Annual Incident Analysis Report for the Trust Service Providers

Analysis of Article 19a annual incident reports under eIDAS - 2016

OCTOBER 2017

About ENISA

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

Contact

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

Acknowledgements

For the completion of this report ENISA has worked closely with a group of experts from Supervisory Bodies and ministries from across Europe. Listing the organizations (in no particular order): ILNAS (LU), CERT LV(LV), Bundesnetzagentur (DE), MCA (MT), NKOM (NO), ANSSI (FR), RTR (AT), Ministry of Digital Affairs (PL), GNS (PT), Agency for Digitisation (DK), Radiocommunications Agency (NL), FPS Economy (BE), EETT (GR), Communications Regulatory Authority (LT), FICORA (FI), CRC (BG), Agenzia per l'Italia Digitale (IT), National Media and Infocommucations Authority (HU), ICO (UK), Ministry of Communications and Informational Society (RO), National Security Authority (SK), Ministry of Industry and Tourism (ES), Swedish Post and Telecom Authority (SE), Ministry of Economy, Entrepreneurship and Crafts (HR), Ministry of the Interior (CZ), RIA (EE), DCCAE (IE), Ministry of Transport, Communications and Works (CY), Ministry of Public Administration, Information Society Directorate (SI)

ISBN: 978-92-9204-234-9, DOI: 10.2824/988312

Executive Summary

This report provides an analysis and evaluation of the incident reporting procedure in the EU under the Article 19 of the eIDAS Regulation (2014/910/EC). Considering the fact that only the second half of 2016 was applicable and moreover that this was the first time for Supervisory Bodies to perform this exercise, a low volume of reported incidents was expected.

In reality, only one incident was notified to ENISA. Thus, more emphasis has been given to the analysis of the incident reporting procedure per se, in an effort to highlight its peculiarities. It came as no surprise that the root cause was a system failure. ENISA's corresponding analysis about significant outage incidents in the European electronic communications sector has identified that system failures are the dominant root cause of incidents for the sixth year in a row[1].

A detailed view on the progress of the reporting procedure explains the minor number of incidents. Legislative delays, incidents slightly below the EU thresholds and incidents reportable in national level but not significant in the EU scale, are the main factors that describe this situation.

In conclusion, this first year's incident reporting is considered as successful, in view of the fact that despite the various difficulties, all the 28 Member States submitted their report in time. ENISA has provided the appropriate framework and worked constructively together with the Supervisory Bodies and the European Commission to facilitate this process.

[1] See https://www.enisa.europa.eu/publications/annual-incident-reports-2016

Table of Contents

1. Introduction

For the first year, ENISA publishes the annual report on significant incidents of breach of security and loss of integrity, which are reported to ENISA under Article 19 of the eIDAS Regulation (2014/910/EC), by the Supervisory Bodies (SBs) of the different EU Member States.

This report covers the incidents that occurred in the second half of 2016, when the Regulation entered into force and it gives a comprehensive overview of the annual summary reporting by the Member States together with the presentation of one incident. This report does not include details about individual countries or providers.

This document is structured as follows: Section 2 briefly summarize Article 19 and the role of ENISA. This is the section that provides the fundamental knowledge for the reader and the basis for our work. Subsequently, section 3 presents the details of the technical implementation of Article 19, as agreed in the Article 19 Experts Group by the different SBs of the EU Member States. In this chapter the reader can go through the definition of the reportable security incidents, be informed about the relevant services in scope and understand the incident reporting flows as they emerge from the regulation.

Finally, Section 4 presents the analysis of this year's incident reporting procedure and summarizes the different steps that have taken place. A brief explanation of the process' evolvement is provided, together with some useful information on the incident and the reasons behind the low volume of registered notifications.

2. Article 19 of the eIDAS Regulation

This chapter outlines 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.

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."[2]

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.

[2] 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)'.

3. Article 19 Experts Group and Incident Reporting Procedure

In 2014, after eIDAS was adopted, ENISA formed an experts group, to work together with experts from competent authorities on the application of Article 19 and, more generally, security incidents in trust services. This group, called the Article 19 Experts Group, reached an agreement on the following non-binding technical document providing guidance to the SBs in the EU Member States:

- Incident reporting framework for eIDAS Article 19[3]

The Article 19 Experts Group organises meetings, workshops and conference calls on a regular basis to develop technical guidelines, to discuss the implementation of Article 19 and to share knowledge and exchange views about past incidents and how to address them.

