EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ANNUAL REPORT TRUST SECURITY INCIDENTS 2022

NOVEMBER 2023

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 incidentreporting@enisa.europa.eu
For media enquiries about this paper, please email press@enisa.europa.eu

AUTHORS

Apostolos Malatras, ENISA

ACKNOWLEDGEMENTS

We are grateful for the review and input received from the experts in the ENISA European Competent Authorities for Trust Services (ECATS) 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

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to the Regulation (EU) No 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2023

This publication is licenced under CC-BY 4.0 "Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (https://creativecommons.org/licenses/by/4.0/). This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated".

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

ISBN: 78-92-9204-654-5, DOI: 10.2824/65720

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 2022, provides an aggregated overview of the notified breaches for 2022, analysing root causes, statistics and trends. This report marks the sixth 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 3 EEA countries took part. They reported **a total of 35 incidents.**

We summarize the key findings from the 2022 incident reports:

- **A steep decrease in notified incidents:** in 2021 notified incidents increased by around 18%, same as the growth observed in 2020. However, in 2022 only 35 incidents were notified, signifying a drop by around 25%. Give that 33% of minor incidents were reported, the reason behind the drop might be due to the fact that several minor incidents did not get reported. In the context of eIDAS Art. 19 incident reporting and the relevant requirements for TSPs, even minor incidents would nonetheless need to be reported. This suggests that authorities should reinforce the necessity and significance of the breach reporting process and raise awareness to TSPs on their obligations under eIDAS.
- **The number of incidents with a large impact has slightly increased:** in 2022, 12 incidents with large impact were reported, continuing the trend observed over the past years. By comparison, in 2020 only 3 incidents were characterized as having had a "large impact" as opposed to 2021 when 11 such incidents had been reported (translating into approximately a quadruple increase). Additionally, 2 very large impact incidents were reported in 2022.

The **ratio of reported incidents concerning qualified trust services over non-qualified ones remains high**. In 2022, 75% of total incidents had an impact on qualified trust services when compared with approximately 15% of incidents reported on non-qualified trust services

HIGHLIGHTS 2022

The number of notified incidents had a 25% decrease compared to 2021.

The number of incidents with minor impact has increased and 2 very large incidents were reported.

As in previous years, most reported incidents concern qualified certificates.

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

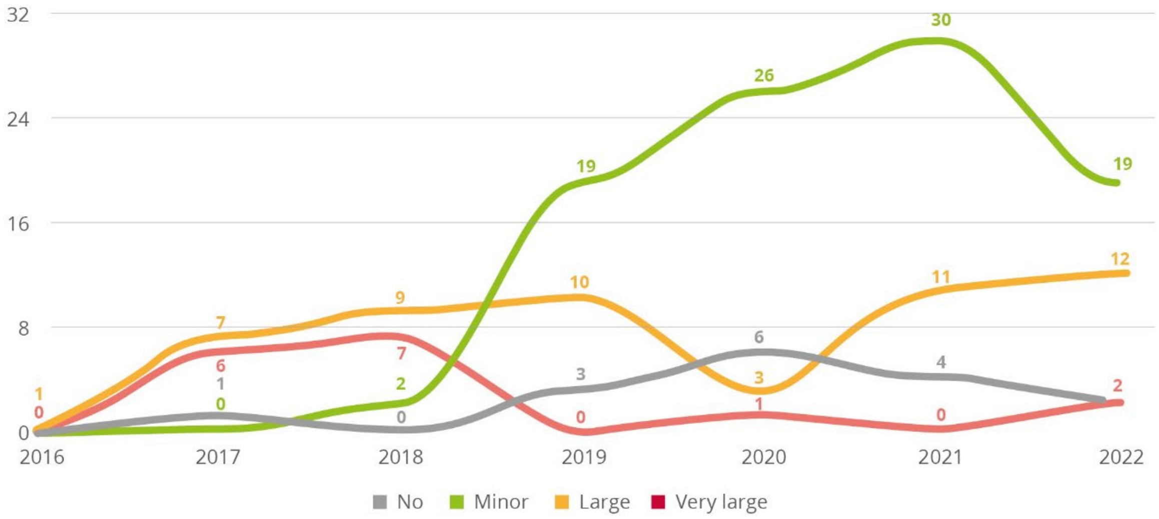
2022 witnessed a minor decrease in incidents caused by malicious actions (14,3%).

and 10% of incidents having provided no relevant information. 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. It needs to be highlighted that in 2021 significant improvement in this particular area was noted compared to 2020 when the observation was first made, and this trend persists in 2022. This is a testament to the value of the work on incident reporting and the relevant analysis, which had a direct positive impact on the overall process. However, we need to highlight the 10% of reported incidents lacking this very piece of information: providing accurate and complete information on reported incidents is essential for proper analysis and follow-up actions.

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. Having said this, compared to 2021, 2022 witnessed a slightly downward trend in this direction with 7 incidents affecting solely non-qualified services being reported (given the 25% decrease in overall reported incidents, the downward trend is justified).

The impact on subservices is mainly divided between certificate management (71,43% of the incidents) and certificate generation (42,86% of the incidents), with 17% of the incidents affecting validation services (Figure 6 in the report provides further details).

Approximately 54% (19 incidents) of the reported incidents were rated as minor, showing a stabilisation compared to 2021 if one takes into account the smaller number of reported incidents. 2 disastrous incidents of very large impact were reported in 2022, whereas a slight increase by 1 was observed for incidents with large impact, which overall quadrupled compared to 2020. Furthermore, a decrease by 50% in minor incidents of no impact has been observed, indicating (combined with the overall smaller number of reported incidents) that while the incident reporting mechanism has become more familiar to the providers and there are still challenges in reporting incidents regardless of their severity.



Severity of impact per year

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. With the advent of the revised NIS (Network and Information Security) Directive 2, incident reporting under Article 19 of eIDAS is repealed and relevant incident reporting will follow the guidelines and process of NIS2 as of October 17th 2024. The goal of this Commission Directive, the NIS2, 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. In 2023, the Commission is also working 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 2022. This annual report marks the sixth round of security incident reporting in the EU's trust services sector, covering security incidents during 2022.

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, and the detailed causes, as well as the affected services. In section 4, the multi-annual trends in incidents over the years 2016-2022 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 ECATS 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 and two vice-chairs by Ministry of Investment and Economic Development, Poland and Luxembourg Institute for Standardization, Accreditation, Security, and Quality of Products and Services (ILNAS). 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

