Article 19 Incident reporting

Incident reporting framework for eIDAS Article 19

DECEMBER 2016

About ENISA

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

Contact

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

Acknowledgements

For the completion of this guideline ENISA has worked closely with a working group of experts from national regulatory authorities and ministries from across Europe: the Article 19 Expert Group. We are grateful for their valuable input and comments.

Last but not least, ENISA would like to acknowledge the contributions by Andrea Servida and Marco Fernandez-Gonzalez from European Commission.

ISBN: 978-92-9204-180-9 doi: 10.2824/67244

Table of Contents

Preface

The new regulation for electronic identification and trust services (Regulation (EU) No 910/2014[1], referred to as eIDAS), adopted on 23 July 2014, contains Article 19 which requires, among other things, that providers of trust services 1) assess risks, 2) take appropriate security measures to mitigate the risks, and 3) notify the supervisory body[2] about significant incidents/breaches. This triangle is also present in Article 13a of the Telecommunications Framework directive, which applies to the telecom sector, and Article 14 of the proposed Network and Information Security (NIS) directive, which applies to operators of critical infrastructures.

Article 19 also addresses various types of incident reporting to other different stakeholders (e.g. users, data protection authorities, competent national bodies for information security, ENISA etc.) involved in its application. Member States should efficiently analyse and then implement these notification flows in order to comply with the incident notification requirements of the eIDAS regulation.

In 2014, after eIDAS was adopted, ENISA initiated contacts with experts from ministries, agencies, supervisory bodies, authorities, et cetera, who are (or might become) involved with the application of Article 19. For the sake of brevity these are referenced as competent authorities[3]. The goal of these contacts has been to discuss and agree on the technical application of Article 19 by Member States. ENISA formed an expert group, to work together with experts from competent authorities on the application of Article 19 and, more generally, security incidents in trust services.

The focus of this document is the implementation of incident reporting and it aims at supporting the supervisory bodies in being aligned with obligations set out in Article 19. The Article 19 incident reporting framework has been prepared in consultation with the members of the expert group and reviewed by the private sector and the Forum of European Supervisory Authorities for Electronic Signatures (FESA) as well. Based on this document, ENISA has developed an on-line tool (CIRAS-T) to facilitate the procedure, which is expected to be finalised and adopted by the Member States and EFTA countries, by the end of 2016. This piece of work falls under Work Package 3.2C, Deliverable no 14 on 'Guidelines for mandatory incident reporting in the context of eIDAS' of the ENISA Work Programme 2016[4].

It has to be noted that article 19(4) of the eIDAS regulation foresees an implementing act on "formats and procedures, including deadlines …". Guidelines, described in this document, are a soft and flexible approach to address supervisory bodies' (SB) needs. The Commission may issue implementing acts in the future if deemed necessary / appropriate building upon the guidelines (and the results of their operational implementation).

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[2] Article 20 of the same regulation mentions that EU Member States supervise the qualified trust service providers (QTSPs) that they conform to the requirements laid down by the Regulation.

[3] Although especially in the first years this work involves also experts from ministries and authorities who are not yet formally appointed as supervisory bodies to implement Article 19.

[4] https://www.enisa.europa.eu/publications/corporate/enisa-work-programme-2016

1. Introduction

This document describes a framework for security incident reporting based on the requirements set by article 19 of the eIDAS regulation. It is being developed on a consensus basis between the experts of the working group formed by ENISA and it is reviewed by various relevant stakeholders from both the private and the public sector. The final report includes the consensual contributions and modifications of all stakeholders involved in its development and as such it is not a binding guideline.

Target audience

This document is primarily for the supervisory bodies (SBs) responsible for the application and enforcement of Article 19 in European Member States.

Scope

The scope of this document is the security incident reporting obligations contained in paragraphs 2 and 3 of Article 19 of the eIDAS regulation. It should be noted that the scope of reporting within MS could be broader than article 19 as defined by national legislation related to supervision.

Goal

This document is published by ENISA to provide support to supervisory bodies responsible for the technical application of Article 19. In particular, the incident reporting set out in paragraphs 2 and 3 of Article 19. However the report might prove useful also to other entities such as trust service providers, TSL scheme operators, conformity assessment bodies etc.

2. Article 19 and the wider policy context

This document regards the incident reporting obligations in Article 19 of the eIDAS regulation, called "Security requirements applicable to trust service providers". For the sake of completeness, and for the convenience of the reader, the full text of Article 19 is quoted below. Incident reporting is addressed in paragraphs 2 and 3, and briefly touched on in the last sentence of paragraph 1. The reader can also find an overview of related EU policy initiatives and legislation.

2.1 Full text of Article 19

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

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

Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA.

The notified supervisory body shall inform the public or require the trust service provider to do so, where it determines that disclosure of the breach of security or loss of integrity is in the public interest.

3. The supervisory body shall provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers."[5]

2.2 Policy context

In the following paragraphs, there is an overview of related EU legislation.

[5] According to article 17 (6) supervisory bodies have to notify Commission too. 'By 31 March each year, each supervisory body shall submit to the Commission a report on its previous calendar year's main activities together with a summary of breach notifications received from trust service providers in accordance with Article 19(2)'.

Article 13a of the Framework directive: *"Security and Integrity"*

The Telecommunications reform[6] package which was adopted in 2009, adds Article 13a to the Telecommunications Framework directive, regarding security and integrity of public electronic communication networks and services. Article 13a states that providers of public communication networks and services should take measures to guarantee security and integrity (i.e. availability) of their networks and that they must report to competent national authorities about significant security breaches. In addition, the Directive imposes obligations to national regulatory authorities to inform ENISA and authorities abroad when necessary, for example in case of incidents with impact across borders, and report to ENISA and to the Commission the summary incident reports annually. Article 13a also says that the Commission may issue more detailed implementation requirements if needed, taking into account ENISA's opinion.

The Commission, ENISA, and national regulators have since collaborated on implementing Article 13a and, in particular, agreed on a single set of security measures for the European electronic communications sector and a model for reporting on security breaches in the electronic communications sector to authorities abroad, to ENISA and the Commission.

While incident reporting is implemented differently at national level, with different procedures, thresholds, et cetera, nearly all national regulators use a common procedure, a common template and common thresholds for reporting to the Commission and ENISA.

In May 2012, ENISA received the first set of annual reports from EU Member States, concerning incidents that occurred in 2011. Every year ENISA receives incident reports from EU Member States and consolidates/aggregates these reports in a single public report.

Collected information is analysed in order to identify the root causes of incidents and recommendations are issued to further improve the resilience and security of EU communication networks. The guidelines together with the aggregated annual reports are public and one can find them at the ENISA website[7]. However, anonymised national reports are only available to the national authorities. National reports according to Article 13a of the Framework Directive are also shared voluntarily with operators who agree to provide information about their own incidents.

The European Parliament and the Council have proposed a Directive, establishing the European Electronic Communications Code under the light of the review of the Telecommunications Framework directive.[8]

---

[6] Available at: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Copy%20of%20Regulatory%20Framework%20for%20Electonic%20Communications%202013%20NO%20CROPS.pdf

[7] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports

[8] More information about the consultation are available at: https://ec.europa.eu/digital-single-market/en/news/proposed-directive-establishing-european-electronic-communications-code

Article 4 of the e-Privacy directive: "Security of processing"

The Telecommunications reform package also amended the e-Privacy Directive[9], which addresses data protection and privacy related to the provision of public electronic communication networks or services. Article 4 of the e-Privacy directive requires providers of public communication networks and services to notify personal data breaches to the competent authority[10] and subscribers concerned, without undue delay. According to this article, providers are obliged to notify personal data breaches to the competent national authority and the subscribers or individuals concerned, when the personal data breach is likely to adversely affect their privacy. In addition, they should take appropriate technical and organisational measures to ensure security of services and keep an inventory of personal data breaches, including the facts surrounding the breaches, the impact and the remedial actions taken.

Article 4 also says that the Commission may issue technical implementing measures regarding the notification formats and procedures, in consultation with the Article 29 Working Party, the European Data Protection Supervisor (EDPS) and ENISA.

In 2011, ENISA started an expert group, including experts from national data protection authorities, industry, and EDPS, to draft recommendations for the technical implementation of Article 4. In 2013, the Commission started an expert group with experts from national competent authorities, to meet and discuss issues concerning e-Privacy.

Data protection reform

The European Commission has proposed to reform the current European data protection framework (Directive 95/46/EC), and has proposed an EU regulation on data protection, which covers those organisations that are processing personal data, regardless of the business sector in which the organisation operates. The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) was adopted on 27 April 2016. It enters into application 25 May 2018 after a two-year transition period. Security measures and personal data breach notifications are addressed in Articles 30, 31 and 32:

- Organisations processing personal data must take appropriate technical and organisational security measures to ensure security appropriate to the risks presented by the processing.
- For all business sectors, the obligation to notify personal data breaches becomes mandatory11.
- Personal data breaches must be notified to a competent national authority without undue delay and, where feasible, within 24 hours, or else a justification should be provided.
- Personal data breaches must be notified to individuals if it is likely there will be an impact on their privacy. If the breached data was unintelligible12, notification is not required.
- Discussions about this proposal are still underway.

---

[9] Directive 2002/58/EC of the European Parliament and of the Council, of 12 July 2002, Concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[10] In a number of countries, the competent body for notification about personal data breaches related to electronic communications networks and services is not the telecom regulator, but a data protection authority or other agency.

[11] This provision extends personal data breach notifications beyond the electronic communications sector.

[12] In the recommendation for the technical implementation of Article 4, unintelligible data is described as data that has either been encrypted (asymmetric or symmetric), or hashed.

Network and information security (NIS) directive

The European Commission also published a European Cyber Security Strategy and proposed a directive on network and information security (NIS). The strategy and the directive explicitly refer to Article 13a as an example, and the proposed directive basically extends Article 13a to other critical sectors. In particular, Article 14 of the proposed NIS directive contains the following provisions:

- Market operators and public administrations should take appropriate security measures to protect their core services.
- Market operators and public administrations should report incidents to competent national authorities.
- Competent authorities should collaborate and share summaries of incident reports amongst the network of competent authorities.

In the preamble of the NIS directive, ENISA is tasked with acting as a bridge between the different types of authorities, including data protection authorities, national telecommunications regulators, and others, and to develop a single reporting template. The promulgation of the NIS directive has yet to be finalised.

ENISA's role and objectives

ENISA's role is mentioned in preamble 39 of the eIDAS regulation; *"To enable the Commission and the Member States to assess the effectiveness of the breach notification mechanism introduced by this Regulation, supervisory bodies should be requested to provide summary information to the Commission and to European Union Agency for Network and Information Security (ENISA)."*

Furthermore, article 19 (2), requires the 'notified supervisory body, where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, to inform the supervisory bodies in other Member States concerned and ENISA'. Finally, article 19 (3), requires the supervisory body to provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers.

ENISA's primary objective is to implement the incident reporting mandated in Article 19, i.e. to agree with the Member States on an efficient implementation of ad-hoc cross border incident and annual summary reporting.

Secondly, ENISA aims to use annual summary reporting for the following purposes:

- To provide feedback to supervisory bodies about:
    - security incidents that have significant impact on trust services and the personal data contained therein,
    - root causes of security incidents,
    - lessons learned from security incidents; and
    - incident trends.
- To provide aggregate (statistical) analysis of incidents for policy makers, the public and the industry, describing overall frequency and impact of trust service security incidents across the EU.
- To facilitate the exchange of experiences and lessons learned among supervisory bodies, to allow them to better understand and address security incidents.
- Issue recommendations and guidance for supervisory bodies, the private sector and policy makers.
- Evaluate the effectiveness of security measures in place.
- Develop more realistic incident scenarios for pan-European exercises.

Thirdly, ENISA aims to support supervisory bodies with the implementation of national incident notification schemes and in this way support efficient and harmonized incident notification schemes across the EU. Harmonized implementation of legislation creates a level playing field and makes it easier for trust service providers (TSPs) and users to operate across different EU countries.

3. Security Incident notification in Article 19

In this section the basic article 19 terms and concepts are presented together with some abbreviations that are used later on in this document.

3.1 Security incidents

Paragraph 1 of Article 19 asks providers to assess risks for the security of the trust services they provide, and take commensurate security measures to mitigate the impact.