3.1 Incident reporting procedure

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

3.1.1 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 incident: 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[4] or on the personal data maintained therein.

Thresholds for trust service providers to notify the national supervisory bodies (i.e. what is significant) depend on national circumstances: different countries will adopt a different approach to setting national reporting thresholds, depending on national specificities, 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[5] 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.

3.1.2 Services in scope

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

[3] See https://www.enisa.europa.eu/publications/article19-incident-reporting-framework
[4] 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.
[5] A threshold is considered as a triad of an indicator accompanied by specific values and measurement unit description.

'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*

ENISA's Article 19 EG has agreed on a more detailed list of services, which can be helpful for the analysis. The full list is available at our Incident Reporting Framework[6].

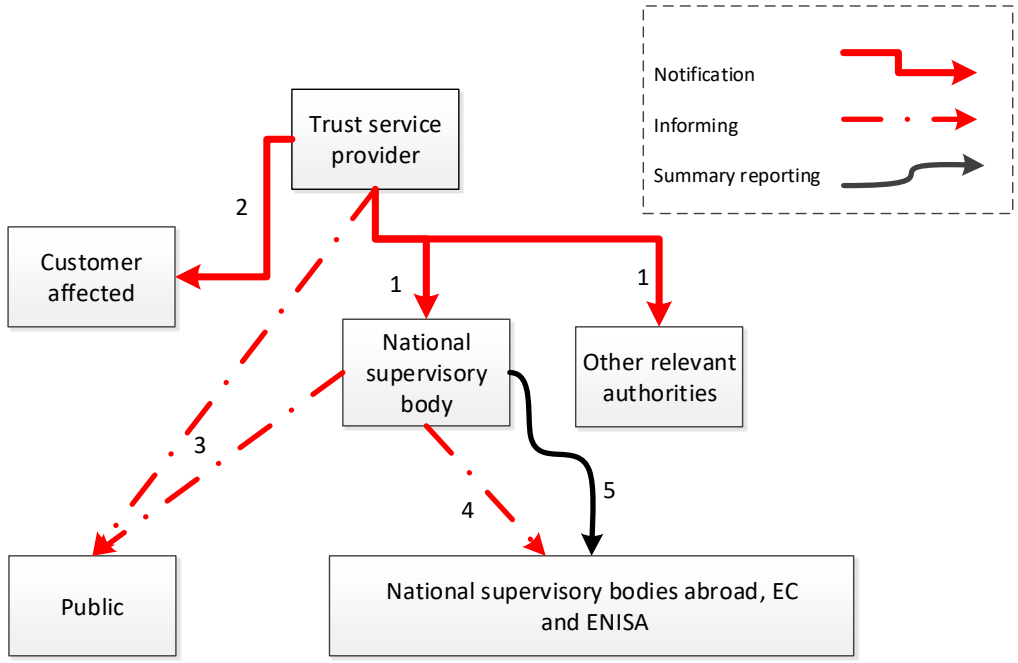
3.1.3 Incident reporting flows

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 becomes aware of it[7], 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.

[6] See https://www.enisa.europa.eu/publications/article19-incident-reporting-framework, paragraph 3.2
[7] 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[8]:

- 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[9], 4) and **national incident notification** (flows 1, 2, 3).

3.2 Indicators for annual summary reporting

ENISA worked together with the Article19 Experts Group on a framework to ease 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.

[8] A relying party is considered as part of the public.
[9] 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.

Member states can take different approaches to defining their national reporting thresholds, thus it is important to set notification indicators and thresholds which are the same for all Member States. ENISA had already gone through this exercise with the Article 13a EG and highlighted from the very beginning the value of defining parameters that could be easily adopted by both SBs and TSPs. However, trust services require a different approach compared to the telco framework, hence two proposals were drafted.