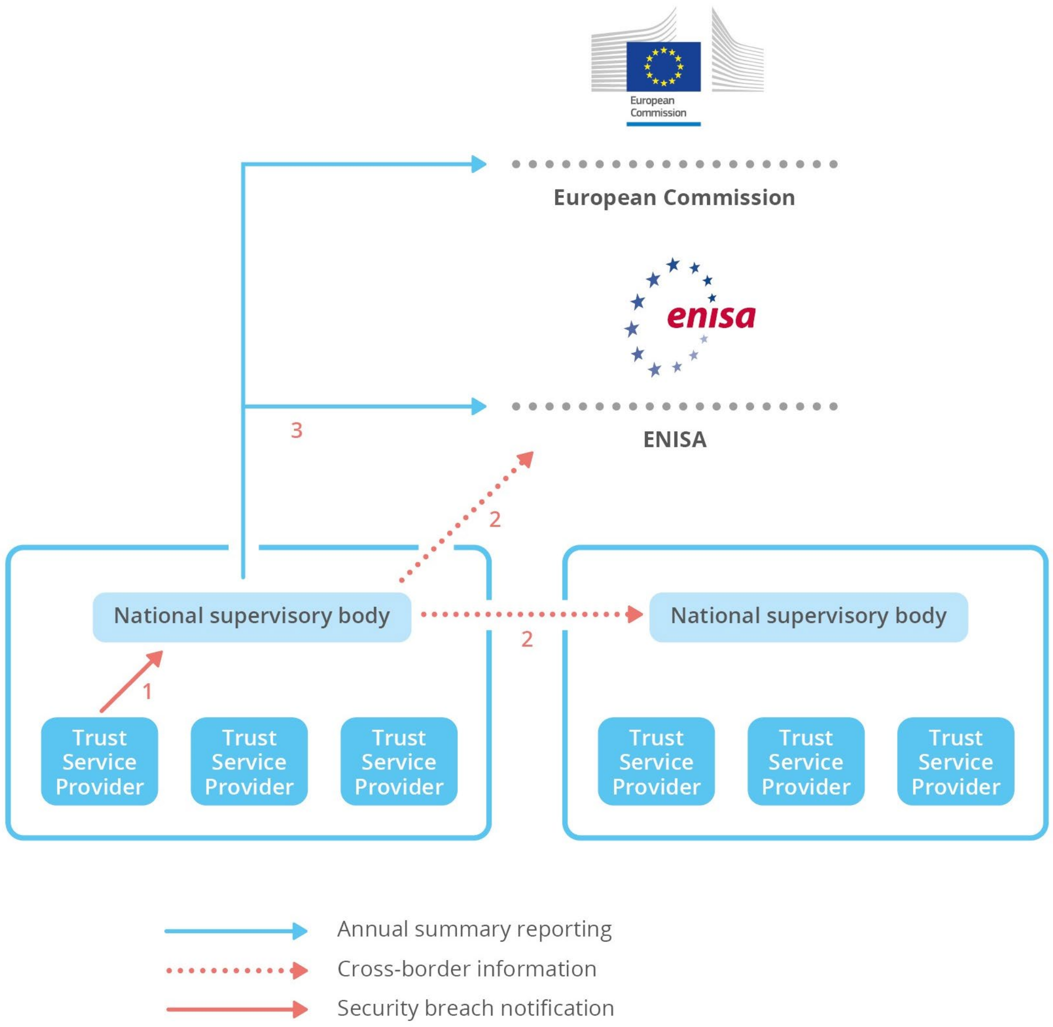
In this section, we give an overview of the formats and procedures for the reporting of incidents (breaches) under Article 19 of the eIDAS regulation.

EIDAS ARTICLE 19 requires trust service providers in the EU to 1) assess risks, 2) take appropriate security measures to mitigate security breaches, and 3) notify breaches to national supervisory bodies.

2.1 OVERVIEW OF INCIDENT REPORTING PROGRESS

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

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

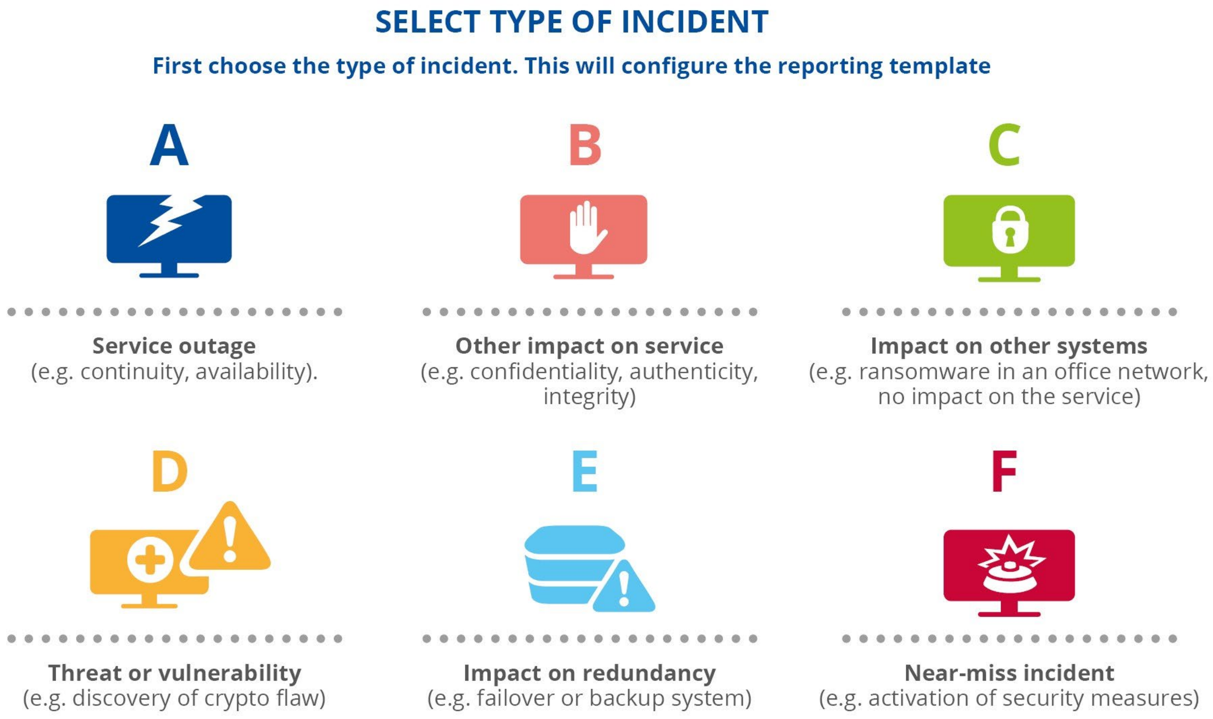


2.2 INCIDENT REPORTING TOOL

Experts from the national authorities have access to the ENISA CIRAS (Cybersecurity Incident Reporting and Analysis System) incident reporting tool[3], where they can upload incident reports and search for and study specific incidents.

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

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



SELECT TYPE OF INCIDENT

First choose the type of incident. This will configure the reporting template

A
Service outage
(e.g. continuity, availability).

B
Other impact on service
(e.g. confidentiality, authenticity, integrity)

C
Impact on other systems
(e.g. ransomware in an office network, no impact on the service)

D
Threat or vulnerability
(e.g. discovery of crypto flaw)

E
Impact on redundancy
(e.g. failover or backup system)

F
Near-miss incident
(e.g. activation of security measures)

- 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.

[3] See https://ciras.enisa.europa.eu/

- 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 detailed and anonymized examples.

Incident example 1	
Incident type	A-Core service outage
Service affected	eSignature, eSeal, eTimestamp
Root cause	System failure
Technical causes	Overload
Assets affected	• Generation (signatures, seals and timestamps) • Certificate management (registration and creation of certificates, suspension, revocation) • Validation
Comment	Unavailability of the eSignature/eSeal/eTimestamp services due to a backend system overload

Incident example 2	
Incident type	A-Core service outage
Service affected	eSignature, eSeal
Root cause	Malicious actions
Technical causes	Ransomware
Assets affected	Certification Authority (CA) platform, Generation and validation of signatures/seals platform, Network platform
Comment	Provider suffered a ransomware attack, but no systems supporting trust services were affected. As a precaution all

	systems were disconnected from the network. No certificates had to be revoked.