Security incidents: Any breach of security or loss of integrity that has an impact on the security of the trust service provided. i.e. an **all-hazard approach** is foreseen– any incident that would have an impact on the security of the trust service.

Reportable security incidents: Any breach of security or loss of integrity that has a significant impact on the trust service provided[13] or on the personal data maintained therein.

Thresholds for trust service providers to notify (i.e. what is significant) the national supervisory bodies depend on national circumstances: different countries will adopt a different approach to setting national reporting thresholds, depending on national details, including: the type of providers in the sector, the population of the country, national legislation, etc. The objective of this document is to agree upon indicators and thresholds[14] which can be used as a basis for the annual summary reports submitted by the supervisory bodies to ENISA and the European Commission; they can also be used as guidance to supervisory bodies when setting national thresholds.

3.2 Services in scope

Services in scope are those defined in article 3 of the eIDAS regulation, namely:

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

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

Examples of business processes following under each service follow. The list of examples is only indicative.

[13] It has to be noted that the TSP shall only be responsible for reporting breaches on systems or processes that are under the TSP's control. In case core functions are subcontracted, the TSP remains liable for notifying security incidents that occur in the sub-contractor's systems.

[14] A threshold is considered as a triad of an indicator accompanied by specific values and measurement unit description.

3.2.1 Electronic signature service

3.2.1.1 Certification services (issuing certificates for electronic signatures)

- Creation
    - Registration and identification
        - Subject device provisioning
        - Certificate delivery to subject
        - Registration data and management (e.g. Subjects' certificates, RA private key destruction)
        - Subject certificate dissemination
        - Subject certificate renewal, rekey and update
    - Certificate creation data and management (e.g. Key pair generation, CA private key destruction)
    - CA Certificate dissemination
- Verification and validation
    - Key pair generation of Validation Authority (VA)
    - VA certificate creation data and management (e.g. Key pair generation)
    - CA private key destruction
    - Validation assets (e.g. CRLs, OCSP servers) management
    - Revocation data (e.g. CRLs) management and dissemination
    - TSP providing verification and validation services identity verification

3.2.1.2 Signature services (signature as a service)[15]

- Creation
- Registration and identification
    - Subject device provisioning
    - Signature delivery to subject
    - Registration data and management (e.g. Subject's signature, subject's certificate, RA private key destruction)
    - Subject signature renewal, rekey and update
    - Signature Creation data and management (e.g. Key pair generation, CA private key destruction)
- Verification and validation
    - Key pair generation of Validation Authority (VA)
    - VA certificate creation data and management (e.g. Key pair generation,)
    - CA private key destruction
    - Validation assets management

[15] The creation of electronic signatures is considered as a trust service. Nevertheless, one should keep in mind that when it is about creation of qualified e-signatures; generic qualified trust services as such are not defined in the Regulation.

- Revocation data management and dissemination
- TSP providing verification and validation services identity verification

3.2.2 Electronic seal service

3.2.2.1 Certification services (issuing certificates for electronic seals)

- Creation
  - Registration and identification
    - Subject device provisioning
    - Electronic seal delivery to subject
    - Registration data and management (e.g. subject's electronic seal, RA private key destruction)
    - Subject electronic seal renewal, rekey and update
  - Certificate creation data and management (e.g. Key pair generation, CA private key destruction)
  - CA Certificate dissemination
- Verification and validation
  - Key pair generation of Validation Authority (VA)
  - VA certificate creation data and management (e.g. Key pair generation)
  - CA private key destruction
  - Validation assets (e.g. CRLs, OCSP servers) management
  - TSP providing verification and validation services identity verification

3.2.2.2 Seal services (seal as a service)

- Creation
  - Registration and identification
    - Subject device provisioning
    - Seal delivery to subject
    - Registration data and management (e.g. Subject's signature, subject's certificate, RA private key destruction)
    - Subject seal renewal, rekey and update
  - Seal creation data and management (e.g. Key pair generation, CA private key destruction)
- Verification and validation
  - Key pair generation of Validation Authority (VA)
  - VA certificate creation data and management (e.g. Key pair generation)
  - CA private key destruction
  - Validation assets management
  - Revocation data management and dissemination
  - TSP providing verification and validation services identity verification

3.2.3 Electronic time stamping service

- Creation
    - Registration and identification
    - Registration data and management (e.g. subject's digital certificate)
    - Certificate creation data and management (e.g. TSA key pair generation, TSA private key destruction)
- TSA Certificate dissemination
- Verification and validation
    - Key pair generation of Validation Authority (VA)
    - VA certificate creation data and management (e.g. Key pair generation)
    - TSA private key destruction
    - Validation assets (e.g. CRLs, OCSP servers) management

3.2.4 Registered delivery service[16]

- Creation: what relates to signing / sealing key creation, certificate generation and distribution, signing / sealing process, control over the transmission path, acceptance of a delivered item by the recipient's delivery system, delivery receipt generation and transmission to the sender,
- Verification and validation
    - what relates to the transmission path
    - what relates to verifying all signatures/seals.

3.2.5 Website authentication certificate service

- Creation
    - Registration and identification
        - Subject device provisioning
        - Certificate delivery to subject
        - Registration data and management (e.g. Subjects' certificates, RA private key destruction)
        - Subject certificate dissemination
        - Subject certificate renewal, rekey and update
    - Certificate creation data and management (e.g. Key pair generation, CA private key destruction)
    - CA Certificate dissemination
- Verification and validation
    - Key pair generation of Validation Authority (VA)
    - VA certificate creation data and management (e.g. Key pair generation)
    - CA private key destruction

[16] For both public and private documents

- Validation assets (e.g. CRLs, OCSP servers) management
- Revocation data (e.g. CRLs) management and dissemination

3.2.6 Preservation services

- Key pair storage, backup and recovery
- RA/CA/VA/TSA private key pair destruction
- Adding information for extended long-term and archival signatures

3.3 Incident reporting flows

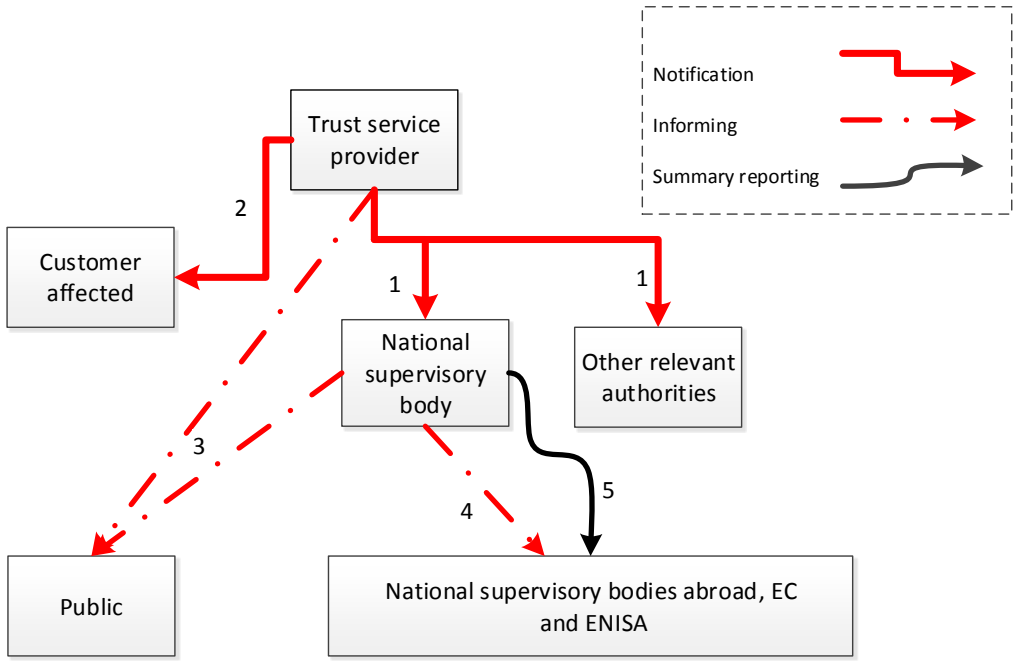
Article 19 addresses different types of reporting:

1. Notification about a security incident, that has a significant impact on the trust service provided or on the personal data maintained therein, within 24 hours after the trust service provider is becoming aware of it[17], to the supervisory body and, where applicable, other relevant bodies (e.g. DPA, national competent authority for information security, etc.).
2. Notification of the natural or legal person to whom the trust service was provided, who was affected by the security incident, without undue delay. In this document and in the diagram below, this abbreviates to 'the customer affected'
3. Informing the public (or requiring the provider to do so)
4. Informing relevant supervisory bodies abroad and ENISA, when a security incident involves two or more Member States.
5. Annual summary reporting to ENISA.

The diagram below shows the different incident reporting flows, numbered as above.

[17] By the provider or by the NRA or by an external party.

Figure 1: Overview of reporting flows in Article 19



Actors are explained in more detail, by referring to the legal text of Article 19[18]:

- Trust service provider: the "Qualified and non-qualified trust service providers" where the security breach is detected.
- Customer affected: the "natural or legal person to whom the trust service has been provided" who is affected by the security breach.
- Supervisory body: the body established in Member State territory or, upon mutual agreement with another Member State, a body established in that other Member State which is responsible for supervisory tasks in the designating Member State.
- Other relevant authorities: any other relevant bodies, depending on the national setting, such as the competent national body for information security or the data protection authority.

The diagram shows a number of reporting flows such as **annual summary reporting** (flow 5), **cross-border notification** (flows 1[19], 4) and **national incident notification** (flows 1, 2, 3). The next sections give more details for each reporting flow.

[18] A relying party is considered as part of the public.

[19] Flow no 1, might be either national or cross border because article 17 (1) of the Regulation foresees that Member States shall designate a supervisory body established in their territory or, upon mutual agreement with another Member State, a supervisory body established in that other Member State.

4. Annual summary reporting

The following are the key elements of annual summary reporting: the reporting template (what is reported), the reporting thresholds (when it is reported) and the means to submit the report (how the report is submitted).

Remark about information sharing: The annual summary reporting is not the only information sharing that happens between supervisory bodies and ENISA. Supervisory bodies have to be informed about cross-border incidents and severe security incidents. These incidents may also be discussed – on a case by case basis – at the regular meetings of ENISA's Article 19 Experts Group.

4.1 Annual summary reporting template

This section defines the reporting template. This will be implemented as a form for authorities to use when reporting to ENISA. Information to be collected, might at least include:

4.1.1 General description of the security incident

Free text description

4.1.2 Total duration of the security incident

The duration of the incident is the time span between the point of time when the degradation of the service is perceived and when the service is available again to the end-user, or simply the length of time the end-user was unable to use the service.

4.1.3 Impact of security incident

- Percentage of subscribers affected
- Severity of the incident: significant or severe impact or disastrous (see section 4.2)
- Personal data impacted
- Number of subscriptions
- Cross-border impact

4.1.4 Services affected

A (multiple) choice of one or more service(s) impacted by the incident. See Section 2.2.

4.1.5 Asset types affected

A (multiple) choice of one or more asset(s) impacted by the incident. See 0 Asset types.

4.1.6 Category of impact

Choose all that apply of: Confidentiality; Integrity; Availability.

4.1.7 Impact on assets

Find on the impact assessment table the corresponding value: Low; Medium; High.

4.1.8 Trust service concerned

Qualified or non-Qualified trust service provider.

4.1.9 Root cause category

Choose one of: human error, external or internal malicious actions, natural disaster, system failure, third party[20].

4.1.10 Detailed causes

Detailed description of causes and the course of the security incident.

4.1.11 Mitigating security measures

Description of mitigating security measures taken to address the security incident (in the response phase).

4.1.12 Improvements and lessons learned

Describe what measures have been taken or are planned to prevent similar incidents from occurring.

4.1.13 Notifications and information

- Other authorities notified, nationally
- Other authorities notified, abroad
- Customers affected notified
- Public informed
- Information disclosure by supervisory body under freedom of information legislation

4.2 Indicators for annual summary reporting

Providing a framework for determining the importance of a TSP's reportable incident is fundamental to the effectiveness of the overall reporting scheme. Paragraph 2 of Article 19 says that security incidents with a "*significant impact"* should be reported. Thus, Article 19 will be most effective if a framework is put in place that allows for consistency and clarity in weighing an incident's significance. Member states can take different approaches to defining reporting thresholds (see 0), thus it is important to set notification indicators and thresholds which are the same for all Member States.

