July 2013 ENISA conducted a survey among trust services providers, in which 46 participants took part. The goal of this survey was to identify security practices in force at these organisations[7].

Among others, it asked respondents to rate the incident scenarios in terms of impact and probability of occurrence for any TSP.

Figure 1 shows the results of the incident impact questionnaire. The estimated impact value represents the median impact score assigned by the trust service providers participating in the survey. Impact scores range from 10 (very high) to 0 (very low). We can see that the compromise of the CA is rated as worst scenario with a very high impact (8.7 of 10). The lowest rate is assigned to the compromise of a subject's key pair having still a medium impact (4.3 of 10). The ratings of the other scenarios are nearly linearly distributed between these two impact levels.

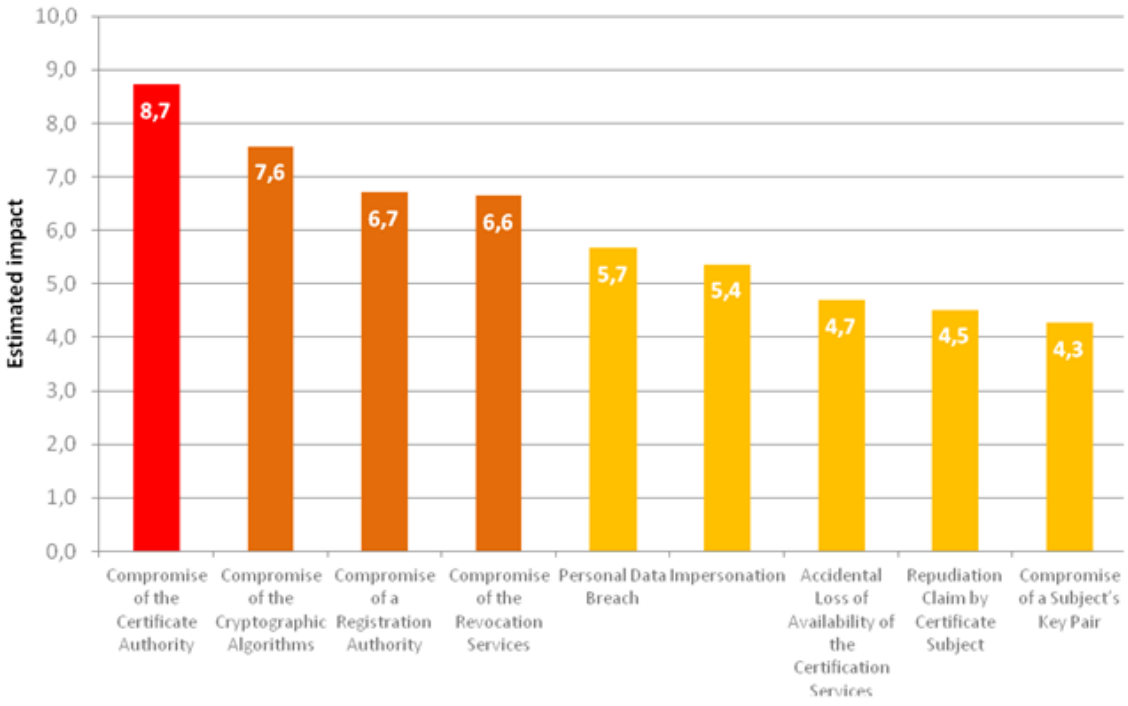

Figure 1: Estimated incident impact (based on survey results)

Figure 2 shows the results of the incident probability questionnaire. The estimated probability value represents the median probability score assigned by the 41 trust service providers participating in the survey. Probability scores range from 10 (very likely) to 0 (very unlikely). We can see that the repudiation claim by certificate subject is rated as most likely scenario with a medium probability. The least likely scenario is the compromise of the CA having a low probability. The second least likely

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

scenario is the compromise of the revocation services already scratching medium probability. The ratings of the other scenarios are nearly linearly distributed between the probability levels of the most likely and second least likely scenario.