Incident example 3	
Incident type	A-Core service outage
Service affected	eSignature, eTimestamp
Root cause	System failure
Technical causes	Software bug, configuration issue
Assets affected	Generation and validation of signatures/seals platform, Software
Comment	An issue with configuration of a supporting system led to the loss of availability of the eSignature and eTimestamp services.

Incident example 4	
Incident type	B-Other impact on core service
Service affected	eSignature
Root cause	Malicious action
Technical causes	Malware and viruses
Assets affected	Generation and validation of signatures/seals platform
Comment	The incident concerns the leak of credentials for qualified signatures. The affected qualified certificates were revoked and users informed.

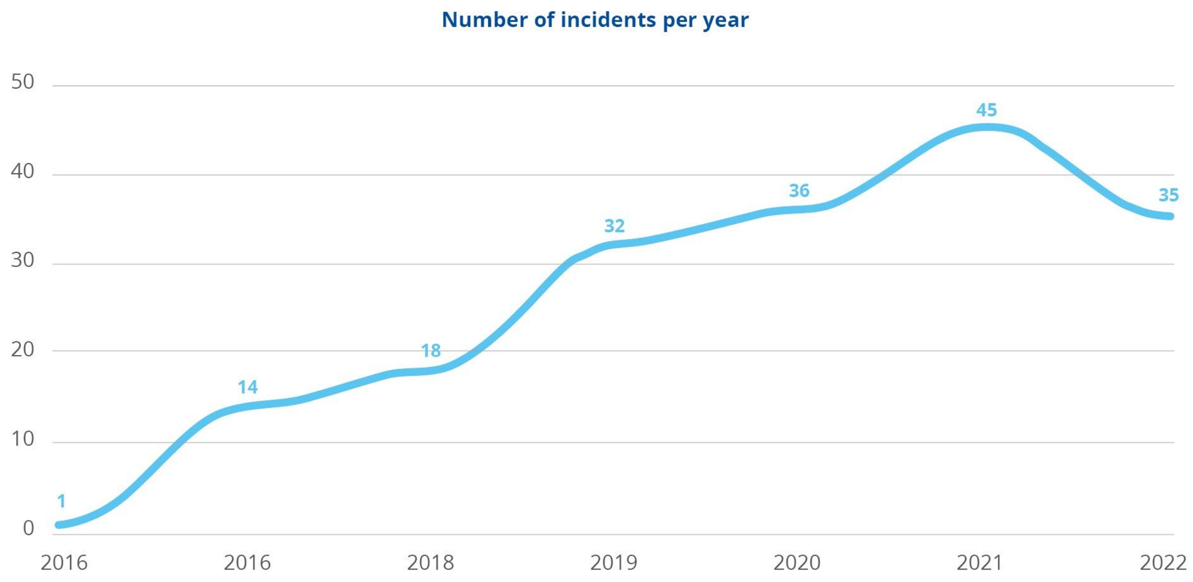
Incident example 5	
Incident type	D-Active threat or vulnerability
Service affected	Generation of signatures/seals platform
Root cause	Human errors
Technical causes	Faulty software change/update

	Malware and viruses
Assets affected	Software
Comment	Potential malware in qualified signature creation device middleware, which was removed immediately after notification.

3. INCIDENT ANALYSIS

The 2022 annual summary reporting, by the 27 EU Member States and 3 EEA countries participating in this process, included in total 35 security incidents[4]. This is the seventh round of annual summary reporting, since eIDAS came into force on the 1st of July 2016.

Figure 1: Number of reported incidents from 2016 - 2022 under Article 19 of the eIDAS regulation



Despite the 25% decrease in reported incidents during 2022, there is a steady stabilisation in the number of incidents reported around 40 per year which, over the years, leans towards becoming linear. This suggests that TSPs are becoming more familiar with the process, with further room for improvement.

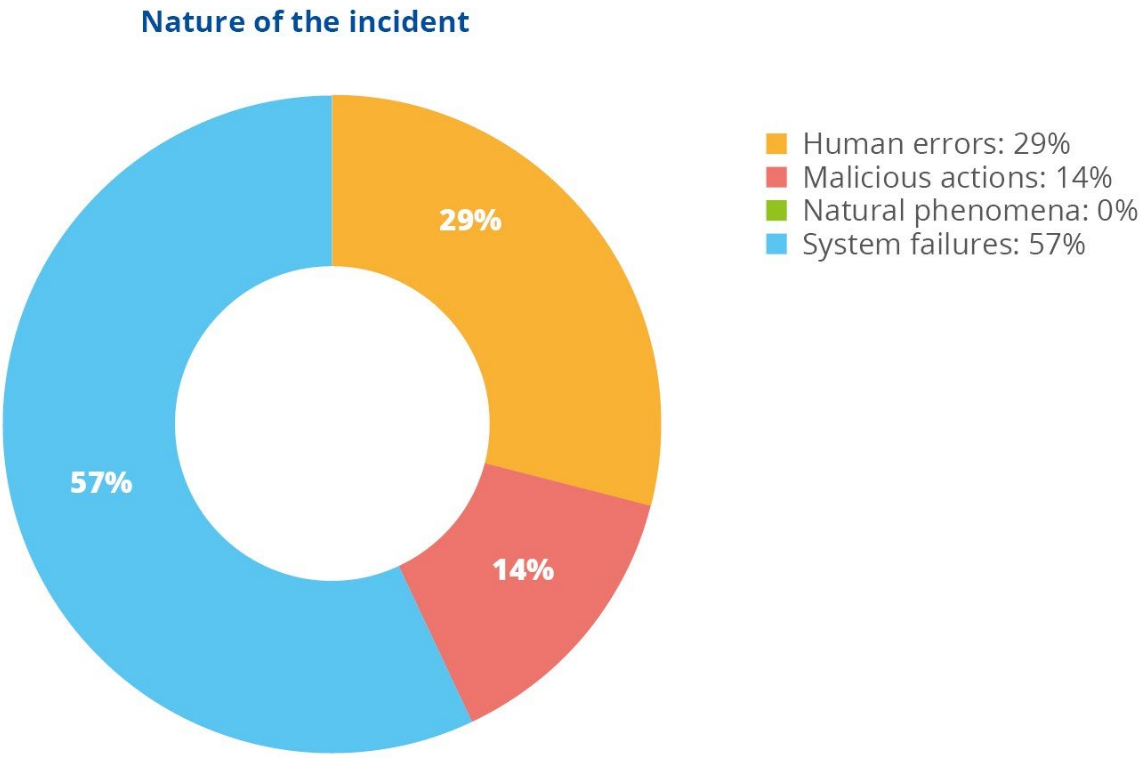
3.1 ROOT CAUSE CATEGORIES

Figure 2 below 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 more than half of total trust services incidents reported (57%, 20 incidents). Typically, system failures are due to either hardware failures or software bugs.
- Almost 29% of incidents were categorised as human errors.
- Around 14% of the incidents were flagged as malicious actions.
- Natural phenomena did not account for any of the reported incidents.

