EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TRUST SERVICES SECURITY INCIDENTS 2020

Annual Report

JULY 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For technical queries about this paper, please email resilience@enisa.europa.eu
For media enquiries about this paper, please email press@enisa.europa.eu

AUTHORS

Vassiliki Gogou, Marnix Dekker and Eleni Vytogianni, European Union Agency for Cybersecurity

ACKNOWLEDGEMENTS

We are grateful for the review and input received from the experts in the ENISA Article 19 Expert Group which comprises experts from more than 30 national supervisory bodies (SBs) in the EU, EFTA, EEA and EU candidate countries. The group is currently chaired by a representative of RTR Austria.

LEGAL NOTICE

COPYRIGHT NOTICE

Catalogue Number: TP-05-21-229-EN-N
ISBN: 978-92-9204-511-1
DOI: 10.2824/277632

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The EU's eIDAS regulation (EU Regulation 910/2014) sets rules for electronic identity schemes and trust services in Europe, national eID schemes, cross-border interoperability and recognition. eIDAS was adopted in July 2014 and came into force in 2016. One of the goals of eIDAS is to ensure that electronic signatures can have the same legal standing as traditional signatures and to remove barriers to electronic commerce and all types of electronic transactions in the EU. The eIDAS regulation aims to:

- ensure that people and businesses can voluntarily use their own national electronic identification schemes (eIDs) to access public services available online in other EU countries.
- create a European internal market for trust services by ensuring that they will work across borders and have the same legal status as their traditional paper-based equivalents.

Article 19 of the eIDAS regulation sets out the security requirements for the trust service providers (TSPs) and introduces mandatory security breach reporting for trust service providers (TSPs) in the EU. The reporting obligations have three parts:

- Trust service providers must notify security breaches that have a significant impact to the national supervisory bodies.
- The national supervisory bodies must inform each other and ENISA if there are breaches which have an impact across borders.
- Every year national supervisory bodies must send *annual summary reports* about the notified breaches to ENISA and the Commission.

This report, the Annual Report Trust Services Security Incidents 2020, provides an aggregated overview of the notified breaches for 2020, analysing root causes, statistics and trends. This report marks the fifth round of security incident reporting for the EU's trust services sector.

In this round of annual summary reporting a total of 27 EU countries and 2 EFTA countries took part. They reported a total of 39 incidents.

KEY FINDINGS

We summarize the key findings from the 2020 incident reports:

- **A steady increase in notified incidents:** in 2020 notified incidents increased by around 18%. This suggests that authorities and TSPs are becoming more familiar with the breach reporting process and their obligations under eIDAS.
- **The number of incidents with a large impact has dropped:** in 2020 only 3 incidents were characterized as having had a "large impact" as opposed to 2019 when 10 such incidents had been reported (translating into approximately 60% decrease).

The ratio of reported incidents concerning qualified and non-qualified trust services remains high: in 2020, 69% of total incidents had an impact on qualified trust services compared to approximately 33% of incidents reported on non-qualified trust services (with some incidents touching both categories.

2020 HIGHLIGHTS

The number of notified incidents is steadily increasing.

The number of incidents with large impacts has dropped.

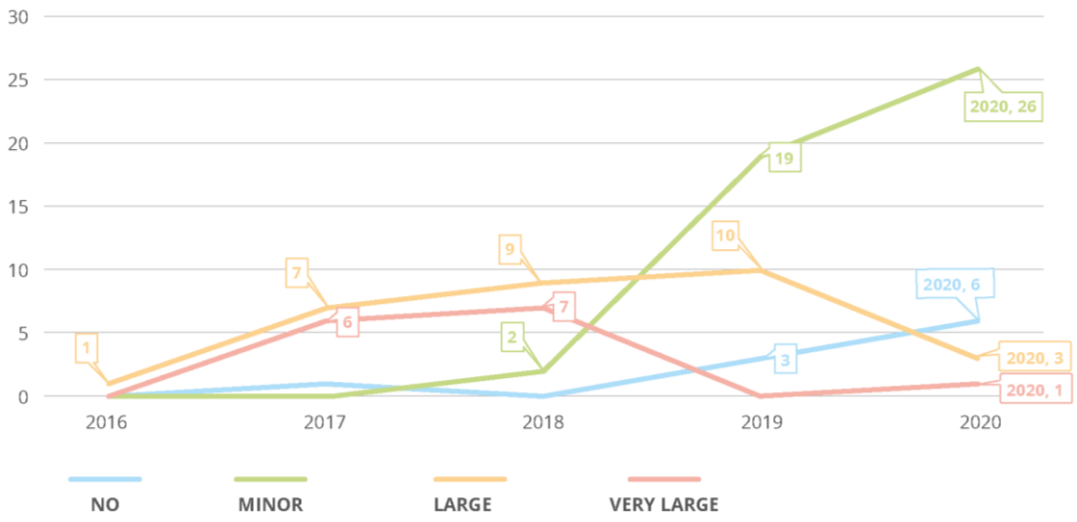
System failures account for more than half of incidents and have been the dominant root cause for the last four years of incident reporting.

Although non-qualified trust services are widely used by citizens and enterprises, it seems that the respective trust services operators do not make much effort to report related incidents. In most cases, the notification is done by a TSP that also offers qualified services, reporting an incident that has affected both their qualified and non-qualified services.

The impact on subservices is mainly divided between certificate management (47% of the incidents) and certificate generation (42% of the incidents).