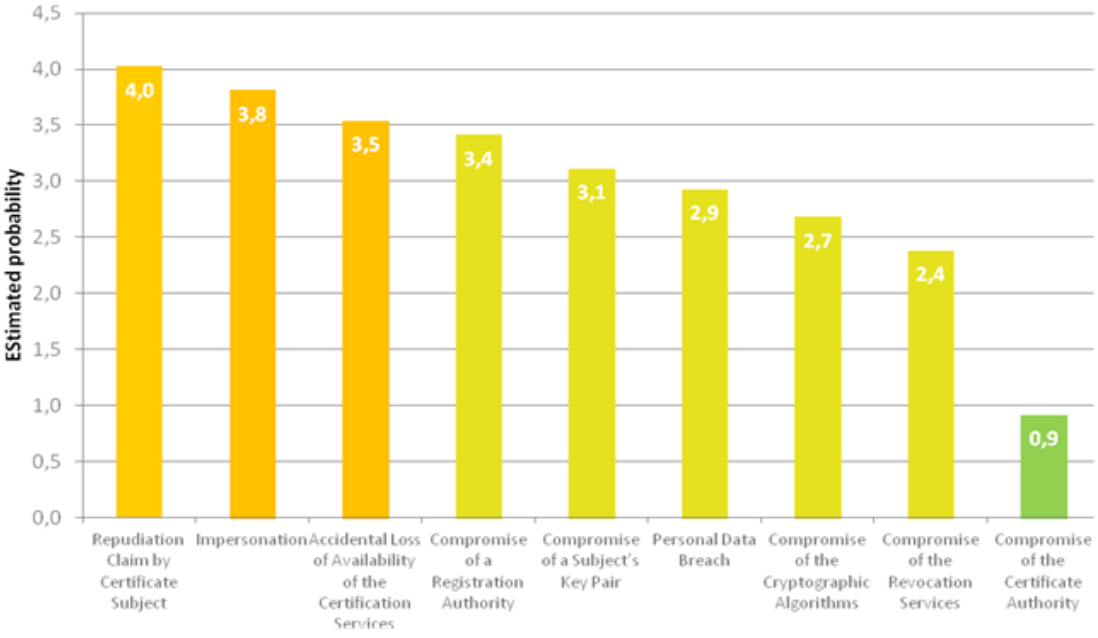

Figure 2: Estimated incident probability (based on survey results)

3.2 Attack vectors

An attack vector is a path or means by which an attack can be or is made[8]. 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 TSP 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.

3.2.1 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 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, TSPs should implement perimeter security measures and all kind of security tools on their networks. The TSP should also apply secure personal security

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

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 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 (SW or HW) 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, TSPs should update their cryptographic parameters (e.g. key length), implementations (e.g. crypto libraries or HSMs), protocols (e.g. key exchange), and even algorithms (e.g. hash algorithm) whenever indicated.

3.2.3 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 TSP personnel. This type of attack is usually hard to detect.

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

3.2.4 Physical attacks

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

TSPs 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 TSP processes.

TSPs 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 TSP 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.

3.2.5 Probability of occurrence of attack vectors

The ENISA survey on security practices of trust service providers asked respondents to rate the identified attack vectors in terms of probability of materialization for any TSP. The values were assigned by the 41 TSPs participating in the survey, from 1 (very unlikely) to 4 (highly likely).

The results, depicted in Figure 3, show that logical attacks are considered the most probable by most respondents (56% say highly likely or likely), followed by insider attacks (55% say likely or unlikely) and cryptographic attacks (55% say unlikely or very unlikely). Physical attacks are considered by the respondents the less likely to occur (89% say unlikely or very unlikely).