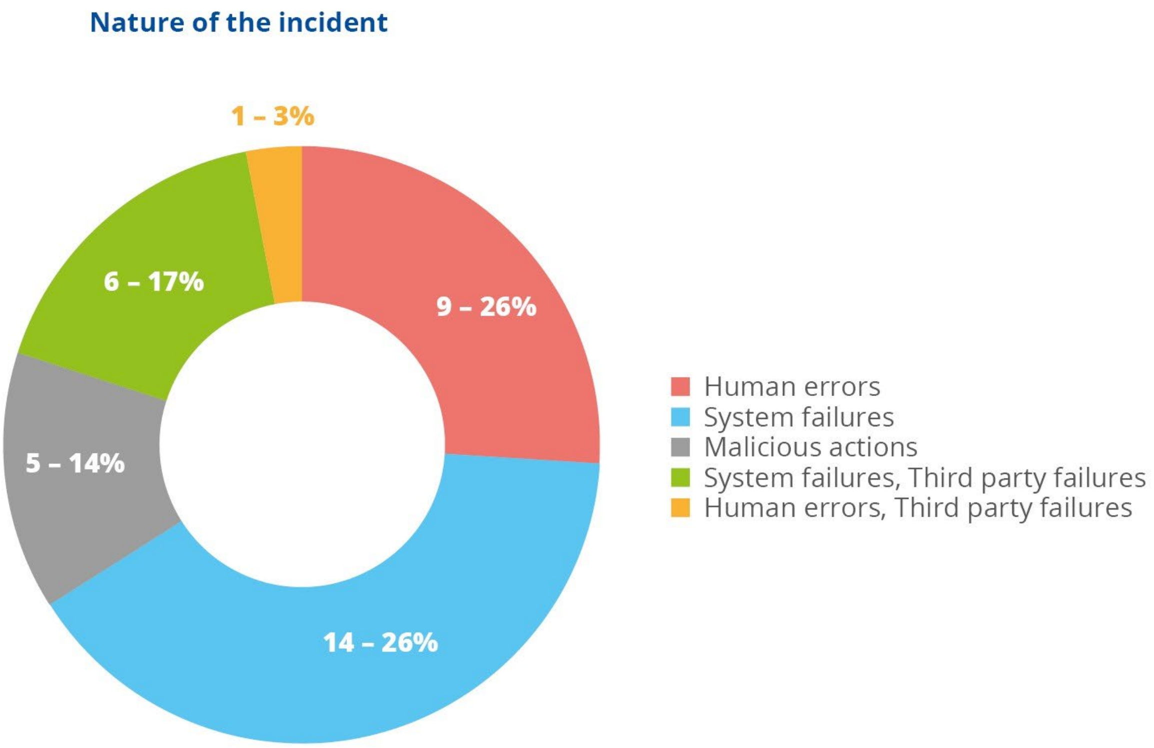
[4] Note that in total 36 incidents were reported, but one of the reported incidents was indicated as type D-Active threats or vulnerabilities and is not included in the analysis.

Figure 2: Root causes of TSP security incidents - 2022



We also keep track of third-party failures, i.e. when the incident really originated at a third party. For 2022, 7 incidents out of 35 (compared to 14 incidents out of 45 in 2021) were flagged as third-party failures (20%), well below the 31,11% of incidents flagged as third-party failures in 2021. This finding reinforces the need to consider supply chain issues when it comes to security, as the increasing expansion and complexity of modern supply chains affects more and more services, despite the apparent drop in reported third-party failure incidents. Out of the 7 third-party failures reported in 2022, 6 were categorized as system failures, and 1 as human error. Figure 3 provides the full picture.

Figure 3: Root causes – third party failures - 2022

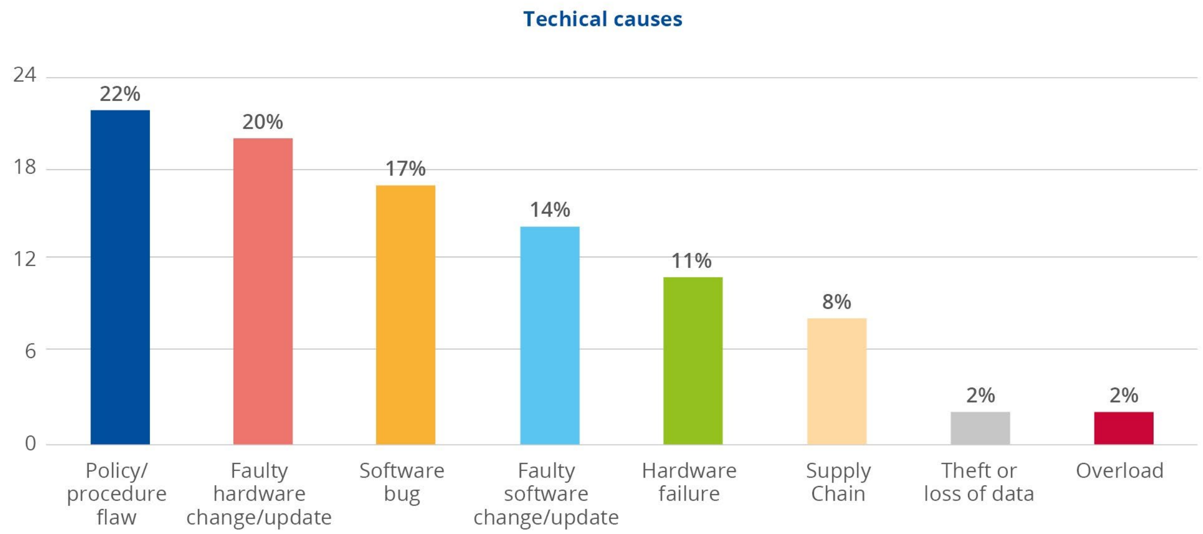


3.2 DETAILED CAUSES

The two most common detailed causes of incidents were flaws in the organization's policy or procedures and faulty hardware changes/updates, with each one accounting for around 20% of the incidents, software bugs (17%), faulty software changes/updates (14%) and hardware failures (11%). Interestingly, 2022 incident reporting witnessed an improvement when it comes to the completeness of provided information, since the 20% undefined nature that was observed in 2021 has completely dissipated. 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). Moreover, supply chain causes that were first introduced in 2021 accounted for 8% of reported incidents in 2022, highlighting the increasing threat caused by supply chains as underlined in the ENISA Threat Landscape for Supply Chain[5] that was published in 2021 (in 2021 only 6% of the incidents were denoted as being supply chain related). The full breakdown of detailed causes[6] for reported incidents may be seen in Figure 4.

[5] See https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
[6] The remaining 4% refers to specific detailed causes such as theft or loss of data (~2%), and overload (~2%).