Approximately 66% (26 incidents) of the reported incidents were rated as minor compared to 2019 when 60% (19 incidents) were rated as having had only a minor impact. Only one incident had a very large (disastrous) impact, and only three incidents had a large impact. Furthermore, a significant increase in minor incidents has been observed, indicating that the incident reporting mechanism has become more familiar to the providers and they are reporting more incidents regardless of their severity.

Figure 1: Severity of impact - Trust services security incidents in the EU reported over 2016-2020



ENISA publishes detailed statistics about trust services security incidents in an online visual tool, CIRAS Visual. This tool allows for custom analysis of trends and patterns[1].

Currently the European Commission, Member States and the European Parliament are discussing policy changes. Last year the Commission proposed to integrate Article 19, the security requirements for TSPs into a revised NIS Directive. The goal of this Commission proposal, the NIS2 proposal, is to simplify EU cybersecurity legislation and to ensure that there is a similar approach across the different sectors, including the telecom sector and the trust services sector, which are currently addressed under separate pieces of legislation. This year the Commission will also make a proposal for a new eIDAS regulation.

ENISA will continue to support national supervisory bodies with the implementation of breach reporting under Article 19 of eIDAS and to work towards making this process efficient and effective, yielding useful data, for the supervising bodies, for the national authorities, as well as for the trust service providers and the organisations relying on these trust services

[1] See https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

1. INTRODUCTION

Under Article 19 of the eIDAS Regulation[2], Trust Service Providers (TSPs) in the EU are expected to notify the national supervisory bodies in their country about security incidents. On an annual basis, the supervisory bodies send summaries of these incident reports to ENISA. Subsequently, ENISA publishes an aggregated overview of the reported security incidents.

This document gives an aggregate overview of the security incident reports submitted by the supervisory bodies during 2020. This annual report marks the fifth round of security incident reporting in the EU's trust services sector, covering security incidents during 2020.

1.1 SCOPE

Incidents reported by authorities under Article 19 of the eIDAS regulation

1.2 TARGET AUDIENCE

Experts at national authorities, experts in the sector

1.3 CONTENT

This document is structured as follows: in section 2, the policy context is briefly summarized as is the underlying eIDAS reporting framework and an overview of the types of incidents reported is provided by anonymized examples. In Section 3, further elaboration of the reported incidents is given, by presenting the categories of root causes, the detailed causes, and the affected services. In section 4, the multi-annual trends in incidents over the years 2016-2020 are highlighted. In Section 5, conclusions and observations based on the available data are drawn.

1.4 DISCLAIMER

This document only contains aggregated and anonymized information about incidents and does not include details about individual countries or individual trust service providers. Detailed discussions about the reported security incidents take place in the ENISA Article 19 expert group, which is an informal group of experts from national supervisory bodies focusing on the practical implementation of Article 19. The group is currently chaired by a representative from RTR, the Austrian regulatory authority. ENISA acts as the secretariat and supports the group with analysis, drafting, logistics, etc.

[2] 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, can be consulted at https://eur-lex.europa.eu/eli/reg/2014/910/oj

2. INCIDENT REPORTING FRAMEWORK

In this section, we give an overview of the formats and procedures for the reporting of incidents (breaches) under Article 19 of the eIDAS regulation.

EIDAS ARTICLE 19

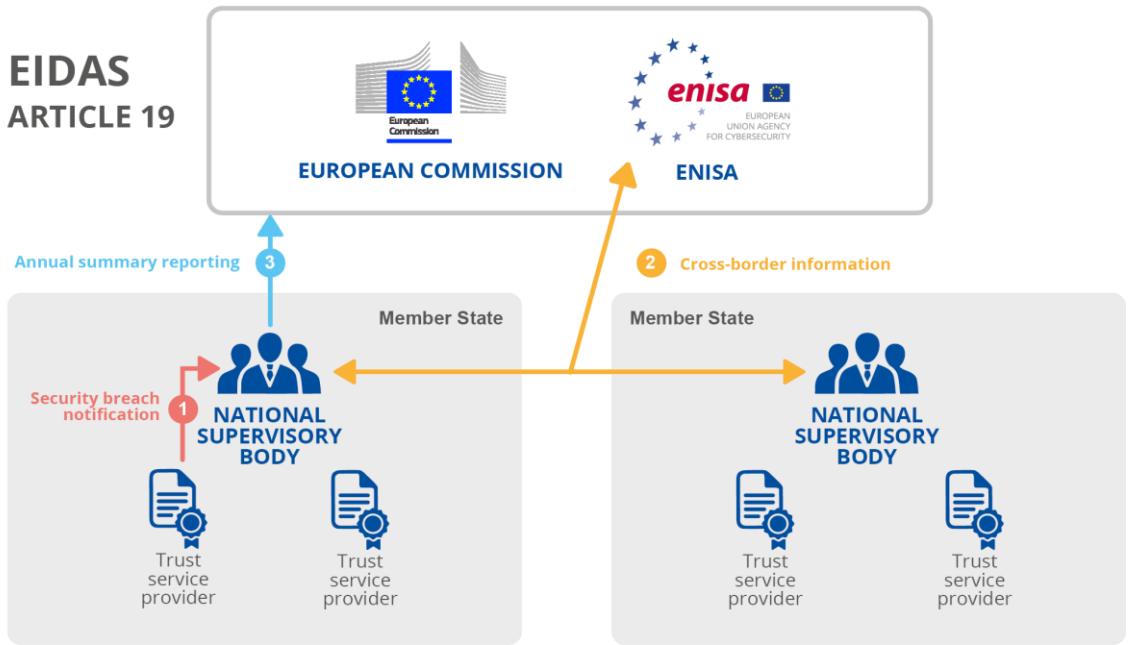
requires trust service providers in the EU to
1) assess risks;
2) take appropriate security measures to mitigate security breaches;
3) notify breaches to national supervisory bodies.