4.2.1 Scenarios/examples of security incidents in the context of eIDAS article 19

Two groups of incident examples are presented: the service specific chapter contains incident examples with an impact on each specific trust service and the generic one which contains grouped incident examples with

[20] The category "third party failure" should be used for incidents where the root cause is outside the direct control of the provider, for example, when the root cause occurred at a contractor used for outsourcing, or at an organization somewhere along the supply chain.

an impact on all or most of the eIDAS service. This approach is based on the classification of incidents in different impact levels. The severity of security incidents is rated on a scale from 1 to 5:

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

Only incidents of severity level 3 and beyond are reportable. Below there is a list of examples of incident scenarios which is not exhaustive. This list should be used as a general guidenline as regards level classification. Given the circumstances of each incident, when core services are affected, it is at the discretion of each Supervisory Body to assign a different level value.

Examples for level 2

- **The same sourced clock signal arrives at different components at different times. This can be produced by many different causes.**
- **Different local timestamping units with local time do not reflect the real time. Not using a real TSA can produce different times when generated locally because they are based on local computer time which can reflect another time different than the official one.**
- **The delivery service produces erroneous evidences due to inaccurate responses by the signing platform.**
- **Unavailability of the recipient address due to several causes.**
- **The evidence is not maintained properly or not even stored.**
- **The request has been delivered correctly, the evidences generated and signed but the sender is unable to check the successful conclusion of the service because he is unable to receive the evidence due to several reasons, for example, in a REM solution, the sender email box is full and can´t receive any email.**
- **Applications are experiencing delays when interacting with the signature/seal creation platform even if the platform is still creating the signature.**
- **Applications are experiencing delays when interacting with the platform even if the platform is still validating the signature.**
- **Issues that can generate a possible compromise of the hardware which supports the software platforms.**

Examples for level 3.

- **An applicant claims an incorrect identity by using a forged ID.**
- **A subscriber denies registration, claiming that did not register that token.**

- A key created by the TSP for a subscriber is copied by an attacker as it is transported from the TSP to the subscriber during token issuance.
- A new password created by the subscriber is modified by an attacker as it is being submitted to the TSP during the credential issuance phase.
- A person claiming to be the subscriber is issued credentials for that subscriber.
- A physical token is stolen by an attacker.
- The responses to token prompts are easily discovered through searching various data sources.
- The subscriber's token has been copied with or without his or her knowledge.
- The token secret or authenticator is revealed to the attacker as the subscriber is submitting the token to send over the network.
- The token is exposed using analytical methods outside the authentication mechanism.
- The token secret or authenticator is captured by fooling the subscriber into thinking the attacker is a third relying party.
- The attacker establishes a level of trust with a subscriber in order to convince the subscriber to reveal his or her token or token secret.
- Usernames and passwords stored in a system file are revealed.
- The file that maps usernames to passwords within the TSP is hacked so that the mappings are modified, and existing passwords are replaced by passwords known to the attacker.
- The credential has been copied without knowledge for fraudulent use.
- An attacker is able to view requests and responses between the CA and the VA.
- An attacker is able to masquerade as the CA and provide bogus responses to the VA verification requests.
- The password file or the TSP is unavailable to provide password and username mappings.
- Password renewed by the TSP for a subscriber is copied by an attacker as it is transported from the TSP to the subscriber.
- New password created by the subscriber is modified by an attacker as it is being submitted to the TSP to replace an expired password.
- The TSP is compromised through unauthorized physical or logical access resulting in issuance of fraudulent credentials.
- An attacker takes advantage of a weak credential issuance/renewal protocol
- Stale CRLs allow accounts (that should have been locked as a result of credential revocation) to be used by an attacker.

- A hardware token is used after the corresponding credential was revoked or expired.
- Applications request for the status of a certificate and they are provided with erroneous answers.
- Lack of synchronisation amongst the different time sources used by the TSP.
- No access to the signature/seal creation and validation and verification services: The services are not accessible.
- No access to the timestamping service: The timestamp service is not accessible.
- No access to the certificate validation service: the validation of certificates service is not accessible.
- Although the signature/seal creation platform can access to the different platforms needed, the response received by these platforms is inaccurate and then the signature/seal can´t be created.
- Due to the lack of updated signature formats the platform creates signatures which are not in line with the standards.
- The TSP provides multiple signature/seal creation service platforms which are not synchronised, and this creates incorrect configurations and issues when accessing one or each other different platform.
- No access to the preservation of electronic signatures/seals service: the preservation service is not accessible.
- The TSP provides multiple validations of signatures/seals service platforms which are not synchronised, and this creates incorrect configurations and issues when accessing one or each other different platform.
- Although VA and/or TSA are accessible by the signature/seal validation platform, the response received by these platforms is inaccurate (see validation and timestamping services) and then the signature can´t be validated.
- No access to the signatures/seals creation and validation and verification services: The service is not accessible.
- An attacker manages to gain access to the data preserved.
- The integrity of the information preserved is altered over the years due to different causes (e.g. improper environmental conditions, media obsolescence, purposeful destruction or theft, computer virus, hardware, software or operator error).
- The tools which were used to generate the original data become obsolete and not supported by their vendors any more.
- Online/offline guessing: An attacker performs repeated logon trials by guessing possible values of the token authenticator.

- **Phishing: A subscriber is lured and tricked into revealing his or her token secret, sensitive personal data or authenticator values.**
- **Pharming: A subscriber is routed to an attacker's website through manipulation of the domain name service or routing tables.**
- **Eavesdropping: An attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the claimant.**
- **Replay: An attacker is able to replay previously captured messages to authenticate as that claimant.**
- **Session hijack: An attacker is able to insert to a successful authentication exchange between the two parties.**
- **Man in the middle: An attacker intercepts and alters the content of the authentication protocol messages.**
- **An incident with an impact on platform software: This scenario covers all the possible impact on the software used for a TSP to provide the trust services specified as in eIDAS. It involves possible compromise of the CA, RA, VA, TSA, signing, preservation and delivery software.**
- **Inadequate use of algorithms: This scenario affects key generation or certificate generation, electronic signature creation, etc. It involves the use of deprecated, weak or obsolete algorithms.**
- **Archive issues: According to eIDAS, the archival assets cover all aspects related to documentation and the log files of all tasks performed by the TSPs.**
- **Networking issues: Unavailability of networking infrastructure including hardware (firewalls, routers, cables …) as well as software (the firmware managing the devices).**
- **Compromise of supporting tools**

Examples for level 4

- **Inconsistency between OCSP and CRL information.**
- **An attacker manages to fraudulently repeat or delay a valid data transmission.**
- **The validation service is temporarily unavailable causing applications fail due to not having a proper response for those who didn´t cache answers.**
- **The validation service is temporarily unavailable causing applications fail due to not having a proper response for those who didn´t cache answers.**
- **A compromised TSA may incur in the issuance of incorrect or fraudulent time stamp tokens**
- **Due to the lack of updated signature formats the signing platform creates signatures which are not in line with the standards and can´t be validated properly.**

- **Due to the lack of updated signature formats the signing platform creates signatures which are not in line with the standards and can´t be validated properly.**
- **Unintentional use of certificates for other purposes.**

Examples for level 5

- **Compromise of private keys: The secrecy of the private key is critical for each asymmetric cryptosystem. Any compromise of the private key severely affects the users and the services which depend on this key[21].**
- **Compromise on key devices: For example HSM (Hardware Security Model), smartcards, USB tokens and FIDO token. It implies the loss, robbery, blocking, etc. of the device and also the unavailability to use/recover/revoke the cryptographic material.**

For detailed mapping of these scenarios with the eIDAS services, please refer to Annex C:.

4.3 ENISA annual incidents report

From January to March of each year, the Member States submit their annual reports to ENISA. Then, ENISA aggregates, via secure communication channels, the Member State's annual summary reports and analyses the data. ENISA's resulting public report will provide an aggregated and anonymized overview of security incidents affecting trusted services across the EU; omitting details on individual incidents.

[21] The impact is not the same for all services e.g. creation, validation, timestamping, signing services, but the compromise of the keys is critical for TSP's business, even if a TSP offers only certificate issuing service or validation service, or more than one services

5. Cross-border notification

Article 19 also requires the supervisory body to *inform* the supervisory bodies in other EU Member States (cross-border notification). Article 19 states: *"Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA."*

The goal of cross-border information is to inform supervisory bodies abroad, about recent and/or ongoing incidents[22], which may be relevant for them.

The key elements of cross-border incident reporting are: the reporting template (what is reported), the criteria for reporting (when it is reported) and the means to submit the report (how the report is submitted).

Remark about incident response: Note that not every supervisory body has a 24/7 or crisis management role, which means that authorities in some Member States may not be able to notify or receive notifications outside office hours. Therefore this cross-border information sharing might not be used for incident response or crisis management purposes, see below. In all EU countries there are national CERTs, which are part of a worldwide network of CERTs for 24/7 communication and response to security incidents.

5.1 Cross-border notification template

Cross-border notification is an informal, ad hoc process, which happens largely at the discretion of supervisory bodies. Depending on the setting, supervisory bodies may use a template, for example, the template for annual summary reporting (see 4.1).

5.2 Criteria for cross-border notifications

The legal text of Article 19 implies two criteria for informing supervisory bodies in other Member States:

- Customers affected: Authorities should inform authorities in other Member States only when customers (i.e. natural or legal persons) in that other member state are affected.
- Appropriate: Authorities should only inform when it is appropriate.

The interpretation of the first criterion has to be seen on a case-by-case basis. Here are some examples:

No need to notify other MS supervisory bodies

- *A breach of security of a TSP in country X impacts a trust service only used by the citizen of country X living in country Y to interact with country X authorities.*

Need to notify other MS supervisory bodies

- *One may consider that a breach of security occurring to a trust service provider providing trust services only at national level might have a cross-border impact if the customers are using such trust services to carry out cross-border transactions (with public authorities in another MS for example).*

[22] In order to achieve this, a two steps reporting approach (see 6.2) might needed.

- *Unavailability of TSL (CRL/OSP) will affect validation services of other EU countries, fake certificate could be used in systems of all EU countries as well. The TSP in country X, where the security breach took place, should assess and then determine on a case-by-case basis to notify the supervisory bodies in other MS as indeed a significant security breach affecting a validation service might potentially concern other MS.*

The following is a non-exhaustive list of examples of cases that it would be appropriate to undertake cross-border notification.

- *Incidents affecting services or websites or legal persons based in other EU countries*
- *Incidents involving equipment or services that are also in use in other EU countries*
- *Incidents with causes affecting other EU countries such as large scale DDoS attacks.*
- *Incidents requiring actions by the supervisory body abroad.*
- *Incidents affecting governmental affairs in other EU countries*

5.3 Cross-border notification process

ENISA maintains a contact list of email addresses and telephone numbers of contact points at supervisory bodies to enable cross-border information sharing. The contact list contains:

- Information about the supervisory body (name, street address, general phone number, URL)
- Information about two contact points (name, phone number, email, contact availability)
- Other remarks (any relevant information for the contacting body, such as X.509 certificates, PGP keys, or response times, shifts, etc.).

The contact list is provided to supervisory bodies upon request (resilience@enisa.europa.eu). The contact list is updated by the bodies when needed. The contact list is maintained and updated at a designated URL.

6. National incident notification

This section does not contain any guidance for Member States because national circumstances are different: in each country, the relevant authorities are different, with different resources, different responsibilities, and so on. The reader can find two fictitious examples of how Member States could set up a framework for notifying supervisory bodies and informing the public about national incidents under the eIDAS regulation as well as with a template for national notifications.

Remark about single point of notification: *Note that the article asks trust service providers to notify the supervisory body and other relevant authorities. In some settings this may be confusing for providers, causing double work and delays in compiling different incident notification templates and forms. To simplify notification procedure, Member States have two options:*

Set up a single-point-of-contact[23] for notification of incidents. In such a setting, the single-point-of-contact would relay or forward the notification to other relevant authorities. This single point of contact might or might not be the supervisory body. However, in some cases this might be cumbersome because:

- communication channels between different national authorities are set by national administrative laws which are difficult and time consuming to change;
- it might add delays to the incident reporting production line because of the extra time needed by the intermediate body which first receives and then evaluates the notification information before forwarding it to the competent authority; and
- different authorities need access to different data subsets of the reported information. This means that the receiving authority should be empowered to take decisions on this matter which sometimes might be proved difficult especially in cases that personal data are involved the decision making.
- TSP's have to consider laws and industrial standards which might not be known to the single point of contact entity.