Figure 4: Detailed causes of trust services security incidents - 2022

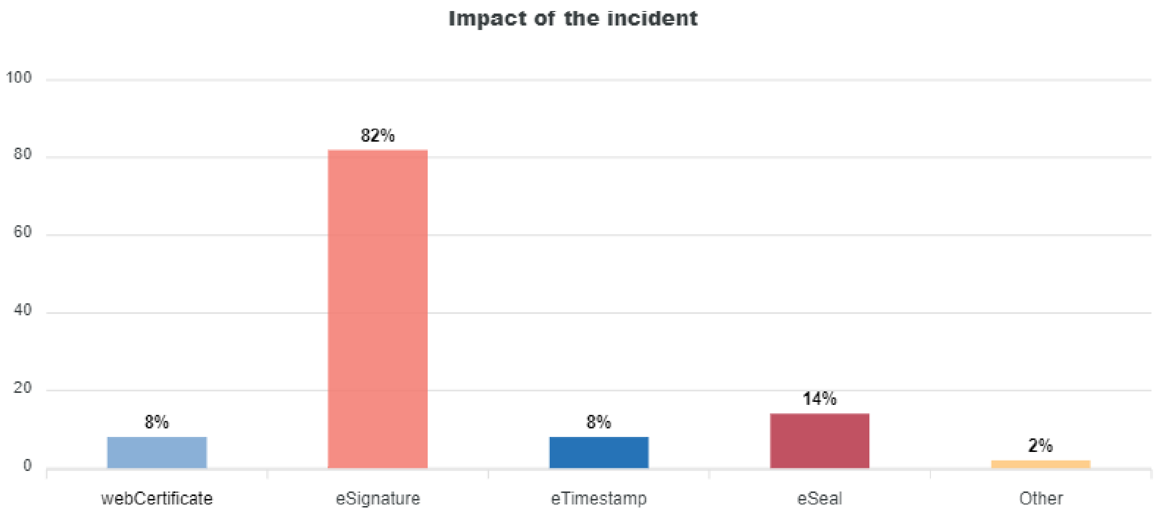


3.3 TYPES OF TRUST SERVICES AFFECTED

Most of the reported incidents (82%) had an impact on electronic signatures as can be seen in Figure 5. This is a notable decrease compared to 91,3% recorded in 2023. Interestingly enough 8% of incidents reported affected web certificates compared to no such incidents reported in 2021. 14% of reported incidents involved electronic seals (19,57% in 2021), and 8% electronic timestamps, the latter exhibiting a 50% decrease compared to 2021 (15,22%). It needs to be noted that several incidents affected multiple services, hence the numbers in the figure correspond to more than 100%. The overall impact of the incidents amounted to 405 million user hours lost, 371 million hours of which reflected human errors.

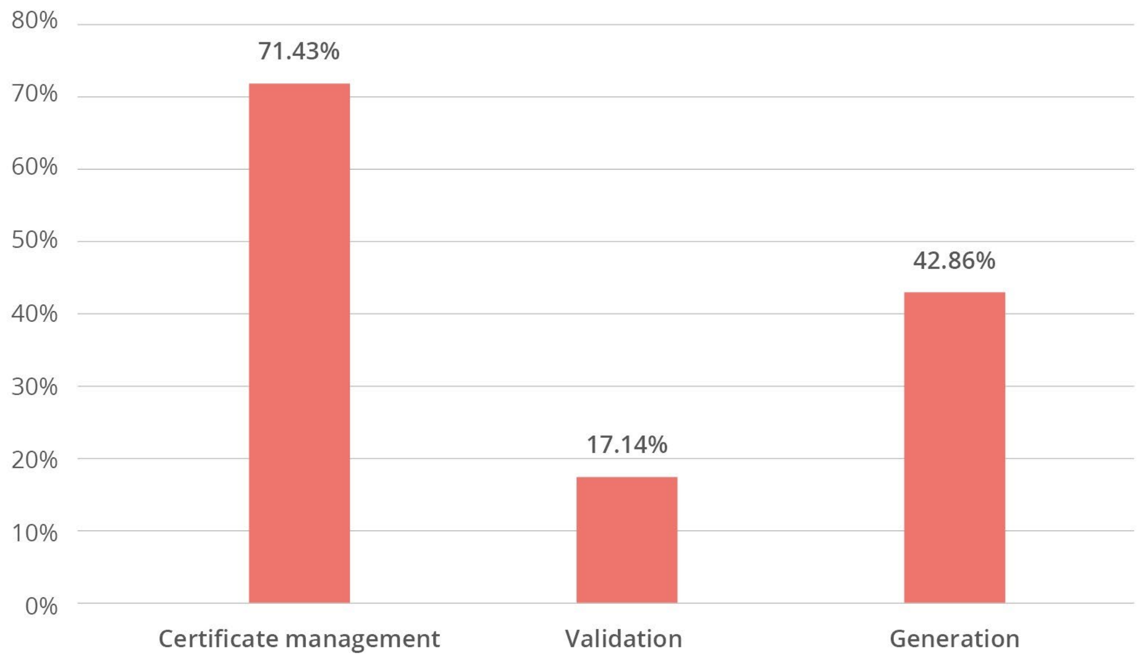
If we look back at the past years of reporting (2016-2022), we see a similar pattern: 82% of all the reported incidents had an impact on electronic signature services, while 20% affected electronic seals and 14% affected timestamping services. In general, most incidents refer to electronic signatures and this may be attributed to their widespread deployment and uptake in comparison to electronic seals and timestamping services.

Figure 5: Impact of incidents on trust services - 2022



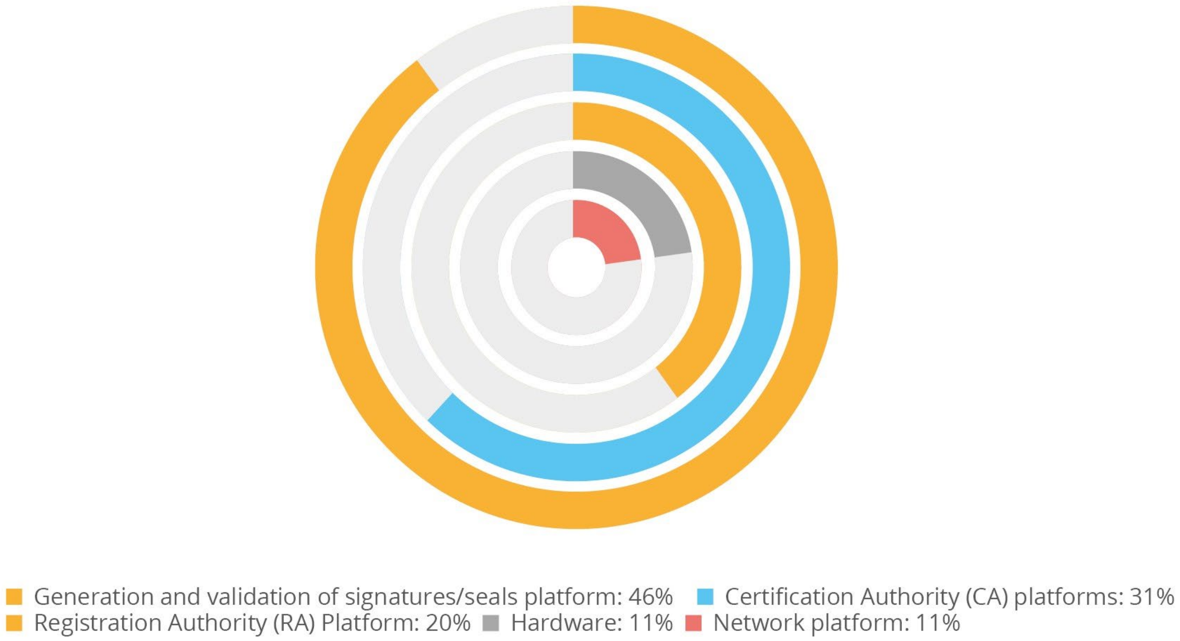
For each incident we keep track of the underlying subservices affected. Most incidents impact the generation of signatures/seals/timestamps (42,86% down from 65,22% in 202) or certificate management (71,43% up from 63,04% in 2021) (see Figure 6). Impact on the validation subservice accounts for 17,14% (up from 15,22% in 2021). Once again, impact on multiple subservices may be reported for incidents, hence the numbers in the figure accounting for more than 100%.