2.1 OVERVIEW OF INCIDENT REPORTING PROCESS

The mandatory security breach notification process has three steps as displayed in the figure below:

1. Trust service providers notify their national supervisory body about security breaches that have significant impact.
2. National supervisory bodies inform each other and ENISA if there is a cross-border impact.
3. National supervisory bodies send *annual summary reports* about the notified breaches to ENISA and the Commission.

Figure 2: Incident reporting under article 19 of eIDAS regulation



2.2 INCIDENT REPORTING TOOL

Experts from the national authorities have access to the ENISA CIRAS incident reporting tool, where they can upload incident reports and search for and study specific incidents.

For the public, ENISA also offers an online visual tool, which is publicly accessible and can be used for custom analysis of the data. This tool anonymizes the country or operator involved.

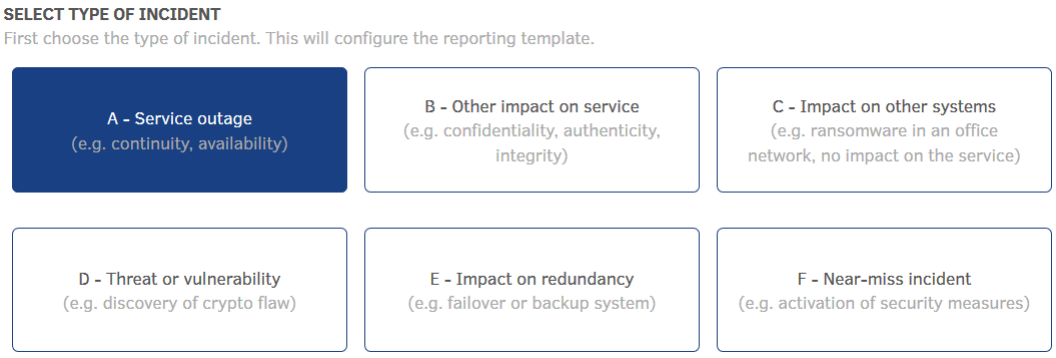
CIRAS

is a free online tool where ENISA stores reported incidents and provides annual and multiannual statistics: https://www.enisa.europa.eu/ciras

We briefly introduce the reporting template. The template starts with a type selector and contains three parts:

1. Impact of the incident - which trust services are impacted and by how much.
2. Nature of the incident - what caused the incident?
3. Details about the incident - detailed information about the incident, a short description, the types of services, the types of assets, the severity level etc.

Figure 3: eIDAS Article 19 incident reporting types



- **Type A**: Service outage (e.g. continuity, availability). For example, *an outage caused by a cable cut due to a mistake by the operator of an excavation machine used for building a new road* would be categorised as a type A incident.

- **Type B**: Other impact on service (e.g. confidentiality, authenticity, integrity). For example, *a popular collaboration tool has not encrypted the content of the media channels, which are being established when a session is started, between the endpoints participating in the shared session. This leads to the interception of the media (voice, pictures, video, files, etc.) through a man-in-the-middle attack*. This incident would be categorised as a type B incident.

- **Type C**: Impact on other systems (e.g. ransomware in an office network, no impact on the service). For example, *a malware has been detected on several workstations and servers of the office network of a telecom provider*. This incident would be categorised as a type C incident.

- **Type D**: Threat or vulnerability (e.g. discovery of crypto flaw). For instance, *the discovery of a cryptographic weakness* would be categorised as a type D incident.

- **Type E**: Impact on redundancy (e.g. failover or backup system). For example, the *breaking of one of two redundant submarine cables* would be categorised as a type E incident.

- **Type F**: Near-miss incident (e.g. activation of security measures). For instance, *a malicious attempt that ends up in the honeypot network of a telecom provider* would be categorised as a type F incident.

Depending on the type selected, some fields in the template are deactivated. For example, in the case of a Type A incident the fields “threat severity factors” and “severity of threat” are not active.

2.3 ANONYMIZED EXAMPLES OF SECURITY INCIDENTS

In this section we present some of the kinds of incidents that are reported, by providing several detailed and anonymized examples.

Incident example 1	
Incident type	A-Core service outage
Service affected	eSignature
Root cause	System failure
Technical causes	Faulty software change/update
Assets affected	Generation and validation of signatures/seals platform
Comment	Unavailability of the eSignature service due to an outage of the front-end application component

Incident example 2	
Incident type	A-Core service outage
Service affected	System failure
Root cause	Faulty software change/update
Technical causes	Generation and validation of signatures/seals platform
Assets affected	Unavailability of the eSignature service due to an outage of the front-end application component
Comment	eSignature

Incident example 3	
Incident type	A-Core service outage
Service affected	eSignature, eTimestamps
Root cause	Natural phenomena
Technical causes	Natural phenomena
Assets affected	Generation and validation of signatures/seals platform, Time Stamping Authority (TSA) platform, Validation Authority (VA) platform
Comment	Consequences of heavy rain caused unavailability of registers and information systems. Synchronisation with redundant hardware of information systems was also disturbed. Additional sealing means was installed.