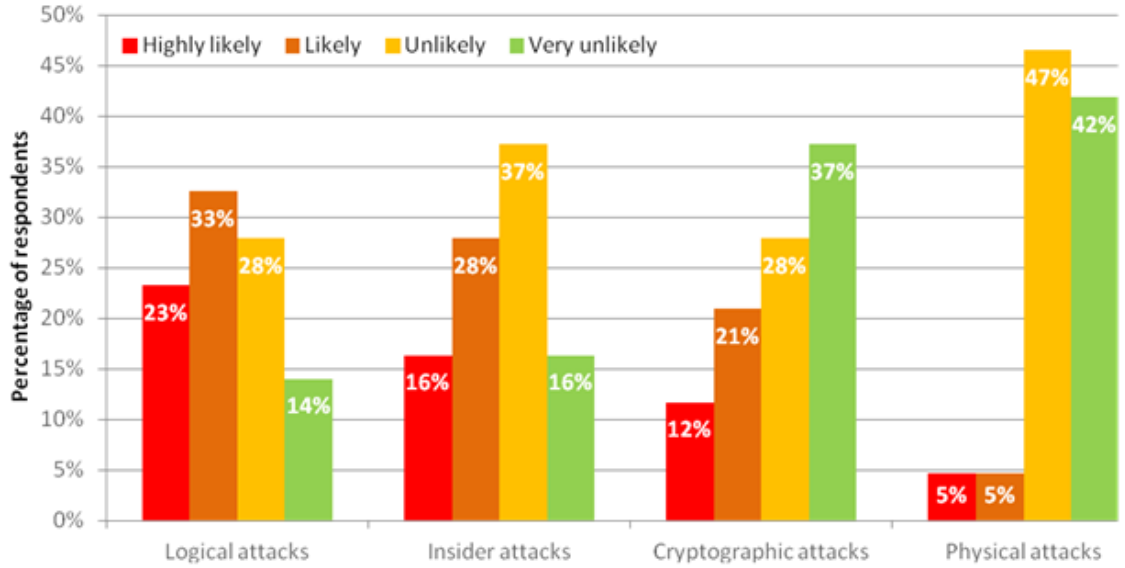

Figure 3: Attack vector occurrence probability (based on survey results)

4 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 TSP should prepare.

4.1 Enable means to gather alerts

4.1.1 Enable outside parties to report incidents

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

4.1.2 Enable systems for staff to report abnormal events

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

4.1.3 Follow alert systems from external sources

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

4.1.4 Activate alerts in internal systems

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

4.1.5 Conduct continuous self monitoring and self testing

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

4.2 Create an incident response capability

4.2.1 Create an incident response team

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

- Whether a 24x7 incident response capability is needed (which seems appropriate for 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.
- Whether central incident management response or distributed incident response is applied.

4.2.2 Create incident response procedures

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

4.3 Prepare staff and systems for an incident

4.3.1 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.

4.3.2 Train personnel

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

4.3.3 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.

4.4 Have means of communication with all stakeholders

4.4.1 Create a repository of certificate holders contact information

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

4.4.2 Create a repository of relying parties

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

4.5 Create a repository of supervisors and competent authorities

The TSP should establish a database with contact information regarding supervisors and competent authorities. Qualified EU providers (and all providers operating in Europe when the new Proposal for a Regulation comes into force) have to inform supervisory authorities of any security incident affecting the service without undue delay. Additionally, the TSP needs 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.

4.6 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.

4.6.1 Have agreements with other TSPs to obtain substitute certificates

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

4.6.2 Maintain updated information of your environment

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

- Lists of assets
- Network diagrams
- Applications and software versions
- Disaster procedures
- Recover and restore procedures
- Contingency plans

4.6.3 Have a service termination plan

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

5 Detecting and assessing the incident

Detection of an incident in a TSP may be triggered by different events. Reports may arrive to the TSP through the helpdesk or support contact addresses, be detected by staff in the internal systems or even by media and public sources.

Although not all unusual events will correspond to an actual incident, they are indicators and should be investigated by the TSP. During the detection phase, the TSP first line respondent should determine whether an incident is actually taking place. Training of personnel is important to help them to detect abnormal behaviour. Also, there should be a review process to assure that no incident slipped through due to wrong assessment.

If the TSP first line respondent assesses an incident may be occurring, the next phase is the incident analysis. 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.

The goal of the analysis phase is to determine the type of incident and execute the appropriate response plan. Events that indicate an incident, especially those concerning the detection of fraudulent certificate activities, are linked to different types of TSP incidents.

The TSP personnel should assess the circumstances of the breach, the information systems affected and all other relevant information to determine the type of breach. Correlation of events, training of personnel and existing procedures play an important role is this phase.

The following paragraphs provide some guidelines regarding different abnormal events that may take place in a TSP and how to assess them in order to identify the appropriate type of incident that is taking place.

5.1 Fraudulent certificate activities

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

- Certificates associated with man in the middle attacks
- Certificates associated to known malware sites
- Malware signed with certificates
- Subjects reporting that certificates associated with their name/organization 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 TSP.
- Contact the certificate subjects' to assess whether fraudulent activities are taking place.
- Assess the circumstances under which the certificate was issued:
    - Contact the RA to check registration logs and records.
    - Check certificate request and generation logs at CA.

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

5.2 Abnormal activities in information systems

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

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

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

5.3 Suspicious information in the certificate lifecycle management logs

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

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

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

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

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

5.4 Unaccounted key media

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

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

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

5.5 Loss of availability

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

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

5.6 Loss of custody of subject key

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

6 Responding to the incident

An effective and prompt response is critical for mitigating the impact of a breach in a TSP.