Figure 6: Impact of incidents on subservices - 2022



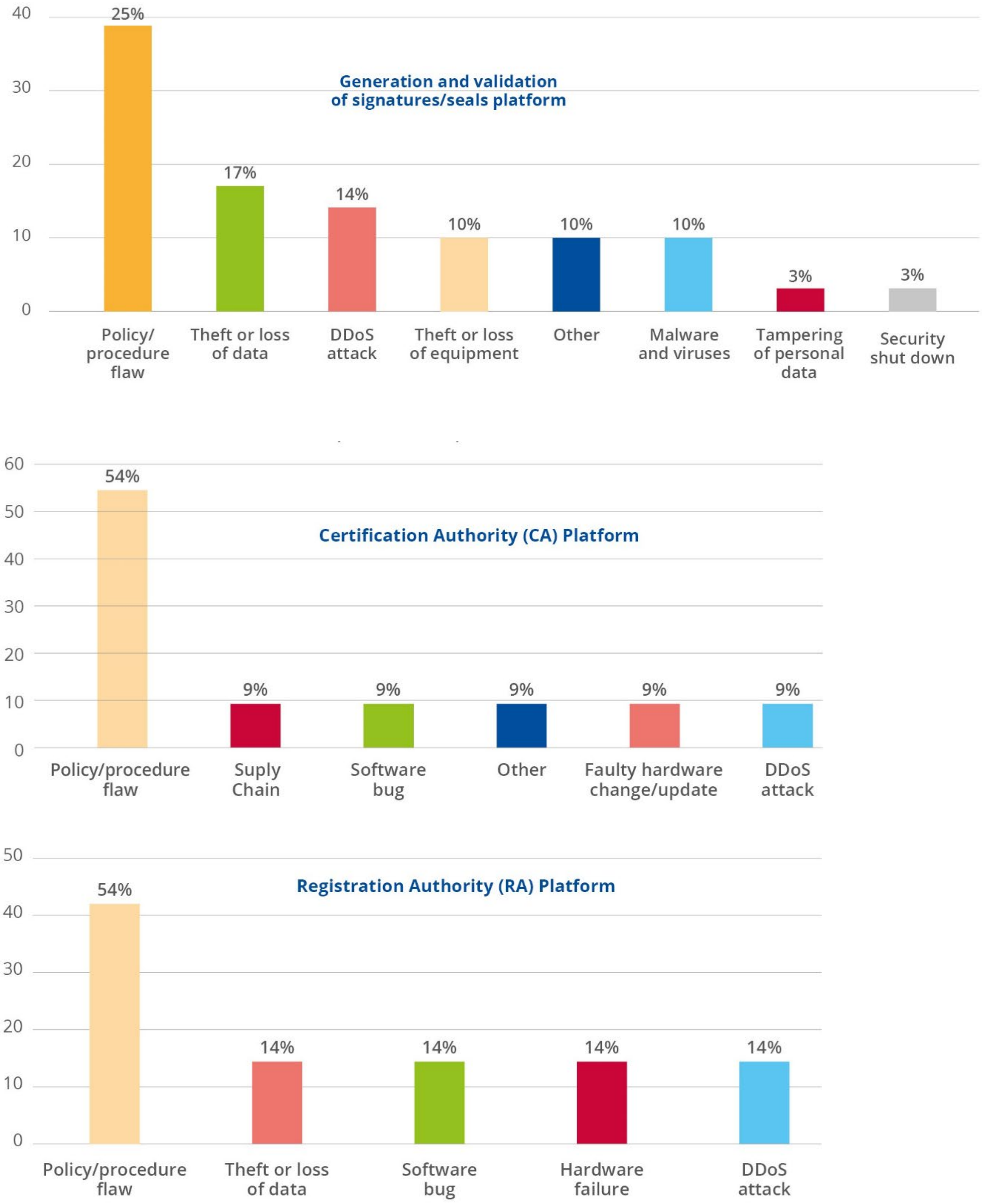
Finally, we also keep track of the underlying assets affected by incidents. In most cases, the assets affected are the platform for the generation and validation of signatures/seals platform (45% compared to 42% in 2021) and the Certification Authority (CA) platform (33% compared to 31% in 2021). Interesting to note that in 20% of the reported incidents (same as in 2021), the affected asset involved the registration authority's platform and in 11% of the cases the network platform (down from 18% in 2021). Hardware assets were affected at a ratio of 11% over the reported incidents. The dispersion of affected assets calls for a holistic approach when it comes to security of trust services, taking into account assets from across the entire lifecycle and supply chain. See the impact on technical assets in Figure 7.

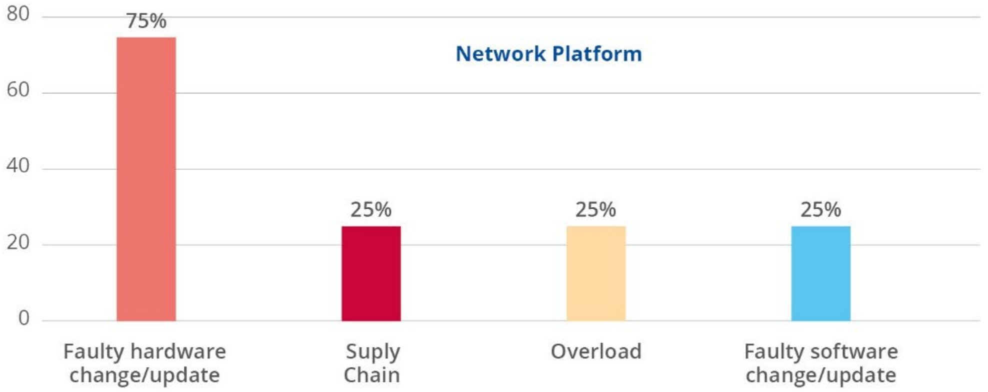
Figure 7: Technical assets affected – TSP security incidents 2022



By delving more into the affected technical assets, one can ascertain noteworthy differences with regard to the corresponding technical causes (see Figure 8). In the case of the platform for the generation and validation of signatures/seals, 25% of the incidents report flaws in policies and procedures as the root cause and 18% software bugs. Conversely, in the case of the Certification Authority's platform, the two main root causes are flaws in processes/procedures (54%) and supply chain, software bugs and DDOS (each one at 9%). The registration platform incidents have a high 42% of flaws in policies and procedures as their root cause, followed by 14% of theft of data and 14% of hardware failures, whereas the network platform has a staggering 75% faulty hardware change/update, 25% faulty software changes, as well as a 25% of overload and 25% of supply chain attacks as root causes. This breakdown is extremely important to understand where emphasis should be prioritised when it comes to targeted security controls in the various technical assets of TSPs.