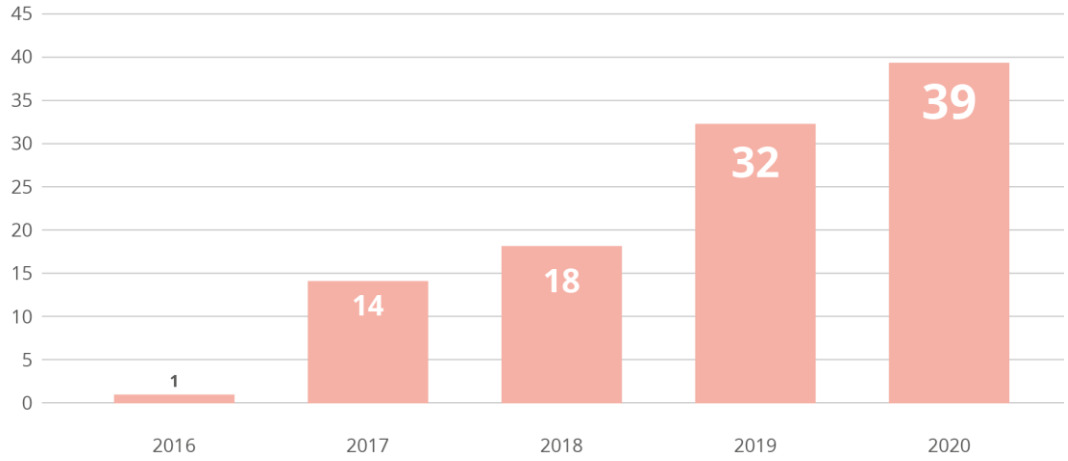
Incident example 4	
Incident type	B-Other impact on core service
Service affected	eSignature
Root cause	Malicious action
Technical causes	Tampering of personal data, theft or loss of data
Assets affected	Generation and validation of signatures/seals platform, Time Stamping Authority (TSA) platform, Validation Authority (VA) platform
Comment	The incident concerns the creation of a qualified certificate following a phishing attack and the creation of a false identity through online banking. The certificate was used only once to sign the terms and conditions for opening an account in another bank. That bank has been warned and closed the account. The qualified certificate has been revoked.

Incident example 5	
Incident type	D-Active threat or vulnerability
Service affected	PDF signing
Root cause	Malicious action, third party failure
Technical causes	Vulnerability inherent to document format
Assets affected	Generation and validation of signatures/seals platform, Time Stamping Authority (TSA) platform, Validation Authority (VA) platform
Comment	Signed PDF files can be manipulated in a way that they look different to the signatory than to relying parties (shadow attacks, https://www.pdf-insecurity.org/). Signing services and validation services are not affected. The vulnerability has been resolved by issuing new versions of PDF viewers. Recommendations for signatories by TSPs have been updated accordingly.

3. INCIDENT ANALYSIS

The 2020 annual summary reporting, by the 27 EU Member States and 2 EFTA countries participating in this process, included in total 39 security incidents[3]. This is the fifth round of annual summary reporting, since eIDAS came into force on the 1st of July 2016.

Figure 4: Number of incidents per year



There is a steady increase in the number of incidents reported which, over the years, leans towards becoming linear. This suggests that TSPs are becoming more familiar with the process.

3.1 ROOT CAUSE CATEGORIES

The figure nr. 5 shows the distribution of the incidents according to their underlying root cause.

We categorize incidents into four categories of root causes: Systems failures, Human errors, Malicious actions and Natural phenomena.

- System failures continue to be the dominant root cause, accounting for just over half of total trust services incidents reported (53%, around 20 incidents). Typically, system failures are due to either hardware failures or software bugs.
- Almost 39% of incidents were categorised as human errors.
- Around 5% of the incidents were flagged as malicious actions.

We also keep track of third-party failures, i.e. when the incident really originated at a third party. For 2020, 14% of incidents were flagged as third-party failures. All these third-party failures were categorized as system failures. See figure nr. 6.

53%
of 2020 trust services incidents reported have System failures as root cause

[3] Note that three of the reported incidents were indicated as type D-Active threats or vulnerabilities and are not included in the analysis

Figure 5: Root causes of TSP security incidents in 2020

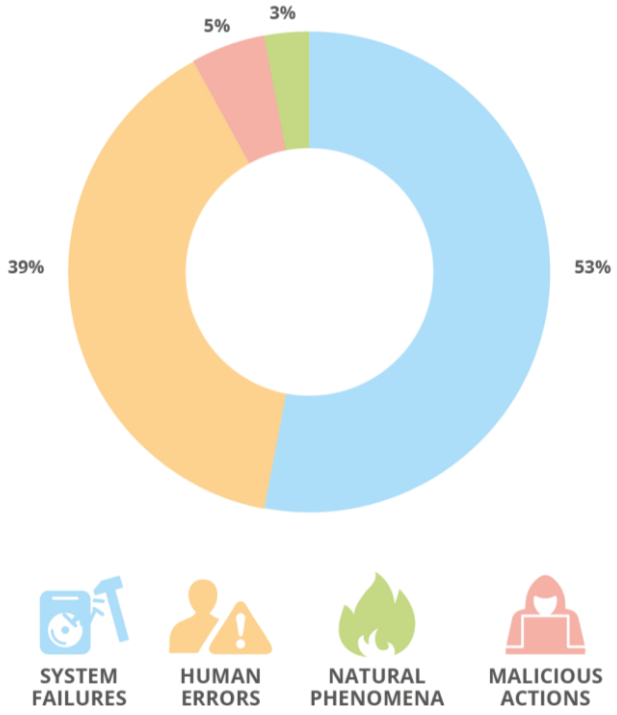
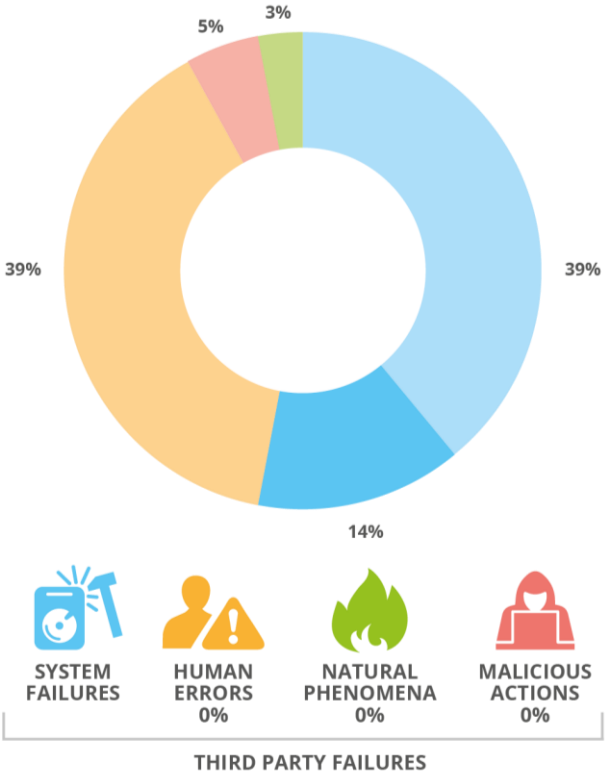