Develop a single template[24] that is sent to different recipients by the TSP.

6.1 National notification framework examples

Example Country A:

Certification service providers have to notify the supervisory body immediately of all circumstances which do not allow to provide the certification services in accordance with the policy documents. Changes of the policy documents must be reported to the supervisory body before they become effective. Termination of services must be reported to the supervisory body three weeks in advance. Failure of both the primary and the secondary system for directory and revocation services must be notified to the supervisory authority within one calendar day.

[23] For more details on the single-point-of-contact principle under eIDAS one can access http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.053.01.0014.01.ENG.

[24] An example of such a template is described in to ISO/IEC 27035:2011 Annex D.4.

There is no standard form for notification because of the very different nature of this kind of incidents. Formally, there is no two-step approach for the notification. But every incident notification of a Trust Service Provider (TSP) leads to an investigation by the supervisory body where the TSP has to answer questions until the circumstances of the incident are sufficiently clear to the supervisory body.

Granting qualified status to TSPs contain, among others, the following notification requirements:

- **System failure, in particular regarding directory and revocation services, has to be reported unless it has been resolved within 24 hours.**
- **Shortage of qualified staff has to be reported if it is impossible to operate in accordance with the provider's role model.**
- **Suspect of compromise of TSP's signature-creation data has to be reported in any case.**
- **Deficiencies detected in the course of internal audits have to be reported unless they do not constitute the breach of minimal prescribed requirements or they have been resolved within three working days.**

Example Country B:

Listing of non-qualified providers, thresholds for reporting, 24/7 point of contact for regulator, CERT and DPA, two-step approach (notify first, report later).

6.2 National notification template example

When it comes to notifying authorities, it is very common that the providers of a service adopt a two phase approach. According to this, the provider submits an initial and short description of the incident to the supervisory body and then, at a later stage, when details of the incident have been identified, he/she provides a more detailed and descriptive notification[25]. Information collected from an incident notification might include:

First incident notification

- Date and time the security incident detected (or started if known already)
- Contact details: contact details for questions about this security incident
- Provider concerned: name of the company
- Trust service(s) impacted (or potentially impacted): description of the service(s)
- Personal data impacted (or potentially impacted): description of the personal data impacted
- Short description of the security incident

[25] In order to follow development of long lasting incidents the supervisory body might require a regular reporting scheme. E.g. by adding a field to the incident notification for expected next report or by requiring one report at regular intervals during the lifetime of the incident.

- Measures taken or planned: summarize what measures are taken or planned
- Cross-border impact

Final incident notification

- Date and time the security incident started
- Date and time the security incident detected by the TSP
- Contact details: contact details for questions about this security incident
- Provider concerned: name of the company
- Trust service(s) impacted: description of the service(s)
- Security feature(s) affected: confidentiality, integrity, availability etc.
- Personal data impacted: description of the personal data impacted
- Number of customers affected
- Duration of the incident
- Root cause category: One of human errors, malicious actions, natural disaster or system failure.
- Detailed cause of the security breach
- Detailed assets affected
- General description of the security incident: For example affected IT-systems, how was the incident detected, how long the incident was active, is there a vulnerability in a software which involves a third party etc.
- Cost estimation
- Measures taken: summarize what measures were taken to mitigate the incident
- long term measures, taken or plan, to avoid similar incidents from happening in the future
- Cross-border impact
- Other authorities notified
- Customers affected notified
- Public informed

Annex A: Threats and assets

This annex contains a dictionary of terms for threats and causes. The main use of this dictionary/vocabulary is to use them in reporting forms.

A.1 Terminology

A threat is defined as follows[26].

Threat: A threat is an event or a circumstance that could cause a security incident

This definition is based on the definition of a security incident that is common in international standards (such as ISO standards).

The word "cause" is used to speak about a threat when it has already caused an incident (in the past).

A.2 Root cause categories

Five different root cause categories are identified. Root cause categories are very broad categories that describe the underlying problem. This categorization is often subjective and a matter of judgement.

A.2.1 Human error

The category "human error" includes incidents caused by human error during the operation of equipment or facilities, the use of tools, the execution of procedures, etc.

A.2.2 System failures

The category "system failures" includes incidents caused by failures of a system, for example, hardware failures, software failures or errors in procedures or policies.

A.2.3 Natural disaster

The category "natural disaster" includes incidents caused by severe weather, earthquakes, floods, wildfires, and so on.

A.2.4 Malicious actions

The category "malicious actions" includes incidents caused by a deliberate act by someone or some organisation.

A.2.5 Third party failures

The category "third party failure" includes incidents where the cause was not under direct control of the provider, but some third-party.

[26] This definition is similar to the definition in ISO27K5, which defines a threat as the cause of an incident.

A.3 Detailed threats and causes

A non-exhaustive list of more detailed threats and causes follows.

A.3.1 Denial of service attack

A Denial of Service (DoS) attack aims to overload systems with traffic; such attacks can have an impact on the continuity of trust services.

A.3.2 Malware and viruses

Malware can affect databases, servers, etc., which could have an impact on the security of trust services.

A.3.3 Theft or loss of equipment

Hardware theft could have an impact on trust services, for example, where theft damage systems, in particular, multi-purpose IT equipment, or valuable items, such as HSM or large batteries, are valuable and portable.

A.3.4 Theft or loss of data

Theft of data may have an impact on the well-functioning of trust services and on the privacy of the customers' personal data as well.

A.3.5 Power cut

Power cuts of the (public) power grid, can have an impact on infrastructure that relies on power.

A.3.6 Hardware failure

Hardware failures (when physical hardware breaks) could affect physical infrastructure such as servers, routers, HSMs, etc. and impact trust services.

A.3.7 Software bug

Software bugs[27] could have an impact on ICT systems, such as routers, servers, databases, et cetera, and in this way impact trust services.

A.3.8 Faulty hardware change/update

A change or update of hardware, for example, for maintenance, replacement, or renewal, could go wrong and have a negative impact on trust services.

A.3.9 Faulty software change/update

Software changes or updates, for example, the installation of new software or software patches, could go wrong and have a negative impact on trust services. Note: this threat includes software such as 'configuration files'.

[27] Zero day threats are also included.

A.3.10 Tampering of personal data

Tampering of personal data has an impact on the well-functioning of trust services and on the privacy of the customers' personal data as well.

A.3.11 Eavesdropping

Eavesdropping may have an impact on the confidentiality of the data and on the privacy of the customers' personal data as well.

A.3.12 Cryptanalysis

Cryptanalysis may have an impact on the confidentiality of the data and on the privacy of the customers' personal data as well.

A.3.13 Overload

Overload of traffic and usage (e.g. too many CRL requests) could impact trust services.

A.3.14 Policy or procedure flaw

A flaw in a policy or procedure, or the absence of a policy or a procedure, could have a negative impact on trust services.

A.3.15 Security shutdown

Security risks could force a provider to shut down a service, for example, in order to have the time to patch software vulnerability.

Annex B: Assets

This annex will contain a dictionary of terms for assets. The main use of this dictionary/vocabulary is to use them in reporting forms

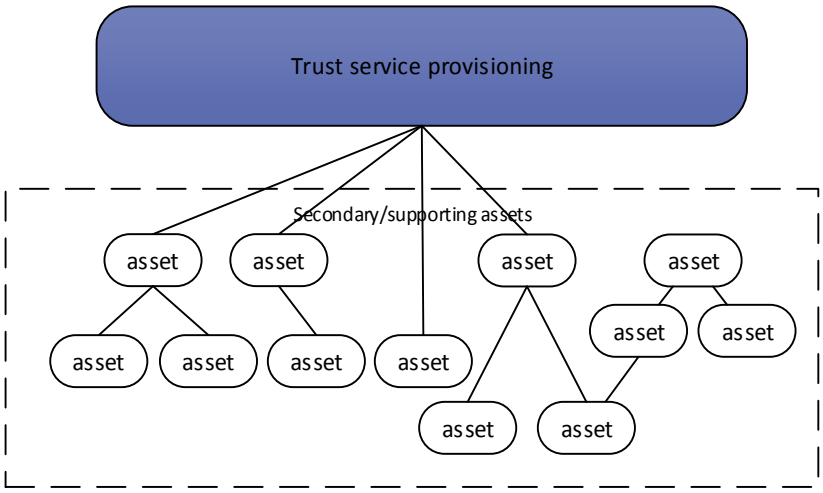
B.1 Terminology

An asset is basically anything of value. Assets could be abstract assets e.g. processes or reputation, virtual assets e.g. data, physical assets e.g. cables or a piece of equipment, human resources, money, etc. In this section, the focus is on the following assets:

Scope: The assets in scope are those assets that support the provision of trust services.

This means that abstract assets like 'money' or 'reputation' are out of scope. Similarly, suppose a provider has an online store for selling smartphones and subscriptions. The shopping cart system is an asset, but it is out of scope of this guideline because it does not directly support the provisioning of network and communication services.

Figure 2: Assets in scope of Article 19



B.2 Asset types

In this section different asset types are listed as a means to provide a vocabulary for authorities to use when reporting security incidents[28]:

- Certification Authority (CA) platform

[28] The ENISA report on "Risk assessment Guidelines for trust services providers – Part 2", contains a comprehensive and detailed list of assets in a Trusted Service Provider (TSP). The report is available at http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp2-risk.

- Validation Authority (VA) platform
- Time Stamping Authority (TSA) platform
- Registration Authority (RA) platform
- Generation and validation of signatures/seals platform
- Preservation of signatures/seals platform
- Registered delivery service platform
- Network platform
- Archive
- Hardware
- Software

Annex C: Scenarios/examples of security incidents in the context of eIDAS article 19

Two groups of incident examples are presented: the service specific chapter contains incident examples with an impact on each specific eIDAS service and the generic one which contains grouped incident examples with an impact on all or most of the eIDAS services.

C.1 Service specific

- A.1 Creation of certificates service
  - A.1.1 Registration process

A.1.1.1 Registration

Impersonation of claimed identity: An applicant claims an incorrect identity by using a forged ID.

Repudiation of registration: A subscriber denies registration, claiming that did not register that token.

A.1.1.2 Issuance

Disclosure: A key created by the TSP for a subscriber is copied by an attacker as it is transported from the TSP to the subscriber during token issuance.

Tampering: A new password created by the subscriber is modified by an attacker as it is being submitted to the TSP during the credential issuance phase.

Unauthorised issuance: A person claiming to be the subscriber is issued credentials for that subscriber.

  - A.1.2 Tokens

Theft: A physical token is stolen by an attacker.

Discovery: The responses to token prompts are easily discovered through searching various data sources.

Duplication: The subscriber's token has been copied with or without his or her knowledge.

Eavesdropping: The token secret or authenticator is revealed to the attacker as the subscriber is submitting the token to send over the network.

Offline cracking: The token is exposed using analytical methods outside the authentication mechanism.

Phishing or pharming: The token secret or authenticator is captured by fooling the subscriber into thinking the attacker is a third relying party.

Social engineering: The attacker establishes a level of trust with a subscriber in order to convince the subscriber to reveal his or her token or token secret.

  - A.1.3 Token and credential management

A.1.3.1 Credential storage

Disclosure: Usernames and passwords stored in a system file are revealed.

Tampering: The file that maps usernames to passwords within the TSP is hacked so that the mappings are modified, and existing passwords are replaced by passwords known to the attacker.

Duplication: The credential has been copied without knowledge for fraudulent use.

A.1.3.2 Token and credential verification services

Disclosure: An attacker is able to view requests and responses between the CA and the VA.

Tampering: An attacker is able to masquerade as the CA and provide bogus responses to the VA verification requests.

Unavailability: The password file or the TSP is unavailable to provide password and username mappings.

A.1.3.3 Token and credential issuance/renewal/re-issuance

Disclosure: Password renewed by the TSP for a subscriber is copied by an attacker as it is transported from the TSP to the subscriber.

Tampering: New password created by the subscriber is modified by an attacker as it is being submitted to the TSP to replace an expired password.