Figure 8: Breakdown of technical causes per affected asset – TSP security incidents 2022

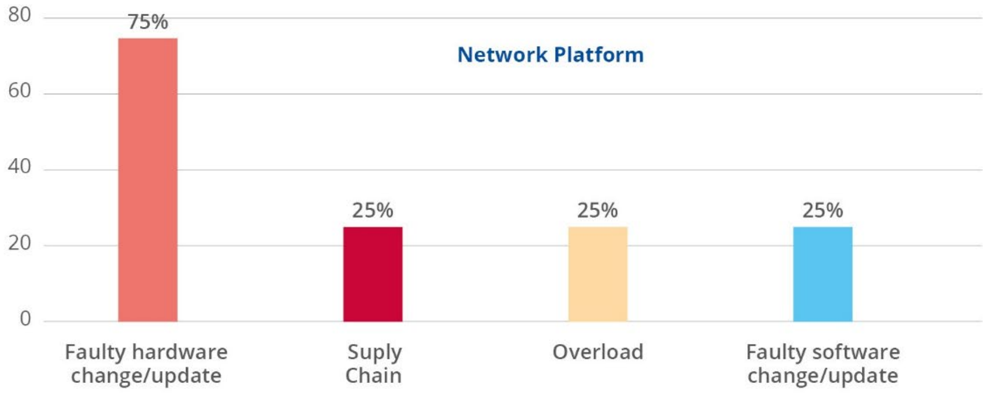


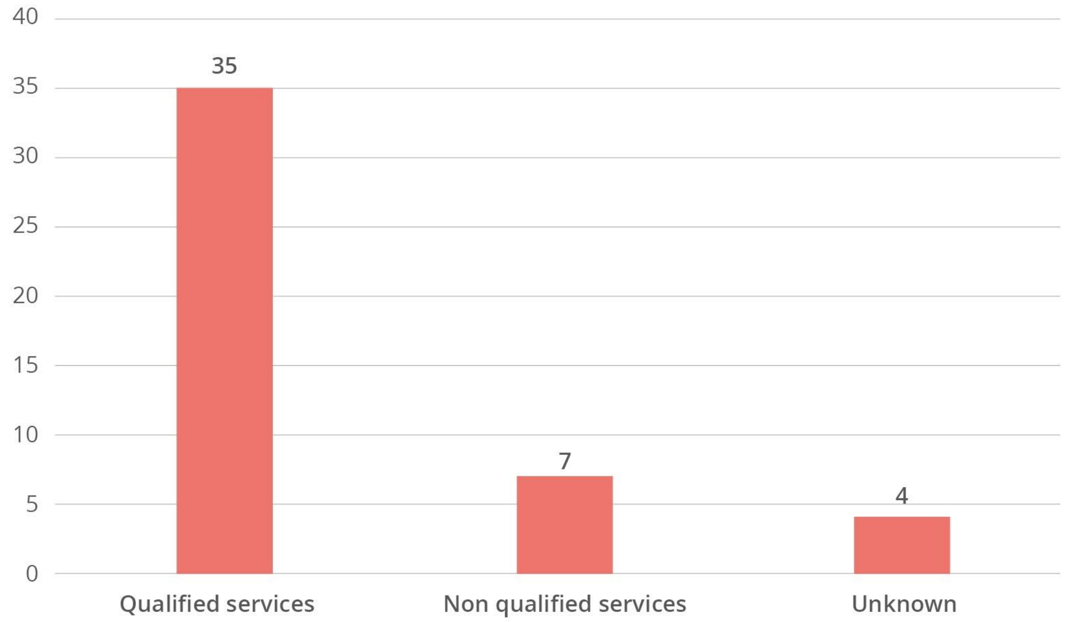


3.4 QUALIFIED SERVICES VERSUS NON-QUALIFIED SERVICES

This year nearly 75% 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 15% of the incidents affected a non-qualified service and for 10% of the incidents no relevant information was reported. Again, it is important to note that one incident report could involve multiple trust services, which explains why the total number of incidents in the Figure 9 below add up to more than 35 (i.e. the total number of 2022 reported incidents).

Figure 9: Reported incidents affecting qualified v non-qualified services - 2022





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 (hence the numbers adding up to more than 100%). 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. Moreover, we need to underline a decrease in the number of non-qualified service incidents being reported, which indicates the need to promote the importance of incident reporting to the respective providers.

4. MULTI-ANNUAL TRENDS 2016-2022

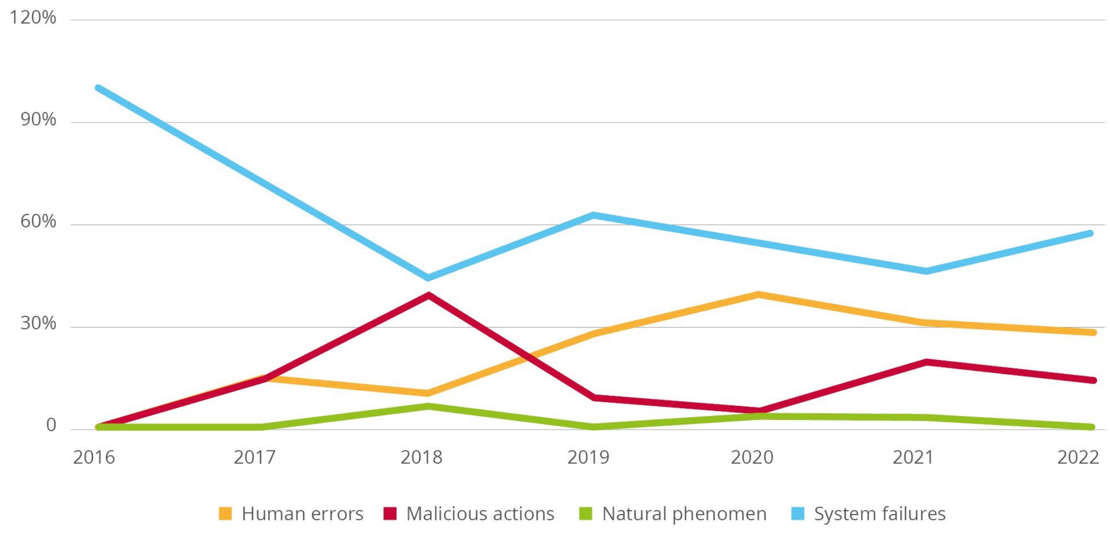
ENISA has been collecting and aggregating trust services incident reports since 2016. In this section, we look at multi-annual trends over the last 7 years, covering the period from 2016 to 2022. The total dataset contains 181 reported incidents.

4.1 MULTI-ANNUAL TREND IN ROOT CAUSE CATEGORIES

Over the last few years of trust services security incident reporting - as displayed in Figure 10 - the most common root cause has been system failures. These add up to 55% as shown in Figure 11, with human errors representing 28% of all reported incidents, 15% involving malicious actions and 2% natural phenomena. One can observe (Figure 10) a relative stabilisation in the number of system failure related incidents over the last 6 years, starting from a peak of 100% in 2016 (first year of trust services annual incident reporting) to a 52,8% in 2020, 46,7% in 2021 and 57,1% in 2022.

Note that we observe the same pattern in electronic communication services[7], where system failures account for almost two thirds (65%) of total incidents (1036 out of 1586 incidents). 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. Accordingly, in the case of natural phenomena as a root cause, consistently low figures are being reported with a peak of 5,6% in 2018 and just 2,2 % being reported in 2021. No such incidents were reported in 2022.