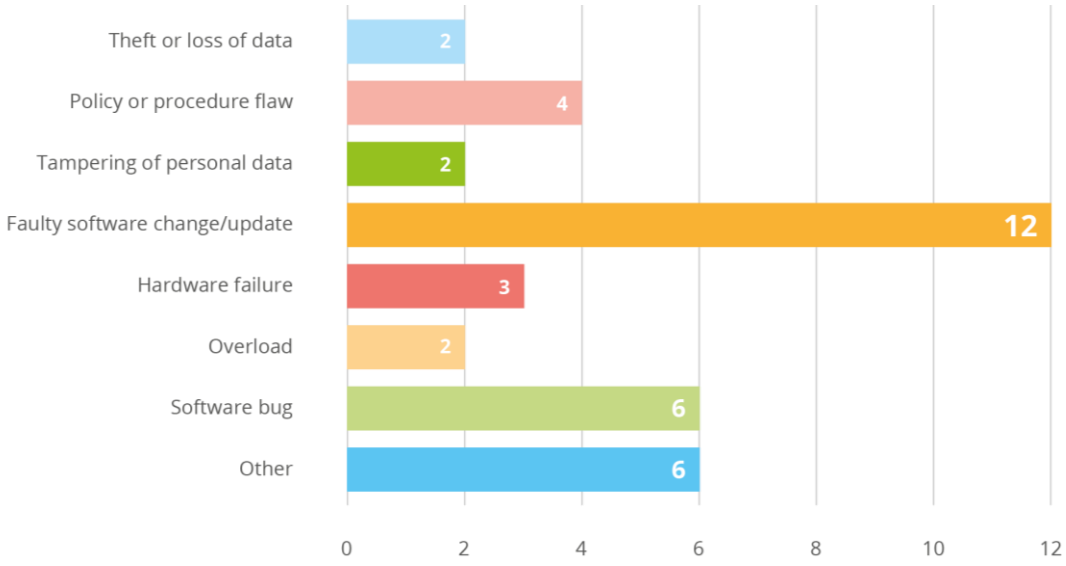
Figure 6: Third party failures - 2020



3.2 DETAILED CAUSES

The two most common detailed causes of incidents were faulty software changes/updates and software bugs. It is important to note that an incident is often not only triggered by one cause but can involve multiple detailed causes (i.e. a chain of events). The third most common detailed cause is flaws in the organization's policy or procedures.

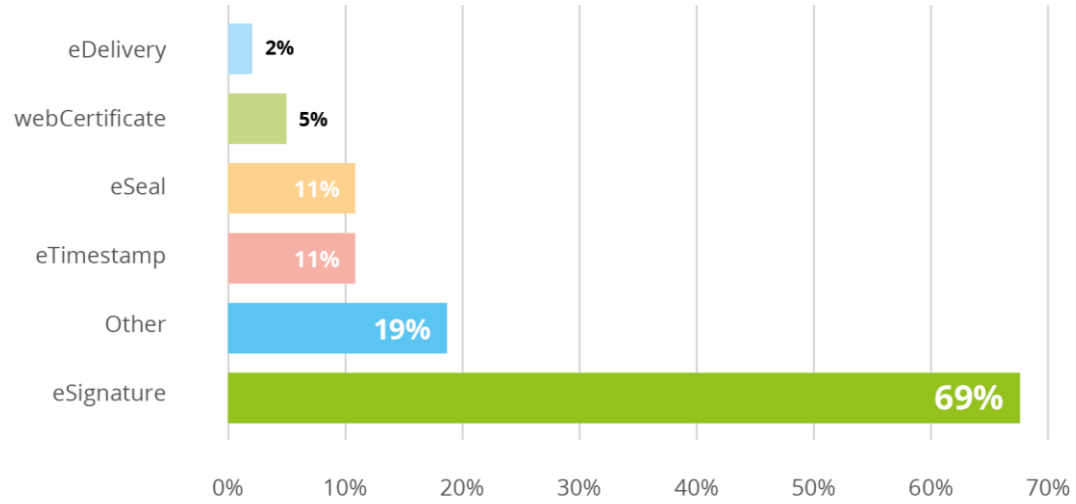
Figure 7: Detailed causes of trust services security incidents - 2020



3.3 TYPES OF TRUST SERVICES AFFECTED

Most of the reported incidents (69%) had an impact on electronic signatures (see the chart below). Electronic seals were affected in about one tenth (11%) of all cases, as were electronic timestamps (another 11%).