6.1 Types of breaches

Incidents at TSPs can be divided into two general types, and this classification plays an important role in selecting the appropriate response. The two mentioned types are:

6.1.1 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 Certificate Authority
- 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.

6.1.2 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 TSP. Among these incidents are:

- Personal data breach
- Loss of availability of the trust services other than revocation
- Repudiation claim
- Unability 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: with personal data breaches, to protect the confidentiality of the data; with loss of availability, to recover the service; with repudiation claim, to ensure traceability and accountability of actions.

6.2 Response guidance

The following sections provide guidance on how to respond to different incident scenarios in TSPs.

6.2.1 Responding to a CA compromise

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

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

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

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

6.2.2 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 issued by the 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 requested from the affected RA.
- Identify affected legitimate subjects and provide them with certificates from another RA, e.g. from a standby system or another TSP.

6.2.3 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.

6.2.4 Responding to a compromise of the cryptographic modules

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

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

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

6.2.5 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).

6.2.6 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.

6.2.7 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 TSP. 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.

6.2.8 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

6.2.9 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.

7 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 TSP should take the appropriate measures to minimize the possibility of the incident occurring again. The measures the TSP should take include:

7.1 Determine what facilitated the incident

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

7.2 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.

7.3 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.

7.4 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.

8 Learning from past incidents

Many trust service providers (TSP) have already been affected by an incident during the course of their operations. Prevention is critical for incidents not to take place, but as the following examples show, once the incident has occurred, the response can certainly make a difference on the impact for the users and the provider.

8.1 CA compromises

A while after the CA compromises presented here, updates of the OCSP standard (RFC 2560 [24] to RFC 6960 [25]) and the CA/B Forum Guidelines[9] (version 1.0.3 to version 1.0.4) have been issued, to address OCSP responses for non-issued certificates.

DigiNotar

One of the most widely known examples of breach in a TSP which illustrates a CA compromise is the DigiNotar case[10]. DigiNotar was a Dutch TSP operating from 1997 until 2011. DigiNotar provided two types of certificates. Certificates from their own root CA: "DigiNotar Root CA", and certificates as an intermediary of the Dutch Government root CA: "Staat der Nederlanden".

In July 2011, a fraudulent SSL certificate for Google domains was generated by an attacker who gained access to DigiNotar's internal systems. In the following weeks, at least 531 fake certificates were issued for popular Internet domains.

DigiNotar failed to react to the breach in due time, making it possible for the attacker to launch man-in-the-middle attacks and eavesdrop on private communications. DigiNotar became aware of an intrusion on July 19th 2011; however they didn't publically admit the breach until end of August 2011. Common Internet browsers started to remove DigiNotar from their trusted certificates list as they became aware of the possible fraudulent use.

An investigation was launched by the Dutch government on the incident. Although it was not clear whether the other CA, the one issuing certificates for the Dutch government systems, had been compromised, they decided to revoke all certificates on September 3rd 2011, making it impossible for many Dutch citizens (those who had obtained their certificates through DigiNotar) to access eGovernment platforms.

All these events and the failure to response diligently to the incident lead to DigiNotar going into bankruptcy. Furthermore, it is difficult to estimate how many entities were subject to an intrusion in their private communications by the use of fraudulent certificates.

The elapsed time frame between the detection and the public admission of the breach was more than one month, effectively giving the attacker an extended amount of time to perform fraudulent operations. The lack of a prompt response and the inability to clearly establish the impact of the incident lead to a loss of trust in DigiNotar that eventually caused the end of the company.

Globalsign

On similar dates to the compromise of DigiNotar, the same hacker who intruded DigiNotar claimed to have intruded Globalsign[11]. Globalsign conducted a throughout investigation by an external party

[9] https://www.cabforum.org/
[10] http://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112
[11] http://www.theregister.co.uk/2011/09/07/globalsign_suspends_ssl_cert_biz/

that concluded that only a peripheral web server was breached, but the intrusion never reached any CA operation systems and no fraudulent certificate issuance activity had taken place.

Turktrust

One of the last publically known incidents affecting a CA is the Turktrust case[12]. Turktrust is a large Turkish TSP. In 2011 Turktrust erroneously issued certificates meant to be subject certificates, but that were actually intermediate CA certificates with the capability of issuing new certificates whose validity would be attested by Turktrust. This case shows an example of a compromise of an intermediate CA due to an erroneous issuing of CA capabilities instead of an end user certificate.