Unauthorised issuance: The TSP is compromised through unauthorized physical or logical access resulting in issuance of fraudulent credentials.

Weak protocol: An attacker takes advantage of a weak credential issuance/renewal protocol

A.1.3.4 Token and credential revocation/destruction

Delayed revocation/destruction of credentials: stale CRLs allow accounts (that should have been locked as a result of credential revocation) to be used by an attacker.

A hardware token is **used after** the corresponding credential was revoked or expired.

A.2. Validation and verification of certificates service

Incorrect answer when validating client certificates: Applications request for the status of a certificate and they are provided with erroneous answers.

Inconsistency between OCSP and CRL information.

Replay attacks: An attacker manages to fraudulently repeat or delay a valid data transmission.

Unavailability[29]: the validation service is temporarily unavailable causing applications fail due to not having a proper response for those who didn´t cache answers.

[29] Provided that unavailability is beyond the communicated SLA and imposes security risks beyond responsibilities communicated to relying parties.

A.3 Creation, validation and verification of electronic Timestamps service

No synchronization of TSA times: Lack of synchronisation amongst the different time sources used by the TSP.

Clock skew: the same sourced clock signal arrives at different components at different times. This can be produced by many different causes.

Local timestamping: Different local timestamping units with local time do not reflect the real time. Not using a real TSA can produce different times when generated locally because they are based on local computer time which can reflect another time different than the official one.

Unavailability[1]: the validation service is temporarily unavailable causing applications fail due to not having a proper response for those who didn´t cache answers.

Fraudulent issuance: a compromised TSA may incur in the issuance of incorrect or fraudulent time stamp tokens

A.4 Creation, validation and verification of electronic registered delivery services

Unavailability[29]**:** the dependencies of the service are not available, directly or indirectly, such as:

> **No access to the signature/seal creation and validation and verification services:** The services are not accessible.
>
> **No access to the timestamping service:** The timestamp service is not accessible.
>
> **No access to the certificate validation service:** the validation of certificates service is not accessible.

Inaccurate evidence of delivery: The delivery service produces erroneous evidences due to inaccurate responses by the signing platform.

Incorrect recipient address: Unavailability of the recipient address due to several causes.

Inaccurate storage: the evidence is not maintained properly or not even stored.

Undelivered evidence: The request has been delivered correctly, the evidences generated and signed but the sender is unable to check the successful conclusion of the service because he is unable to receive the evidence due to several reasons, for example, in a REM solution, the sender email box is full and can´t receive any email.

A.5 Creation of electronic signatures/seals service

Incorrect response from the platform when creating an electronic signature/seal: Although the signature/seal creation platform can access to the different platforms needed, the response received by these platforms is inaccurate and then the signature/seal can´t be created.

Incorrect creation of signatures/seals: Due to the lack of updated signature formats the platform creates signatures which are not in line with the standards.

Unavailability[29]**:** The service can´t provide its functions causing applications to fail

> **No access to the Timestamping service:** The timestamping service is not accessible.

No access to the preservation of electronic signatures/seals service: the preservation service is not accessible.

Long response times: Applications are experiencing delays when interacting with the signature/seal creation platform even if the platform is still creating the signature.

No synchronisation of the signature/seal creation services: The TSP provides multiple signature/seal creation service platforms which are not synchronised, and this creates incorrect configurations and issues when accessing one or each other different platform.

A.6 Validation and verification of signatures/seals service

Incorrect response from the platform when validating a certificate: Although VA and/or TSA are accessible by the signature/seal validation platform, the response received by these platforms is inaccurate (see validation and timestamping services) and then the signature can´t be validated.

Incorrect validation of signatures/seals: Due to the lack of updated signature formats the signing platform creates signatures which are not in line with the standards and can´t be validated properly.

Unavailability[29]: The service can´t provide its functions causing applications to fail

No access to the Timestamping service: The timestamping service is not accessible.

No access to the validation of certificates service: The validation service is not accessible.

No access to the preservation of electronic signatures/seals service: the preservation service is not accessible.

Long response times: Applications are experiencing delays when interacting with the platform even if the platform is still validating the signature.

No synchronisation of the validation services: The TSP provides multiple validations of signatures/seals service platforms which are not synchronised, and this creates incorrect configurations and issues when accessing one or each other different platform.

A.7 Preservation of electronic signatures/seals service

Unauthorised access: An attacker manages to gain access to the data preserved.

Data integrity over the years: The integrity of the information preserved is altered over the years due to different causes (e.g. improper environmental conditions, media obsolescence, purposeful destruction or theft, computer virus, hardware, software or operator error).

Incorrect validation of signatures/seals: Due to the lack of updated signature formats the signing platform creates signatures which are not in line with the standards and can´t be validated properly.

Unavailability[29]: The service can´t provide its functions causing applications to fail

No access to the Timestamping service: The timestamping service is not accessible.

No access to the validation of certificates service: The service is not accessible.

No access to the signatures/seals creation and validation and verification services: The service is not accessible.

Obsolete data formats: The tools which were used to generate the original data become obsolete and not supported by their vendors any more.

C.2 Cross cutting examples/scenarios

• B.1 Authentication service

Online/offline guessing: An attacker performs repeated logon trials by guessing possible values of the token authenticator.

Phishing: A subscriber is lured and tricked into revealing his or her token secret, sensitive personal data or authenticator values.

Pharming: A subscriber is routed to an attacker's website through manipulation of the domain name service or routing tables.

Eavesdropping: An attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the claimant.

Replay: An attacker is able to replay previously captured messages to authenticate as that claimant.

Session hijack: An attacker is able to insert to a successful authentication exchange between the two parties.

Man in the middle: An attacker intercepts and alters the content of the authentication protocol messages.

• B.2 An incident with an impact on platform software

This scenario covers all the possible impact on the software used for a TSP to provide the trust services specified as in eIDAS. It involves possible compromise of the CA, RA, VA, TSA, signing, preservation and delivery software.

• B.3 An incident with an impact on platform hardware

This scenario refers to all issues that can generate a possible compromise of the hardware which supports the software platforms. It involves all hardware failures that affect the assets and thus the services associated with them.

• B.4 Compromise of private keys[30]

The secrecy of the private key is critical for each asymmetric cryptosystem. Any compromise of the private key severely affects the users and the services which depend on this key. Of course, there are different types of compromises with different level of impact. For example, a lost key can be recovered depending on the recovery procedures and/or policies of the issuer/owner, but a stolen key might have a disastrous impact on the services offered.

[30] The impact is not the same for all services e.g. issuance, validation, timestamping, signing,… services, but the compromise of the keys is critical for TSP's business, even if a TSP offers only certificate issuing service or validation service, or more than one services.

B.5 Inadequate use of algorithms

This scenario affects key generation or certificate generation, electronic signature creation, etc. It involves the use of deprecated, weak or obsolete algorithms.

B.6 Unintentional use of certificates for other purposes

A high level of trust is provided through the use of public key certificates. The certificates are based on standards, e.g. X.509, and any unintentional use of the certificates affect the trust between two parties. The unintentional use of the certificates is a significant incident when affecting core services.

B.7 Compromise on key devices

For example HSM (Hardware Security Model), smartcards, USB tokens and FIDO token. It implies the loss, robbery, blocking, etc. of the device and also the unavailability to use/recover/revoke the cryptographic material.

B.8 Archive issues

According to eIDAS, the archival assets cover all aspects related to documentation and the log files of all tasks performed by the TSPs.

Some examples of these issues can be found using an accountability or traceability of the logs, such as:

- Modification of logs related to the life-cycle of certificates
- Stop logging requests relating to revocation
- Stop logging of archive security events as start-up, shutdown, system crashes, hardware failures, multiple login attempts, etc.

Personal data compromise is also considered under this scenario.

B.9 Networking issues

Unavailability[29] of networking infrastructure including hardware (firewalls, routers, cables …) as well as software (the firmware managing the devices).

B.10 Compromise of supporting tools

Refers to all other than B2 and B3 platforms, hardware and software, which support eIDAS services e.g. databases, LDAP server, the web servers, applications, etc.

C.3 Service specific examples

This table shows the possible specific impacts for the services listed in eIDAS with examples of the more typical impacts per service.

SERVICE			INCIDENT SCENARIO	SEVERITY[31]	THREATS[32]
A.1. Creation of certificates					
	A.1.1 Registration process				
		A.1.1.1 Registration			
			Impersonation	3	A.2.1, A.3.14
			Repudiation	3	A.2.1, A.3.14
		A.1.1.2 Issuance			
			Disclosure	3	A.2.1, A.3.14
			Tampering	3	A.2.1, A.3.10, A.3.14
			Unauthorised issuance	3	A.2.1, A.3.14
	A.1.2 Tokens				
			Theft	3	A.2.1, A.3.3, A.3.4, A.3.14
			Discovery	3	A.2.1, A.2.4
			Duplication	3	A.2.1, A.2.4, A.3.3, A.3.4
			Eavesdropping	3	A.2.4, A.3.11
			Offline cracking	3	A.2.4, A.3.4
			Phishing or farming	3	A.2.4, A.3.4
			Social engineering	3	A.2.4, A.3.2, A.3.4, A.3.7
	A.1.3 Token and credential management				
		A.1.3.1 Credential Storage			
			Disclosure	3	A.2.1, A.2.2, A.2.4, A.2.5, A.3.2, A.3.3, A.3.4, A.3.6, A.3.14
			Tampering	3	A.2.1, A.2.2, A.2.4, A.2.5, A.3.2, A.3.4,

[31] As defined in section 3.2.1.

[32] As listed in Annex A.

					A.3.6, A.3.10, A.3.14
			Duplication	3	A.2.1, A.2.4, A.3.3, A.3.4
		A.1.3.2 Verification services			
			Disclosure	3	A.2.1, A.2.2, A.2.4, A.2.5, A.3.2, A.3.3, A.3.4, A.3.6, A.3.14
			Tampering	3	A.2.1, A.2.2, A.2.4, A.2.5, A.3.2, A.3.4, A.3.6, A.3.10, A.3.14
			Unavailability	3	A.2.2, A.2.4, A.2.5, A.3.1, A.3.2, A.3.3, A.3.4, A.3.6, A.3.7, A.3.8, A.3.9, A.3.13, A.3.14
		A.1.3.3 Issuance/renewal/re-issuance services			
			Disclosure	3	A.2.1, A.2.2, A.2.4, A.2.5, A.3.2, A.3.3, A.3.4, A.3.6, A.3.14
			Tampering	3	A.2.1, A.2.2, A.2.4, A.2.5, A.3.2, A.3.4, A.3.6, A.3.10, A.3.14
			Unauthorised access	3	A.2.1, A.2.2, A.2.4, A.2.5, A.3.2, A.3.3, A.3.4, A.3.6, A.3.9, A.3.10, A.3.14
			Weak protocol	3	A.2.2, A.2.4, A.2.5, A.3.1, A.3.2, A.3.4, A.3.7, A.3.9
		A.1.3.4 Revocation/destruction services			

			Delays	3	A.2.2, A.2.4, A.2.5, A.3.2, A.3.4, A.3.7, A.3.9
			Use after decommis-sioning	3	A.2.1, A.2.4, A.3.3
A.2 Validation and verification of certificates					
	Incorrect answer			3	A.2.2, A.2.4, A.2.5, A.3.14
	Inconsistency be-tween CRL/OCSP			4	A.2.2, A.2.4, A.2.5, A.3.7, A.3.9, A.3.14
	Reply attack			4	A.2.2, A.2.4, A.2.5, A.3.7, A.3.4, A.3.9, A.3.14
	Unavailability			4	A.2.2, A.2.4, A.2.5, A.3.1, A.3.2, A.3.3, A.3.4, A.3.6, A.3.7, A.3.8, A.3.9, A.3.13, A.3.14
A.3 Creation, validation and verification of Timestamps					
	No synchroniza-tion			3	A.2.2, A.2.4, A.2.5, A.3.1, A.3.2, A.3.6, A.3.7, A.3.9, A.3.14
	Clock skew			2	A.2.2, A.2.4, A.2.5, A.3.1, A.3.2, A.3.6, A.3.7, A.3.9, A.3.14
	Local timestamp-ing			2	A.2.1, A.2.2, A.2.4, A.3.2, A.3.6, A.3.7, A.3.9, A.3.14
	Unavailability			4	A.2.2, A.2.4, A.2.5, A.3.1, A.3.2, A.3.3, A.3.4, A.3.6, A.3.7, A.3.8, A.3.9, A.3.13, A.3.14