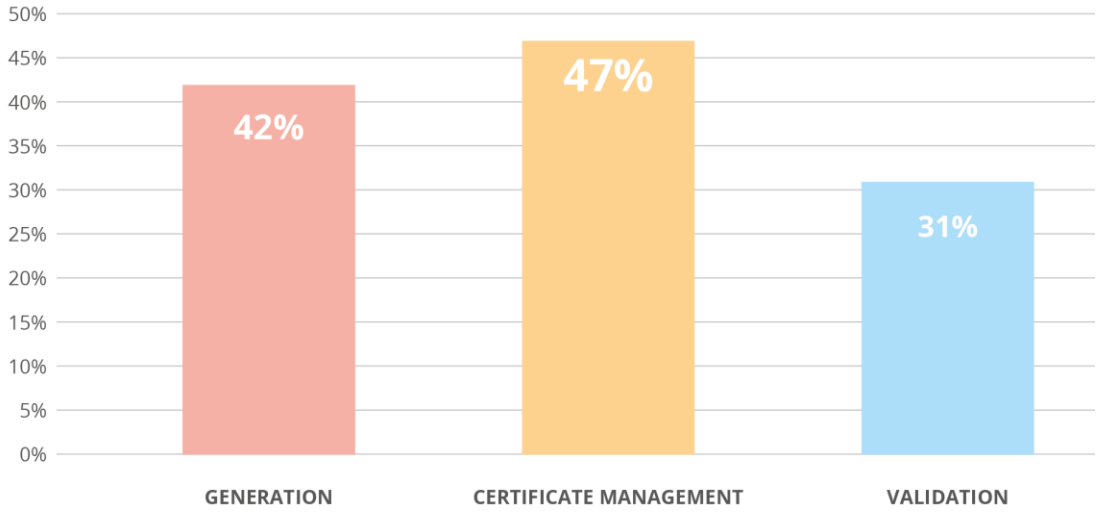
Figure 8: Impact of incidents - 2020



If we look back at the past four years of reporting, we see a similar pattern: 83% of the reported incidents had an impact on electronic signature services, while 29% affected electronic seals and 20% affected timestamping services.

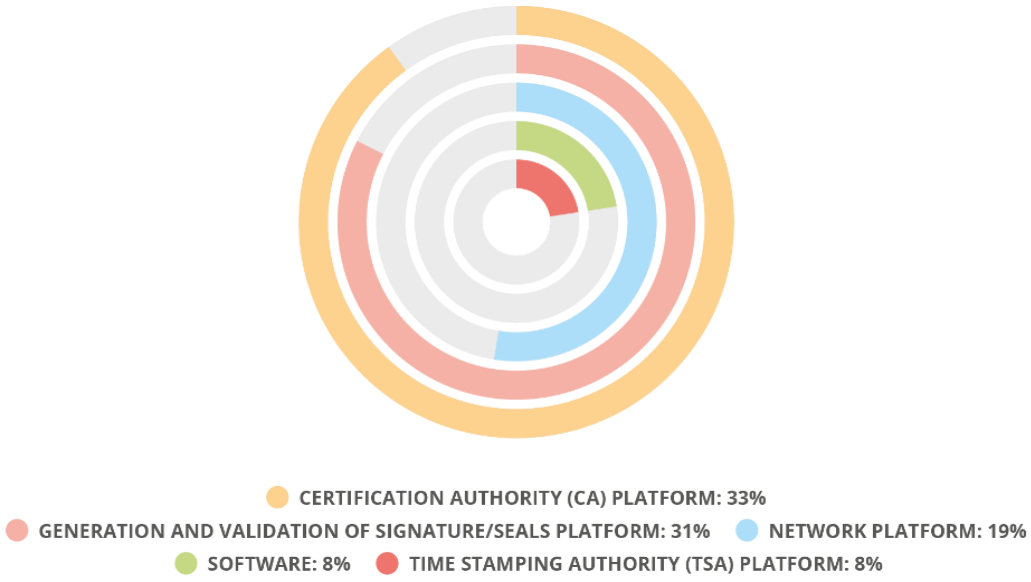
For each incident we keep track of the underlying subservices affected. Most incidents impact the generation of signatures/seals/timestamps (42%) or certificate management (47%)

Figure 9: Impact of incidents on subservices



Finally, we also keep track of the underlying assets affected by incidents. In most cases the assets affected are the Certification Authority (CA) platform (33%) and the platform for the generation and validation of signatures/seals platform (31%). See the impact on technical assets in the chart below.