One of the receivers of the erroneous certificates reported it to Turktrust and the certificate was revoked. However, the receiver of the other certificate, the public transport authority in Ankara, did not report the incident.. Google discovered in December 2012 that Chrome users are presented Google certificates which were not issued by order of Google. The investigation lead by Turktrust determined that the second certificate was installed in a proxy server which automatically generated certificates for visited sites to conduct security scans of the traffic. Aside from that no misuse of the certificate had taken place.

8.2 RA compromises

Comodo

Another example illustrates a Registration Authority compromise, such as the Comodo case[13]. On March 15th 2011 an affiliate Registration Authority of Comodo, a large TLS certificates provider, was compromised and nine rogue certificates were created for common Internet domains. The attack targeted a user account in the RA, which had the capability to issue requests for new certificates. In this case, the compromise was not of the CA, but of the RA, which has the responsibility to validate the identity of subjects requesting certificates.

Comodo became aware of the intrusion on March 26th 2011 and immediately revoked all fraudulent certificates and informed all relevant stakeholders. Activity was detected in Internet for only one of the rogue certificates.

The Comodo case shows an example of how compromising Registration Authorities can lead to fraudulent certificates. Comodo acted promptly and was able to determine the extent of the incident, revoking the fraudulent certificates.

8.3 Impersonation

VeriSign

Another case illustrates the example of an impersonation incident, the VeriSign case[14]. The VeriSign case is one of the first publicly known compromises to have occurred in a TSP. The breach was due to an attacker claiming to be an employee of Microsoft to whom VeriSign issued two code signing certificates. The fraudulent certificates could be used to sign malicious code to make it appear as signed by Microsoft, which would avoid raising any security alerts in the browser.

[12] http://nakedsecurity.sophos.com/2013/01/08/the-turktrust-ssl-certificate-fiasco-what-happened-and-what-happens-next/
[13] http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/
[14] http://news.cnet.com/2100-1001-254586.html

The certificates were issued on January 29th and 30th January 2001, and Microsoft was informed in March of the same year. VeriSign claimed they detected the possible fraudulent issuance on a routine audit.

VeriSign revoked the certificates, and included them in VeriSign's current CRL. However, because VeriSign's code-signing certificates didn't specify a link to the CRL location, browsers could not verify this information. Therefore Microsoft had to issue a security update in order for the browser to be able to check the revocation status of these certificates locally.

The fraudulent certificates were not detected to have been used in the Internet. VeriSign acted promptly revoking the certificates before they were used.

8.4 Cryptographic compromises

RSA-512

In November 2011, Fox-IT reported on several abused subject certificates[15]. The certificates in question were legitimately issued 512bit RSA certificates. In addition to their legitimate usage (e.g. for HTTPS servers), the corresponding private keys had been used to sign malware.

Presumably, attackers had successfully derived the private key from the public key contained in the certificates, which is known to take for 512bit keys at most a couple of weeks with modern equipment. As most of the certificates did not include any usage restrictions, it was possible to use e.g. certificates meant for authentication for signature purposes.

At least one of the CAs (Digicert Sdn. Bhd.) did not include a link for revocation checking into its subject certificates, which led to the revocation of the respective CA certificate to contain the damage.

8.5 Organizational failures

RSA-1024

In summer 2013, an international research team made their success in factoring 184 real world RSA-1024 keys public[16]. These keys were generated by smart cards issued by the Taiwanese government that were certified secure by multiple important standards: FIPS certification from NIST (U.S. government) and CSE (Canadian government), and Common Criteria certification from BSI (German government).

The cards were erroneously delivered in non-certified mode leading to the usage of a weak random number generator. This lead to keys sharing primes that could relatively easy be computed by bulk greatest common divider (GCD) extractions. By further investigating the randomness-generation failures, more keys, that did not share primes, were factored.

8.6 Lessons learned

Summarizing the paragraphs above, the main lessons learned are:

- Many types of TSP compromises have already happened; partly with serious consequences. More incidents are to be expected.