	Fraudulent issuance			4	A.2.1, A.2.2, A.2.4, A.3.2, A.3.6, A.3.7, A.3.9, A.3.14
A.4 Creation, validation and verification of electronic Registered Delivery services					
	Unavailability			3	A.2.2, A.2.4, A.2.5, A.3.1, A.3.2, A.3.3, A.3.4, A.3.6, A.3.7, A.3.8, A.3.9, A.3.13, A.3.14
	Incorrect evidences			2	A.2.2, A.2.4, A.2.5, A.3.2, A.3.4, A.3.7, A.3.9, A.3.14
	Incorrect recipient address			2	A.2.2, A.2.4, A.2.5, A.3.2, A.3.4, A.3.7, A.3.9, A.3.14
	Inaccurate storage			2	A.2.1, A.2.2, A.2.5, A.3.2, A.3.3, A.3.4, A.3.7, A.3.9, A.3.13
	Undelivered evidence			2	A.2.2, A.2.4, A.2.5, A.3.2, A.3.4, A.3.7, A.3.9, A.3.14
A.5 Signature/seal creation service					
	Unavailability			3	A.2.2, A.2.4, A.2.5, A.3.1, A.3.2, A.3.3, A.3.4, A.3.6, A.3.7, A.3.8, A.3.9, A.3.13, A.3.14
	Incorrect response			3	A.2.2, A.2.4, A.2.5, A.3.2, A.3.4, A.3.7, A.3.9, A.3.14
	Incorrect creation of signatures			4	A.2.2, A.2.4, A.2.5, A.3.2,

					A.3.4, A.3.7, A.3.9, A.3.14
	Long response times			2	A.2.2, A.2.4, A.2.5, A.3.1, A.3.2, A.3.3, A.3.4, A.3.6, A.3.7, A.3.8, A.3.9, A.3.13, A.3.14
	No synchronisation			3	A.2.2, A.2.4, A.2.5, A.3.1, A.3.2, A.3.6, A.3.7, A.3.9, A.3.14
A.6 Signature/seal validation and verification service					
	Unavailability			3	A.2.2, A.2.4, A.2.5, A.3.1, A.3.2, A.3.3, A.3.4, A.3.6, A.3.7, A.3.8, A.3.9, A.3.13, A.3.14
	Incorrect response			3	A.2.2, A.2.4, A.2.5, A.3.2, A.3.4, A.3.7, A.3.9, A.3.14
	Incorrect validation of signatures			4	A.2.2, A.2.4, A.2.5, A.3.2, A.3.4, A.3.7, A.3.9, A.3.14
	Long response times			2	A.2.2, A.2.4, A.2.5, A.3.1, A.3.2, A.3.3, A.3.4, A.3.6, A.3.7, A.3.8, A.3.9, A.3.13, A.3.14
	No synchronisation			3	A.2.2, A.2.4, A.2.5, A.3.1, A.3.2, A.3.6, A.3.7, A.3.9, A.3.14
A.7 Preservation service					
	Unavailability			3	A.2.2, A.2.4, A.2.5, A.3.1, A.3.2, A.3.3, A.3.4, A.3.6, A.3.7, A.3.8,

					A.3.9, A.3.13, A.3.14
	Access rights			3	A.2.1, A.2.2, A.2.4, A.2.5, A.3.10, A.3.11, A.3.12, A.3.14
	Data integrity			3	A.2.1, A.2.2, A.2.4, A.2.5, A.3.2, A.3.6, A.3.7, A.3.8, A.3.9, A.3.14
	Incorrect validation of signatures			4	A.2.2, A.2.4, A.2.5, A.3.2, A.3.4, A.3.7, A.3.9, A.3.14
	Data formats			3	A.2.1, A.2.2, A.2.4, A.2.5, A.3.2, A.3.6, A.3.7, A.3.8, A.3.9, A.3.14

C.4 Generic examples

IMPACTS	SEVERITY	THREATS
B.1 Authentication		
Online/offline guessing	3	A.2.4
Phishing or pharming	3	A.2.1, A.2.2, A.2.4, A.3.4
Eavesdropping	3	A.2.4, A.3.11
Replay	3	A.2.4
Session hijack	3	A.2.4
Man in the middle	3	A.2.4
B.2 Impact on platform software	3	A.2.1, A.2.2, A.2.4, A.3.2, A.3.4, A.3.7, A.3.9, A.3.15
B.3 Impact on platform hardware	2	A.2.1, A.2.2, A.2.3, A.2.4, A.3.3, A.3.5, A.3.6, A.3.8, A.3.15
B.4 Compromise of private keys	5	A.2.1, A.2.2, A.2.3, A.2.4, A.3.3, A.3.4, A.3.5, A.3.6, A.3.8, A.3.9, A.3.14, A.3.15
B.5 Inadequate use of algorithms	3	A.2.1, A.2.2, A.2.4, A.2.5, A.3.4, A.3.7, A.3.9, A.3.12, A.3.14
B.6 Unintentional use of certificates for other purposes	4	A.2.1, A.2.2, A.2.4, A.3.2, A.3.4, A.3.7, A.3.9, A.3.14
B.7 Compromise on key devices	5	A.2.1, A.2.2, A.2.3, A.2.4, A.2.5, A.3.2, A.3.3, A.3.4, A.3.5, A.3.6, A.3.7, A.3.8, A.3.9, A.3.10, A.3.11, A.3.12, A.3.14, A.3.15

B.8 Archive issues	3	A.2.1, A.2.2, A.2.3, A.2.4, A.2.5, A.3.1, A.3.2, A.3.3, A.3.4, A.3.5, A.3.6, A.3.7, A.3.8, A.3.9, A.3.10, A.3.13, A.3.14
B.9 Network issues	3	A.2.1, A.2.2, A.2.3, A.2.4, A.2.5, A.3.1, A.3.4, A.3.5, A.3.6, A.3.8, A.3.13, A.3.15
B.10 Compromise of supporting tools	2	A.2.1, A.2.2, A.2.3, A.2.4, A.2.5, A.3.2, A.3.3, A.3.4, A.3.5, A.3.6, A.3.7, A.3.8, A.3.9, A.3.10, A.3.11, A.3.12, A.3.14, A.3.15

Annex D: Services defined at EIDAS regulation and relevant assets used to offer these services

D.1 Assets and the eIDAS services.

Creation of (qualified) certificates (including renewal and revocation)

CA PLATFORM	HARDWARE	CA ROOT(S) SERVER(S)
		QSCD: HSMs CA root(s) and subCA(s)
		Other CA equipment
		SubCA(s) (issuing CA) server
	Software	CA root(s) certificate(s)
		CA software
		subCA(s) certificate(s)
		QSCD: HSM storing subCA(s) private key(s) and certificate(s)
		QSCD: HSM CA root(s) storing CA root private key
		CARL(s)
		CRL
VA platform	Hardware	VA server(s)
		QSCD: HSM(s) for VA(s)
		Other VA equipment
	Software	VA software
		VA certificate(s)
		QSCD: HSM storing VA(s) private key(s) and certificate(s)
RA platform	Hardware	RA equipment
		RA operator devices
	Software	RA software
		RA operator credentials
TSA platform	Hardware	TSA server(s)
		QSCD: HSM(s) for TSA(s)
		Other TSA equipment
	Software	TSA software
		TSA certificate(s)

		QSCD: HSM storing TSA(s) private key(s) and certificate(s)
Documentation		Documentation: issuance policies and practices. Evidences.
Network platform		Communication lines, firewall, …

When issued "locally", also

SUBJECT DEVICE	HARDWARE	QSCD: SUBJECT TOKEN
	Software	Subject certificate
		Subject keys

When issued "remotely"

REMOTE SUBJECT DEVICE	HARDWARE	QSCD: HSM OR SERVER
	Software	keys and certificates

Validation and verification of (qualified) certificates

CA PLATFORM	HARDWARE	CA ROOT(S) SERVER(S)
		QSCD: HSMs CA root(s) and subCA(s)
		Other CA equipment
		SubCA(s) (issuing CA) server
	Software	CA root(s) certificate(s)
		CA software
		subCA(s) certificate(s)
		QSCD: HSM storing subCA(s) private key(s) and certificate(s)
		QSCD: HSM CA root(s) storing CA root private key
		CARL(s), CRL(s)
VA platform	Hardware	VA server(s)
		QSCD: HSM(s) for VA(s)
		Other VA equipment
	Software	VA software
		VA certificate(s)

		QSCD: HSM storing VA(s) private key(s) and certificate(s)
Network platform		Communication lines, firewall …
Documentation		Documentation: validation policies and practices. Evidences

Creation, validation and verification of electronic timestamps service

TSA PLATFORM	HARDWARE	TSA SERVER(S)
		QSCD: HSM(s) for TSA(s)
		Other TSA equipment
	Software	TSA software
		TSA certificate(s)
		QSCD: HSM storing TSA(s) private key(s) and certificate(s)
Network platform		Communication lines, firewall, …
Documentation		Documentation: policies and practices. Evidences

Creation of electronic signatures/seals service

CREATION OF SIGNATURES/SEALS PLATFORM	HARDWARE	SERVER FOR THE CREATION AND VALIDATION OF SIGNATURES/SEALS PLATFORM
		QSCD: HSM for the platform
	Software	Signing and validation software
		Signing tool certificate(s)
		QSCD: HSM storing signing keys and certificates
CA platform	Software	CARL(s), CRL(s)
VA platform	Hardware	VA server(s)
		QSCD: HSM(s) for VA(s)
		Other VA equipment
	Software	VA software
		VA certificate(s)
		QSCD: HSM storing VA(s) private key(s) and certificate(s)

TSA platform	Hardware	TSA server(s)
		QSCD: HSM(s) for TSA(s)
		Other TSA equipment
	Software	TSA software
		TSA certificate(s)
		QSCD: HSM storing TSA(s) private key(s) and certificate(s)
Network platform		Communication lines, firewall, …
Documentation		Documentation: signature/seals creation policies and practices.

For local signing

The document is stored and kept locally

SUBJECT DEVICE FOR LOCAL SIGNING	HARDWARE	QSCD
		Smartcard reader, USB port…
	Software	Subject certificate
		Subject keys

For remote signing

SUBJECT DEVICE FOR REMOTE SIGNING	HARDWARE	QSCD
	Software	Keys and certificates

When a document is uploaded to the service and stored there

ARCHIVE	DOCUMENTS UPLOADED AND SIGNED REMOTELY

Validation and verification of electronic signatures/seals service

VALIDATION OF SIGNATURES/SEALS PLATFORM	HARDWARE	SERVER FOR THE VALIDATION OF SIGNATURES/SEALS PLATFORM
		QSCD: HSM for the platform
	Software	Validation software
		Signing tool certificate(s)
		QSCD: HSM storing signing keys and certificates
CA platform	Software	CARL(s), CRL(s)

VA platform	Hardware	VA server(s)
		QSCD: HSM(s) for VA(s)
		Other VA equipment
	Software	VA software
		VA certificate(s)
		QSCD: HSM storing VA(s) private key(s) and certificate(s)
TSA platform	Hardware	TSA server(s)
		QSCD: HSM(s) for TSA(s)
		Other TSA equipment
	Software	TSA software
		TSA certificate(s)
		QSCD: HSM storing TSA(s) private key(s) and certificate(s)
Network platform		Communication lines, firewall, …
Documentation		Documentation: signatures/seals validation policies and practices.