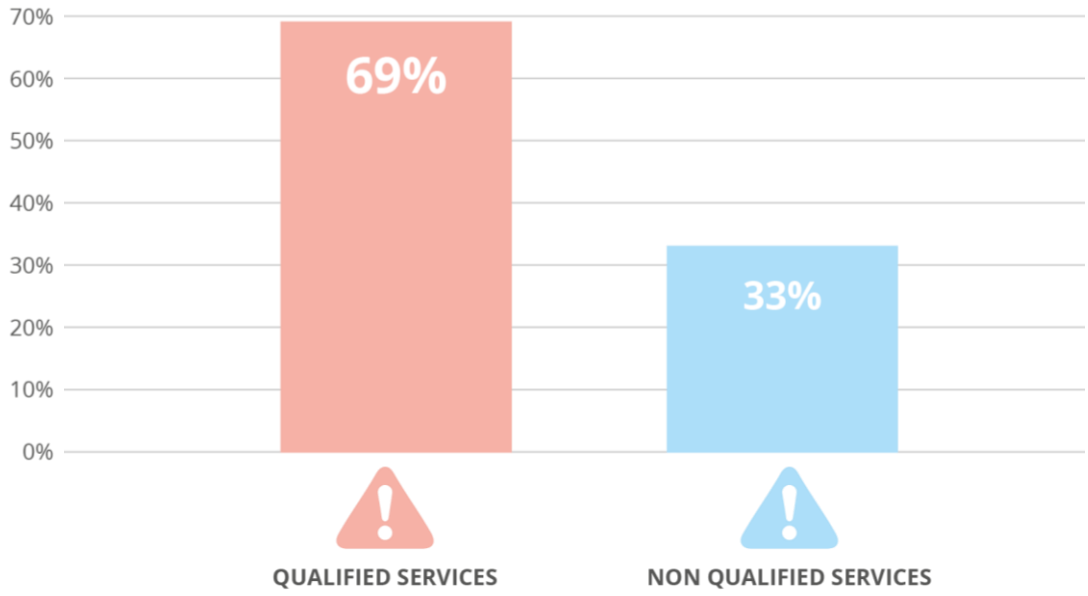
Figure 10: Technical assets affected



3.4 QUALIFIED SERVICES VERSUS NON-QUALIFIED SERVICES

This year nearly 70% of total trust services security incidents had an impact on qualified services (i.e. qualified signature certificate creation, qualified seal certificate creation, etc.), while only a third of the incidents affected a non-qualified service. Again, it is important to note that one incident report could involve multiple trust services, which explains why the percentages in the graph 8 below add up to more than 100%.

Figure 11: Reported Incidents affecting Qualified v Non-qualified services



Note that in most cases, the TSP notifying an incident is also offering qualified services and that in most cases the impact on non-qualified services is reported as part of an incident report for a qualified trust service. This suggests that there is a gap in the reporting and that, while Article 19 is also concerned with non-qualified services, only the TSPs offering qualified trust services are reporting incidents, and mostly do so concerning incidents that impact qualified services.

4. MULTI-ANNUAL TRENDS 2016-2020

ENISA has been collecting and aggregating trust services incident reports since 2016. In this section, we look at multi-annual trends over the last 5 years, covering the period from 2016 to 2020. The total dataset contains 104 reported incidents.

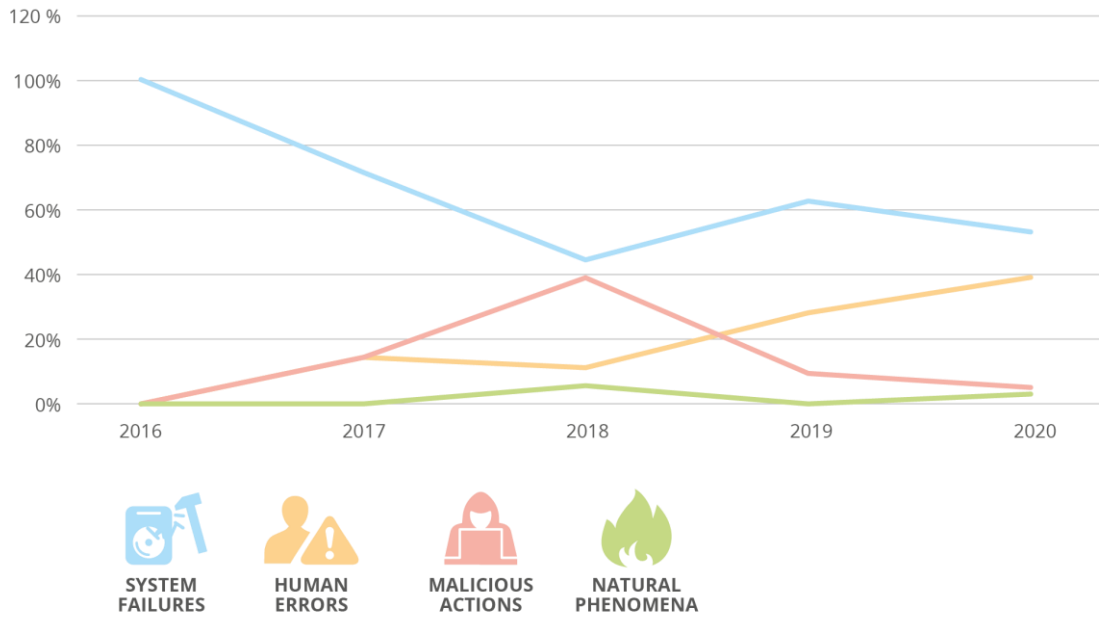
68%
of total trust services incidents reported since 2016 have hardware failures (35%) and software bugs (33%) as main root causes

4.1 MULTI-ANNUAL TREND IN ROOT CAUSE CATEGORIES

Over the last few years of trust services security incident reporting – as displayed in the graph below – the most common root cause has been system failures. These add up to 68% over the period since 2016. For this specific root cause, the most common detailed causes were hardware failures (35%) and software bugs (33%).

Note that we observe the same pattern in electronic communication services[4], where system failures account for almost two thirds (67%) of total incidents (722 out of 1093 incidents).

Figure 12: Root cause categories – Trust services security incidents in the EU reported over 2016-2020



Around a fifth of the reported incidents (18%) were caused by malicious actions and another fifth were flagged as human errors.