[15] https://www.fox-it.com/en/blog/rsa-512-certificates-abused-in-the-wild/
[16] http://smartfacts.cr.yp.to/smartfacts-20130916.pdf

- Serious compromises may happen without being attacked, just by an unfortunate series of events / human errors.
- Failure of responding diligently damages both the client and the provider.
- Awareness and quick and proper reaction to an incident limits the damage to both the client and the provider.
- Having proper processes, policies (including but not limited to validity periods and updates of cryptographic modules) and their enforcement and traceability are equally important as the technical security measures.
- Strong authentication of operators is of the essence, not only for CAs but also for RAs and other TSP authorities.
- Apart from algorithms and formats, the right choice of cryptographic parameters (e.g. key length) and additional attributes (e.g. validity period, key usage, revocation information, …) in certificates are of the essence.
- Security certifications of individual modules, even those following internationally renowned standards, do not guarantee the security or flawlessness of the services composed using such modules.

9 Recommendations

This section provides the most important recommendations contained in this document in short and general form. These recommendations target the Trust Service Providers and cover the following areas:

- Remember that security is an ongoing process that never stops
- Be aware of possible incidents and attack vectors
- Prepare for known and unknown incidents
    - The TSP should establish, if appropriate according to local legislation and field of use, a database of issued certificates with the contact information
    - The TSP should establish a database with contact information regarding (known) relying parties (or their representatives) that use their certificates
    - The TSP should establish a database with contact information regarding supervisors and competent authorities
    - The TSP should foster a culture of self monitoring and self testing
    - The TSP should define procedures for incident management
    - The TSP should have an updated list of roles and responsibilities of staff in case of an incident
    - The TSP should conduct incident response exercises periodically
- Have means to actually detect and assess incidents
    - The TSP should establish a support line or helpdesk where any information regarding suspicious activity can be received
    - The TSP should follow security alert systems and forums and be aware of the latest threats
    - The TSP should establish an adequate level of logging in all information systems
- Respond to incidents in a quick, effective, and reasonable way
    - TSPs should have an incident response team
    - The TSP should provide means to register any incident in a standardized format so that incident management personnel can response more effectively
    - Have (cold or hot) standby systems in place to take over the duties of the main system in case of an incident
    - TSP should be able to provide subjects with services from other providers until the operations can be resumed
- After an incident, close the gaps that made it possible
- Learn from past incidents – own and others'

Annex 1 – Definitions

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

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

Certificate: Electronic attestation which links electronic signature or seal validation data of a natural or a legal person respectively to the certificate and confirms those data of that person; **Certification Authority:** An entity trusted to issue certificates. A certification service provider may have one or several Certificate Authorities. It is generally a trusted party or trusted third party that accepts the responsibility of managing the certificate process by issuing, distributing and verifying certificates.

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

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

Cryptographic module: An umbrella term covering:

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

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

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

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

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

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

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

Event: Occurrence of a particular set of circumstances

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

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

Impact: The result of an incident.

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

Mitigation: Limitation of any negative consequence of a particular event

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Annex 2 – Abbreviations

CA Certification Authority

CABF CA/Browser Forum

CC Common Criteria

CEN European Committee for Standardization (Comité Européen de Normalisation)

CIMC Certificate Issuance and Management Components

CP Certificate Policy

CPS Certification Practice Statement

CRL Certificate Revocation List

CSP Certification Service Provider

CWA CEN Workshop Agreement

EAL Evaluation Assurance Level

ECC Elliptic Curve Cryptography

ECDSA Elliptic Curve Digital Signature Algorithm

EN European Standard

ETSI European Telecommunications Standards Institute

FIPS Federal Information Processing Standards

GCD Greatest Common Divider

HSM Hardware Security Module

HTTP Hypertext Transfer Protocol

HTTPS HTTP Secure

HW Hardware

ISO International Organization for Standardization

NIST National Institute of Standards and Technology

OCSP Online Certificate Status Protocol

PDS PKI Disclosure Statement

PIN Personal Identification Number

PKI Public Key Infrastructure

PP Protection Profile

PSE Personal Security Environment

QCP Qualified Certificate Policy

RA Registration Authority

RFC Requests For Comments

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

SHA Secure Hash Algorithm

SSCD Secure Signature Creation Device

SW Software

TLS/SSL Transport Layer Security/Secure Socket Layer protocol

TS (ETSI) Technical Specification

TSA Time Stamping Authority

TSP Trust Service Providers

TR (ETSI) Technical Report

VA Validation Authority

Annex 3 – Bibliography

ISO

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

ETSI

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

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

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

IETF

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

CEN

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CA/B Forum

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

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

NIST

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

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

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

Legislation

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

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

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

Others

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

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

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

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

European Commission standardisation mandate

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

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

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

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

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

NOTE:

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

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

Annex 4 – List of organisations taking part in the survey

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

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

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

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

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

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