When a document is uploaded to the service and stored there

ARCHIVE	DOCUMENTS UPLOADED AND SIGNED REMOTELY

Preservation of electronic signatures/seals service

PRESERVATION OF SIGNATURES/SEALS PLATFORM	HARDWARE	SERVER(S) FOR THE PRESERVATION PLATFORM
		QSCD: HSM(s) for the platform
	Software	Preservation software
		Preservation tool certificate(s)
		QSCD: HSM(s) storing signing keys and certificates
CA platform	Software	CARL(s), CRL(s)
VA platform	Hardware	VA server(s)

		QSCD: HSM(s) for VA(s)
		Other VA equipment
	Software	VA software
		VA certificate(s)
		QSCD: HSM storing VA(s) private key(s) and certificate(s)
TSA platform	Hardware	TSA server(s)
		QSCD: HSM(s) for TSA(s)
		Other TSA equipment
	Software	TSA software
		TSA certificate(s)
		QSCD: HSM storing TSA(s) private key(s) and certificate(s)
Network platform		Communication lines, firewall, …
Documentation		Documentation: preservation policies and practices. Evidences

When a document is uploaded to the service and stored there

ARCHIVE	DOCUMENTS UPLOADED AND PRESERVED REMOTELY

Creation, validation and verification of electronic registered delivery services

REGISTERED DELIVERY PLATFORM	HARDWARE	SERVER(S) FOR THE REGISTERED DELIVERY PLATFORM
		ASCD: HSM(s) for the platform
	Software	Registered delivery software
		Platform signing certificate(s)
		QSCD: HSM storing signing keys and certificates
CA platform	Software	CRL(s)
VA platform	Hardware	VA server(s)
		QSCD: HSM(s) for VA(s)
		Other VA equipment

	Software	VA software
		VA certificate(s)
		QSCD: HSM storing VA(s) private key(s) and certificate(s)
TSA platform	Hardware	TSA server(s)
		QSCD: HSM(s) for TSA(s)
		Other TSA equipment
	Software	TSA software
		TSA certificate(s)
		QSCD: HSM storing TSA(s) private key(s) and certificate(s)
Network platform		Communication lines, firewall, …
Documentation		Documentation: policies and practices. Evidences

See table 1 for a detailed mapping of the services and the assets.

Table 1: Mapping assets with services

SERVICES / ASSETS		CREATION OF (QUALIFIED) CERTIFICATES	VALIDATION AND VERIFICATIONOF (QUALIFIED) CERTIFICATES	CREATION, VALIDATION AND VERIFICATION OF ELECTRONIC TIME STAMPS	CREATION, VALIDATION AND VERIFICATION OF ELECTRONIC REGISTERED DELIVERY SERVICES	CREATION OF ELECTRONIC SIGNATURES/SEALS	VALIDATION AND VERIFICATION OF ELECTRONIC SIGNATURES/SEALS	PRESERVATION OF ELECTRONIC SIGNATURES/SEALS
CA Platform	*Hardware*							
	CA root(s) server(s)	✓						
	QSCD: HSM CA root(s)	✓	✓					
	SubCA(s) (issuing CA) server	✓	✓					
	Other CA equipment	✓	✓					
	QSCD: HSM SubCA(s)	✓	✓					
	Software							

	QSCD: HSM CA root(s) storing CA root private key	✓	✓					
	CA software	✓	✓					
	CA root(s) certificate(s)	✓						
	subCA(s) certificate	✓	✓					
	QSCD: HSM storing subCA(s) private key(s) and certificate(s)	✓	✓					
	CARL	✓	✓				✓	✓
	CRL	✓	✓		✓		✓	✓
RA platform	*Hardware*							
	RA equipment	✓						
	RA operator devices	✓						
	Software							
	RA software	✓						
	RA operator credentials	✓						
VA platform	*Hardware*							
	VA server(s)	✓	✓		✓		✓	✓
	QSCD: HSM(s) for VA	✓	✓		✓		✓	✓
	Other VA equipment	✓	✓		✓		✓	✓
	Software							
	VA software	✓	✓		✓		✓	✓
	VA certificate(s)	✓	✓		✓		✓	✓
	QSCD: HSM storing VA(s) private key(s) and certificate(s)	✓	✓		✓		✓	✓
TSA platform	*Hardware*							
	TSA server(s)	✓		✓	✓	✓	✓	✓

	QSCD: HSM(s) for TSA	✓		✓	✓	✓	✓	✓
	Other TSA equipment	✓		✓	✓	✓	✓	✓
	Software							
	TSA software	✓		✓	✓	✓	✓	✓
	TSA certificate(s)	✓		✓	✓	✓	✓	✓
	QSCD: HSM storing TSA(s) private key(s) and certificate(s)	✓		✓	✓	✓	✓	✓
Documentation	Documentation	✓	✓	✓	✓	✓	✓	✓
Network platform	Communication lines, firewalls, etc.	✓	✓	✓	✓	✓	✓	✓
Subject device	*Hardware*							
	QSCD: Smartcard, USB token, FIDO, mobile, browser, …	✓				✓		
	Software							
	Subject certificate	✓				✓		
	Subject keys	✓				✓		
Remote subject device	*Hardware*							
	QSCD: HSM or server	✓				✓		
	Software							
	Keys and certificates	✓				✓		
Creation of signatures/seals platform	*Hardware*							
	Server(s) for the platform					✓		
	QSCD: HSM(s) for the platform					✓		
	Software							
	QSCD: HSM(s) storing keys					✓		

	and certificates							
	Signature creation software					✓		
	Platform certificates					✓		
Validation of signatures/seals platform	*Hardware*							
	Server(s) for the platform						✓	
	QSCD: HSM(s) for the platform						✓	
	Software							
	QSCD: HSM(s) storing keys and certificates						✓	
	Registered delivery software						✓	
	Platform certificates						✓	
Subject device for local signing	Smartcard reader, USB port, …					✓		
Documentation uploaded	Documents signed remotely					✓	✓	
Preservation of signatures/seals platform	*Hardware*							
	Server(s) for the platform							✓
	QSCD: HSM(s) for the platform							✓
	Software							
	QSCD: HSM(s) storing keys and certificates							✓
	Preservation software							✓

	Platform certificates							✓
Documentation uploaded	Documents preserved remotely							✓
Registered delivery platform	*Hardware*							
	Server(s) for the platform				✓			
	QSCD: HSM(s) for the platform				✓			
	Software							
	QSCD: HSM(s) storing keys and certificates				✓			
	Registered delivery software				✓			
	Platform certificates				✓			

D.2 Assets assigned impact values according to the eIDAS mentioned services

The following table shows the corresponding impact values considered for the assets taking into account the impact regarding the service and the assets affected as they have different risks associated.

This table shows the impact of having compromised one of the three basic security principles (Confidentiality, Integrity, Availability) for each service and the associated assets.

Integrity is considered as the most critical vector for all services.

Note: the NA (Not Applicable) is used basically for integrity and confidentiality vectors related to the hardware assets as they can´t be measured except those related to the network platform and HSMs.

Table 2: Impact assessment of assets relevant to eIDAS services

SERVICES	ASSETS			AVAILABILITY	INTEGRITY	CONFIDENTIALITY
Creation of (qualified) certificates	CA Platform	Hardware	CA root(s) server(s)	High	NA	NA
			QSCD: HSM CA root(s)	High	NA	NA
			SubCA(s) (issuing CA) server	High	NA	NA
			Other CA equipment	High	NA	NA

			QSCD: HSM subCA(s)	High	NA	NA
		Software	CA root(s) certificate(s)	Medium	High	Low
			QSCD: HSM CA root(s) storing CA root private key	High	High	High
			subCA(s) certificate	Medium	High	Low
			QSCD: HSM storing subCA(s) private key(s) and certificate(s)	High	High	High
			CARL	Medium	Medium	Low
			CRL	Medium	Medium	Low
			CA software	Medium	Medium	Medium
	RA platform	Hardware	RA equipment	High	NA	NA
			RA operator devices	High	NA	NA
		Software	RA software	Medium	Medium	Medium
			RA operator credentials	Medium	Medium	Low
	VA platform	Hardware	VA server(s)	High	NA	NA
			QSCD: HSM(s) for VA(s)	High	NA	NA
			Other VA equipment	High	NA	NA
		Software	VA software	Medium	High	Medium
			VA certificate(s)	Medium	High	Low
			QSCD: HSM storing VA(s) private key(s) and certificate(s)	High	High	High
	Procedures		Documentation	Medium	Medium	Medium
	Network platform		Communication lines, firewalls, etc.	Medium	Medium	Medium
	Subject device	Hardware	QSCD: Smartcard, USB token, FIDO, mobile, browser,…	High	NA	NA
		Software	Subject certificate	Medium	High	Medium
			Subject keys	High	High	High
	Remote subject device	Hardware	QSCD: HSM or server	High	High	High
		Software	keys and certificates	High	High	High
	TSA platform	Hardware	TSA server(s)	High	NA	NA
			QSCD: HSM(s) for TSA(s)	High	NA	NA

			Other TSA equipment	High	NA	NA
		Software	TSA software	Medium	High	Medium
			TSA certificate(s)	Medium	High	Low
			QSCD: HSM storing TSA(s) private key(s) and certificate(s)	High	High	High
Validation and verification of (qualified) certificates	CA platform	Hardware	CA root(s) server(s)	High	NA	NA
			QSCD: HSM CA root(s)	High	NA	NA
			SubCA(s) (issuing CA) server	High	NA	NA
			Other CA equipment	High	NA	NA
			QSCD: HSM subCA(s)	High	NA	NA
		Software	QSCD: HSM storing subCA(s) private key(s) and certificate(s)	High	High	High
			CA software	Medium	High	Medium
			CA root(s) certificate(s)	Medium	High	Low
			QSCD: HSM CA root(s) storing CA root private key	High	High	High
			subCA(s) certificate	Medium	High	Low
			CARL	High	High	Low
			CRL	High	High	Low
	VA platform	Hardware	VA server(s)	High	NA	NA
			QSCD: HSM(s) for VA(s)	High	NA	NA
			Other VA equipment	High	NA	NA
		Software	VA software	Medium	High	Medium
			VA certificate(s)	Medium	High	Low
			QSCD: HSM storing VA(s) private key(s) and certificate(s)	High	High	High
	Procedures		Documentation	Medium	Medium	Medium
	Network platform		Communication lines, firewalls, etc.	High	High	High

Electronic timestamps	TSA platform	Hardware	TSA server(s)	High	NA	NA
			QSCD: HSM(s) for TSA(s)	High	NA	NA
			Other TSA equipment	High	NA	NA
		Software	TSA software	Medium	High	Medium
			TSA certificate(s)	Medium	High	Low
			QSCD: HSM storing TSA(s) private key(s) and certificate(s)	High	High	High
	Procedures		Documentation	Medium	Medium	Medium
	Network platform		Communication lines, firewalls, etc.	High	High	High
Electronic registered delivery	CA platform	Software	CRL	Medium	Medium	Low
	VA platform	Hardware	VA server(s)	High	NA	NA
			QSCD: HSM(s) for VA(s)	High	NA	NA
			Other VA equipment	High	NA	NA
		Software	VA software	Medium	High	Medium
			VA certificate(s)	Medium	High	Low
			QSCD: HSM storing VA(s) private key(s) and certificate(s)	High	High	High
	TSA platform	Hardware	TSA server(s)	High	NA	NA
			QSCD: HSM(s) for TSA(s)	High	NA	NA
			Other TSA equipment	High	NA	NA
		Software	TSA software	Medium	High	Medium
			TSA certificate(s)	Medium	High	Low
			QSCD: HSM storing TSA(s) private key(s) and certificate(s)	High	High	High
	Procedures		Documentation	Medium	Medium	Medium
	Network platform		Communication lines, firewalls, etc.	Medium	Medium	Medium
	Registered delivery platform	Hardware	Platform server(s)	High	NA	NA
			QSCD: HSM(s) for the platform	High	NA	NA
		Software	Registered delivery software	Medium	Medium	Medium

			Platform signing certificates	Medium	High	Low
			QSCD: HSM storing platform private key(s) and certificate(s)	High	High	High
creation of electronic signatures/seals	TSA platform	Hardware	TSA server(s)	High	NA	NA
			QSCD: HSM(s) for TSA(s)	High	NA	NA
			Other TSA equipment	High	NA	NA
		Software	TSA software	Medium	High	Medium
			TSA certificate(s)	Medium	High	Low
			QSCD: HSM storing TSA(s) private key(s) and certificate(s)	High	High	High
	Procedures		Documentation	Medium	Medium	Medium
	Network platform		Communication lines, firewalls, etc.	High	High	High
	Subject device	Hardware	QSCD: Smartcard, USB token,…	High	NA	NA
		Software	Subject certificate	Medium	High	Medium
			Subject keys	High	High	High
	Remote subject device	Hardware	QSCD:HSM or server	High	High	High
		Software	Keys and certificates	High	High	High
	Creation of signatures/seals platform	Hardware	Platform server(s)	High	NA	NA
			QSCD: HSM(s) for the platform	High	NA	NA
		Software	Signature creation software	Medium	High	Medium
			Platform signing certificates	Medium	High	Low
			QSCD: HSM storing platform private key(s) and certificate(s)	High	High	High
	Subject device for local signing	Hardware	Smartcard reader, USB port, …	Medium	High	High
	Documentation uploaded		Documents signed remotely	Medium	Medium	Medium