In the trust services sector, natural phenomena are not a common root cause. In comparison, the telecom sector is quite different because it has extensive over-the-ground IT infrastructure which is vulnerable to natural phenomena such as storms.

[4] See ENISA Annual Report Telecom Security Incidents 2019

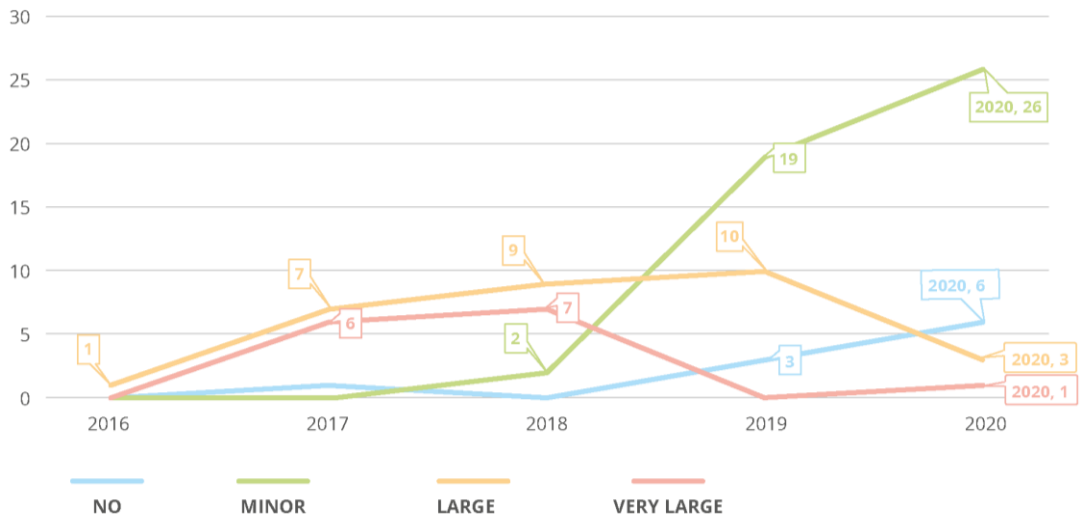
4.2 MULTI-ANNUAL TREND IN SEVERITY OF IMPACT

In the multi-annual trend concerning the severity of impact, the EU Cybersecurity incident taxonomy is again followed where the severity of the impact has the following values: no impact, minor, large and very large impact[5].

While comparing the statistics for severity since 2016 (Graph 10 below), it is quite clear that the number of incidents with large impacts is decreasing significantly although it was rather stable for the previous four years. It is interesting to see that there was a rather linear increase in minor incidents since last year.

This is again an indication that the incident reporting mechanism has become more familiar to trust services providers and also more effective; providers are reporting more incidents regardless of their severity. In contrast to 2018, there were no very large (i.e. disastrous) incidents during 2019 and 2020.

Figure 13: Severity of impact–- Trust services security incidents in the EU reported over 2016-2020



[5] See CG Publication 04/2018 - Cybersecurity incident taxonomy

5. CONCLUSIONS

We conclude with the main findings and some more general observations about this process and the broader policy context.

MAIN FINDINGS

- **A steady** lower level of severity confirms that TSPs are become more familiar with the incident reporting process and that they are reporting more incidents, even if they are less severe.
- **Qualified trust services versus non-qualified trust services:** The ratio of reported incidents concerning qualified trust services over non-qualified ones remains high. In 2020, 69% of total incidents had an impact on qualified trust services when compared with approximately 33% of incidents reported on non-qualified trust services. Although non-qualified trust services are widely used, not so much effort is made by operators on related incident reporting. In most cases, notifications are performed by a TSP offering all types of services (qualified and non-qualified), reporting an incident that has affected both their qualified and non-qualified services.
- **System failures (53%) remain the dominant root cause** and the second most dominant are human errors with 39%.

GENERAL OBSERVATIONS

- **PDF signing vulnerabilities in 2020:** in 2020 authorities discussed and reported on several vulnerabilities with PDF signatures. In 2020, the so-called “shadow attacks” emerged as a new class of attacks, where signed documents contain hidden content, which an attacker can reveal after the document has been signed. These vulnerabilities affect a wide range of software products. These vulnerabilities, which are not under the control of a TSP and therefore can hardly be supervised, were reported as type D-incidents/vulnerabilities during 2020.
- **Supervision of non-qualified services:** The supervision of, and incident reporting by, non-qualified services remains a concern. As already mentioned, non-qualified trust services are widely used. A good example is website (TLS) certificates, which are a staple of online/internet security. Globally around 80% of websites use web certificates. The fact that under Article 19 there are hardly any reports about incidents with non-qualified trust services suggests there is still under-reporting in this area, although one MS reported 11 incidents during 2020.
- **EU policy changes:** eIDAS regulations and eIDAS incident reporting have been in place for more than four years now and eIDAS is currently under review. The Commission will make a proposal for a revised eIDAS regulation in 2021. In 2020, the Commission also made a proposal for a revised NIS Directive, i.e. NIS2, which proposes the integration of eIDAS Article 19 to the NIS Directive. Both policy proposals are expected to deliver important improvements. These policy changes present an opportunity to address some of the gaps in policy, for example, the issue of supervision of and reporting by the providers of non-qualified services. We look forward to supporting the Commission and the EU Member States with implementing eIDAS security incident reporting in an efficient and effective manner

TP-05-21-229-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-511-1
DOI: 10.2824/277632