The first proposal was composed by two groups of incident examples/scenarios: the service specific one which contains incident examples with an impact on each specific trust service and the generic one which contains grouped incident examples with 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. The full list is available in the Incident reporting framework for eIDAS Article 19 publication[10]. This list should be used as a general guideline 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.

The second proposal, was based on an impact assessment of assets, relevant to the eIDAS services. A table that shows the impact of having compromised one of the three basic security principles (Confidentiality, Integrity, Availability) for each service and the associated assets has been created. In order to produce a clear and concise presentation of the impact, a uniform scale of low, medium and high has been used.

Ultimately, the Supervisory Bodies, decided to adopt the first proposal in order to determine the significance of an incident. Nevertheless, when CIRAS-T, the online tool to facilitate the incident reporting procedure was under development, both proposals were incorporated. There was a common agreement, that implementing both schemes is not considered to be duplicate information on the same issue, but an approach that can offer substantial information for the analysis.

[10] See https://www.enisa.europa.eu/publications/article19-incident-reporting-framework, Annex D

4. Analysis of Incident Reporting procedure

As expected, as this was the first year of the incident reporting, some delays occurred in the process. First and foremost, during our Article 19 EG meetings, we identified slow adoption of the Regulation and consequently of the national secondary legislation. Apart from the transposition of the eIDAS Regulation to the national legislation, each Member State had to appoint a competent authority as the Supervisory Body.

The Supervisory Bodies landscape is mixed. In some cases, Member States (MS) followed the Article 13a approach and appointed an existing National Regulatory Authority for the Telecom sector. In other Member States, another national authority took over this responsibility, while there are some cases where this role was granted to a ministry. Moreover, in some Member States, there are more authorities involved, with different tasks, e.g. a National CSIRT or a Data Protection Authority, a scheme which is depicted in section 3.1.3.

Considering that the Regulation's rules for trust services entered into force on July 1, 2016, the reference period was the second half of 2016. At that time, the above mentioned legislative procedures were on-going for many Member States, thus there was a gap in the reporting procedure between TSPs and SBs.

In total, all 28 EU Member States participated in this process. Out of these, only one Member State reported one significant incident and 27 countries submitted empty annual reports. There are possible various reasons for this figure. Firstly, as stated before, some incidents might not be registered due to the legislative delays and the absence of a SB. Secondly, there might be incidents on the boundary of the thresholds, eventually classified as not significant. Thirdly, SBs recorded incidents with minor significance in EU-level, but reportable in national level. Finally, other incidents are excluded from reporting because they had happened into a closed system[11].

The registered incident's significance was assigned with the value 3 on the adopted severity scale. The Supervisory Body indicated that the root cause was a system failure and more particularly after a system update there was no access to the validation of (qualified) certificates for electronic signatures service. Thus, the category of the impact is only availability. The affected Trust Service Provider was a qualified one and the incident's duration was 10 hours. About 20 percent of the subscribers (41.000) were potentially impacted by this, however it had happened on a public holiday, consequently the actual percentage is considered to be far lower. In general, this incident can be marked as medium-impact, with no cross-border implications. Moreover, the TSP dealt promptly with this issue and took the appropriate measures to avoid the re-occurrence of the same problem. The new software includes a new feature which performs some additional checks in order to enhance the CRL accessibility.

At this point, we should highlight a very important peculiarity of incidents falling under Article 19. There is the possibility that an incident has cross-border impact. According to the Regulation (see 2.1), these kind of incidents require immediate notification. Therefore, a productive endeavour is needed, to deal with them promptly, in an effective and efficient manner. Despite the fact that the Regulation is quite new, this will be important in the future. Recently, considerable attention has been placed on the role of the blockchain technology and the possible implications on the eIDAS. As the environment is continuously evolving, we might soon be confronted with the need of an updated incident reporting framework.

[11] The Regulation states that "In particular, it should not cover the provision of services used exclusively within closed systems between a defined set of participants, which have no effect on third parties. For example, systems set up in businesses or public administrations to manage internal procedures making use of trust services should not be subject to the requirements of this Regulation. Only trust services provided to the public having effects on third parties should meet the requirements laid down in the Regulation."

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

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

TP-04-17-958-EN-N

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

ISBN: 978-92-9204-234-9
DOI: 10.2824/988312