Validation and verification of electronic signatures/seals	CA platform	Software	CARL	High	High	Low
			CRL	High	High	Low
	VA platform	Hardware	VA server(s)	High	NA	NA
			QSCD: HSM(s) for VA(s)	High	NA	NA
			Other VA equipment	High	NA	NA
		Software	VA software	Medium	High	Medium
			VA certificate(s)	High	High	Low
			QSCD: HSM storing VA(s) private key(s) and certificate(s)	High	High	High
	TSA platform	Hardware	TSA server(s)	High	NA	NA
			QSCD: HSM(s) for TSA(s)	High	NA	NA
			Other TSA equipment	High	NA	NA
		Software	TSA software	Medium	High	Medium
			TSA certificate(s)	High	High	Low
			QSCD: HSM storing TSA(s) private key(s) and certificate(s)	High	High	High
	Procedures		Documentation	Medium	Medium	Medium
	Network platform		Communication lines, firewalls, etc.	High	High	High
	Validation of signatures/seals platform	Hardware	Platform server(s)	High	NA	NA
			QSCD: HSM(s) for the platform	High	NA	NA
		Software	Signature/seals validation software	Medium	High	Medium
			Platform signing certificates	Medium	High	Low
			QSCD: HSM storing platform private key(s) and certificate(s)	High	High	High
	Documentation uploaded		Documents signed remotely	Medium	Medium	Medium

Preservation of electronic signatures/seals	CA platform	Software	CARL	High	High	Low
			CRL	High	High	Low
	VA platform	Hardware	VA server(s)	High	NA	NA
			QSCD: HSM(s) for VA(s)	High	NA	NA
			Other VA equipment	High	NA	NA
		Software	VA software	Medium	High	Medium
			VA certificate(s)	Medium	High	Low
			QSCD: HSM storing VA(s) private key(s) and certificate(s)	High	High	High
	TSA platform	Hardware	TSA server(s)	High	NA	NA
			QSCD: HSM(s) for TSA(s)	High	NA	NA
			Other TSA equipment	High	NA	NA
		Software	TSA software	Medium	High	Medium
			TSA certificate(s)	Medium	High	Low
			QSCD: HSM storing TSA(s) private key(s) and certificate(s)	High	High	High
	Procedures		Documentation	Medium	Medium	Medium
	Network platform		Communication lines, firewalls, etc.	High	High	High
	Preservation platform	Hardware	Platform server(s)	High	NA	NA
			QSCD: HSM(s) for the platform	High	NA	NA
		Software	Preservation software	Medium	High	Medium
			Platform signing certificates	Medium	High	Low
			QSCD: HSM storing platform private key(s) and certificate(s)	High	High	High
	Documentation uploaded		Documents preserved remotely	Medium	Medium	Medium

D.3 Examples

These examples affect more than one trust service provided by a TSP and have a significant impact on the users affected; even this can vary depending on the nature of the TSP and the services it provides.

The assessment of the incident equals the security concept affected at the highest level.

The following is a list of examples with high total impact on the three security concepts (C,I,A).

- ### Issues with the private key of the TSP services

This is an example of a security incident which involves the loss of a private key of a service and might have an impact on one or various trust services e.g. the Certification Authority, the time stamping authority, etc.

The cause might be for example the loss or unavailability of the private key (which can or can´t be regenerated), during an update/migration in the hardware or software platform (that affects the services (it can affect the CA root or subordinates, the TSA, the signing service, etc.)

Other typical issue is the control by an attacker over the private key of one or more of the trust services during an attack against the TSP, or the stealing of the private key, etc. Loss of control of the private key makes a service distrustful and might lead the TSP even to bankruptcy.

Services and platforms affected

eIDAS services: issuance of certificates, validation of certificates, electronic timestamping, creation and validation of signatures/seals, electronic registered delivery and/or preservation.

Platforms: main primary and supporting hardware and software platforms.

Security principles: availability, confidentiality and integrity.

- ### Issues with the certificates of the TSP services

This is a different version of the above example but the attacker does not control the keys. Therefore, the impact, even still high, has different implications although the services and platforms affected remain the same.

Services and platforms affected

eIDAS services: issuance and validation of certificates, electronic timestamping, creation and validation of signatures/seals, electronic registered delivery and/or preservation.

Platforms: main primary and supporting hardware and software platforms

Security principles: availability, confidentiality and integrity

- ### General failure on communications

It concerns outages in the communications, the networks and all the devices used/affected in the system. There are different issues depending on the affected services but all of them can be affected and cause a high impact on the TSPs services.

Examples of these failures can either affect a specific service or all the services provided by the TSP.

Services and platforms affected

eIDAS services: issuance and validation of certificates, electronic timestamping, creation and validation of signatures/seals, electronic registered delivery and/or preservation.

Platforms: main primary and supporting hardware and software platforms

Security principles: availability

- Subject keys/certificates

This is an example of keys or certificates affected due to a failure of the different services provided by the TSP.

The compromise of a key is of a higher importance because one might take the control over the operations. However, the compromise of a certificate, being quite important as well, is less significant.

Services and platforms affected

eIDAS services: issuance and validation of certificates, electronic timestamping, creation and validation of signatures/seals, electronic registered delivery and/or preservation.

Platforms: main primary and supporting software platforms

Security principles: availability, integrity and confidentiality

- QSCD: Subject devices

This example involves the compromise or loss of the keys' and certificates' storage devices.

It can affect personal devices (smartcards, USB tokens (FIDO), mobile phones …) or remote devices managed by a TSP or not such as HSMs.

Services and platforms affected

eIDAS services: issuance of certificates, electronic timestamping, creation and validation of signatures/seals, electronic registered delivery and/or preservation.

Platforms: main primary and supporting software platforms

Security principles: availability, integrity and confidentiality

- Validation of certificates services

This example involves the different methods to validate a certificate, such as the OCSP (Online Certificate Status Protocol) and the CRL (Certificate Revocation List) valid for end user certificate or CA certificates.

It can affect all the applications that rely on these services providing wrong answers (incorrect, erroneous, different or none) causing applications to fail due to accepting those wrong responses.

Services and platforms affected

eIDAS services: validation of certificates

Platforms: main primary and supporting software platforms

Security principles: availability, integrity and confidentiality

D.4 Specific examples

This list shows other specific examples based on one single security concept and including medium and/or low levels

- Availability
  - Errors when accessing to the TSP website to read/download/access the CPS and the website is not up and running due to changes in the webserver OS, or not applying patches, etc. Severity: Medium
  - Errors in the supporting assets, for example the webserver or application servers and the supporting applications can´t work properly. Severity: Medium
  - When patching the DB some errors can occur an affect the normal processing. Severity: Low
  - When restarting services not all of them work properly. Severity: Medium
  - When updating the Java virtual machine in the RA, some Java applications (applets) can´t be executed due to an incompatibility of the Java versions. Severity: Low
  - Running long term commands in HSMs making them consume all the memory and not be able to have enough capacity for the rest of the operations. Severity: Low
  - Filesystem filled up making applications fail. Severity: Low
- Integrity
  - Error when trespassing data from development to production affecting the integrity of the data. Severity: Medium
  - Not publication of the CPS/CP in the website remaining pending. Severity: Low
  - Removing files from the RA. Severity: Low
- Confidentiality
  - Error in the RA system allowing for example an access to a sheet with the pin/puk of the certificates. Severity: Low
  - The IPS detects an attack trying to download the /etc/passwd from the application servers. Severity: Medium

Annex E: Informing the public and/or victims

Article 19 imposes an obligation to TSPs to notify customers affected to whom the trusted service has been provided and the public in case that disclosure of the breach of security or loss of integrity is in the public interest. Each TSP must be prepared to respond to a possible breach of security of the services it provides. Apart from the technical skills, the TSP should have the right communication capabilities in order to inform the involved, in the breach of security, parties. For this reason it must prepare a communication plan emphasizing on: a) internal communications, b) communication with supervisory bodies and law enforcement authorities where relevant and c) the affected individuals. The aim of this communication plan is to minimize the impact of the breach on the individuals and on the reputation of the organization. The TSP should exercise the effectiveness of its communication plan from time to time and keep it up to date.

E.1 Informing customers affected

It is particularly relevant to assess the consequences of security incidents on the customers affected to determine whether or not the breach of security should be notified to individuals. The harm that an individual may suffer as a result of the breach of security has to be first determined by the TSP and then he has to send a notification to the individuals affected. ENISA has published a report which provides useful tips when notifying individuals[33] in case of a data breach. In addition, the Article 29 Working Party has issued an opinion which provides guidance to controllers (the TSPs) in order to help them to decide whether to notify data subjects (individuals) in case of a "personal data breach"[34]. TSPs might get inspiration from these documents when it comes to notify the customers affected by a security breach.

E.2 Informing the public

TSPs will likely provide this notification in the form of a press release to appropriate information security media outlets. Like individual notice, this media notification should be provided without unreasonable delay and might include the same information required for the individual notice (see previous paragraph).

Spokesperson(s) need to be prepared to respond to media inquiries. The plan should anticipate the need to provide access to services and information to help those impacted. In addition to email, written correspondence, and web site postings, companies should monitor the use of social networking sites such as Facebook, Twitter and blogs for consumer sentiment. Companies may consider using them for controlled, scripted and moderated postings, but need to be prepared for a debate or dialog, which may follow.

The TSP might also consider to create a set of pre-approved web pages and templates staged, phone scripts prepared and frequently asked questions (FAQs) drafted and ready for posting. TSP personel needs to anticipate call volumes and steps to minimize hold times following a significant breach of security and to consider the need of multi-lingual support.

[33] ENISA report on 'Recommendations on technical implementation guidelines of Article 4[33]', pp. 28-36, available at https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech

[34] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

Annex F: Informing other authorities

Notification to other national authorities is an informal, ad hoc process, which happens largely at the discretion of supervisory bodies. Depending on the setting, supervisory bodies may use a template, for example, the template for annual summary reporting (see 4.1).

References

Legislation

[1] Article 13a of the Framework directive of the EU legislative framework on electronic communications: http://ec.europa.eu/information_society/policy/ecomm/doc/140framework.pdf

[2] Article 4 of the e-Privacy directive, part of the EU legislative framework on electronic communications: http://ec.europa.eu/information_society/policy/ecomm/doc/24eprivacy.pdf

[3] The electronic communications regulatory framework (incorporating the telecom reform): http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf

[4] Article 15 of the Regulation on electronic identification and trust services for electronic transactions in the internal market: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm

[5] Article 30, 31 and 32 of the proposed Data Protection regulation: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf The regulation is part of a wider reform of the data protection framework: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[6] Roadmap for a proposal on a European strategy for internet security: http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf

[7] The speech of EU Commissioner Neelie Kroes on the EU strategy for internet security: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/204&format=HTML&aged=0&language=EN&guiLanguage=en

[8] The speech of EU Commissioner Cecilia Malmström on the EU Cyber security strategy: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/315

Related ENISA papers

[1] ENISA's Article 13a Guidelines on Incident reporting and Minimum security measures.

[2] ENISA's Recommendations for the technical implementation of Article 4.

[3] ENISA's 2009 paper on incident reporting shows an overview of the situation 3 years ago.

[4] ENISA's 2011 paper on data breach reporting across the EU shows an overview of the different national approaches to personal data breach notifications.

[5] ENISA's paper on National Cyber Security Strategies shows commonalities and differences between national cyber security strategies across the EU Legislation.

[6] ENISA's report on Security framework - Guidelines for trust services providers – Part 1.

[7] ENISA's report on TSP Risk assessment - Guidelines for trust services providers – Part 2.[8] ENISA's report on Mitigating the impact of security incidents - Guidelines for trust services providers – Part 3.

ENISA

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

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Athens, Greece

TP-05-16-011-EN-N

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

ISBN: 978-92-9204-180-9
doi: 10.2824/67244