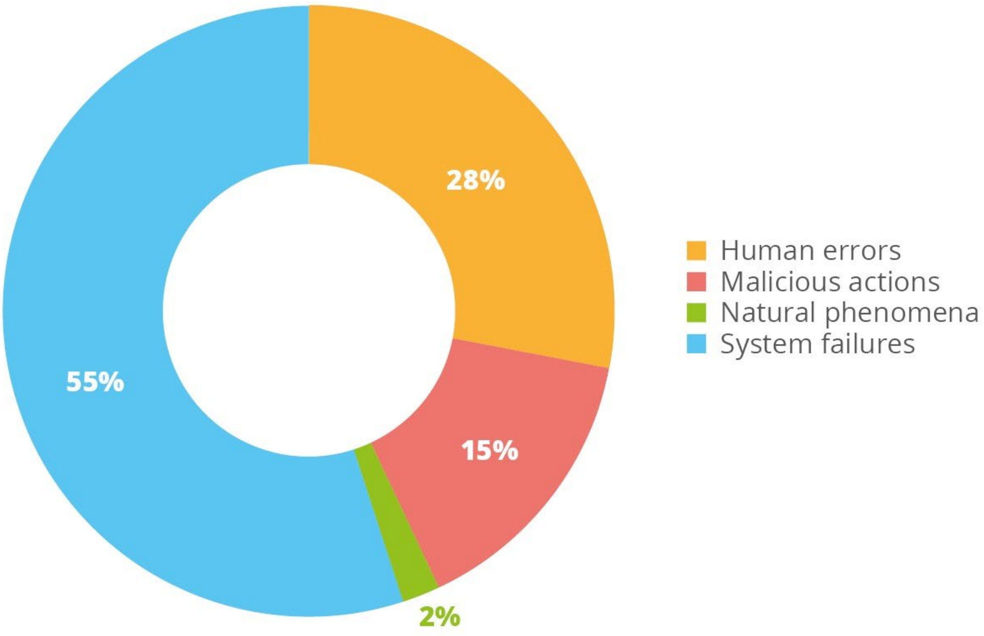
Figure 10: Root cause categories - Trust services security incidents in the EU [reported over 2016-2022]



[7] See https://www.enisa.europa.eu/topics/incident-reporting/for-telcos

Moreover, incidents concerning human errors exhibit an increasing rate of being reported with a slight dip in values of 2022, with 28,1% in 2019, 38,9% in 2020, 31,1% in 2021 and 28,6% in 2022. Malicious actions vary across the years, with the peak observed during 2018 (38,9%) and a value as low as 5,6% during 2020. During 2022, malicious actions were the root cause for 14,3% of the reported incidents.

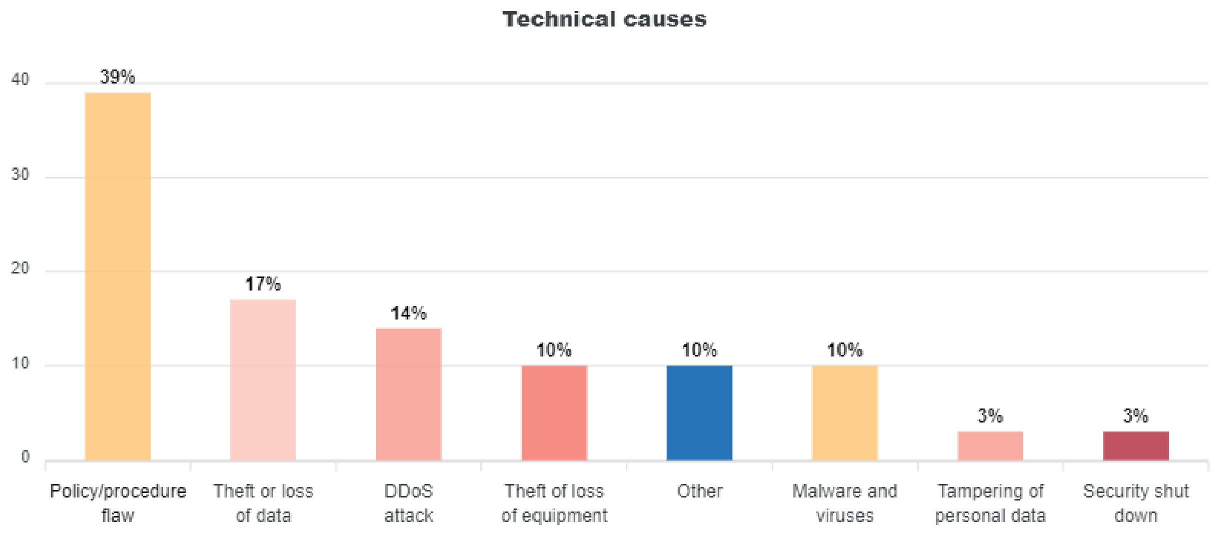
Figure 11: Nature of reported incidents - Trust services security incidents in the EU [reported over 2016-2022]



In particular for the incidents reported under the malicious actions category, the most common detailed causes over the years as shown in Figure 12 were policy/procedure flaws (39%), theft/loss of data (17%), DDoS attacks (14%), theft/loss of equipment (10%), malware (10%) and tampering of personal data (3%). It is interesting to contrast these findings with the latest version of the ENISA Threat Landscape[8] and the identified prime threats (threats against data, malware, threats against availability, non-malicious threats, etc.). Despite the low number of incidents reported in the field of trust services, there is an alignment with the findings of the ENISA Threat Landscape, which illustrates the representative nature of trust services security incident reporting.

[88] See https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Figure 12: Detailed technical causes - Trust services security incidents in the EU [reported over 2016-2022]



4.2 MULTI-ANNUAL TREND IN SEVERITY OF IMPACT

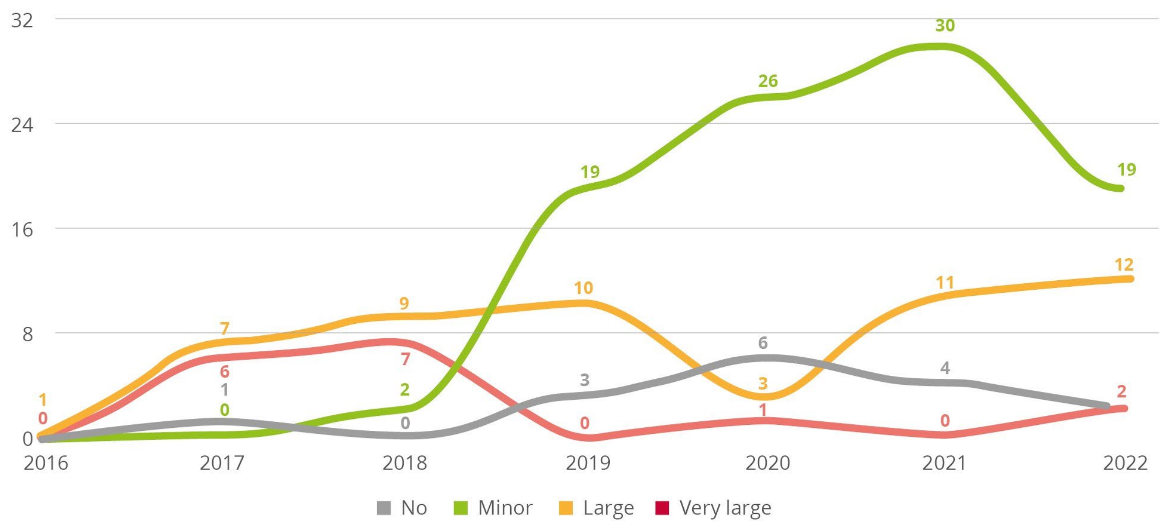
In the multi-annual trend concerning the severity of impact, the EU Cybersecurity incident taxonomy is again followed where the severity of the impact has the following values: no impact, minor, large and very large impact[9].

While comparing the statistics for severity since 2016 (Figure 13), it is quite clear that the number of incidents with large impact increased slightly over the course of 2022 compared to the drop that was observed in 2020 (also taking into account the smaller number of incidents reported overall). It seems that the drop that was observed in 2020 was the outlier, and a circa 25% of incidents every year are reported as having large impact. It is interesting to see that there is a rather linear increase in minor incidents over the course of the last years, with a significant drop in 2022 values that is attributed to an equivalent drop in the overall number of reported incidents.

This is again an indication that the incident reporting mechanism has become more familiar to trust services providers and also more effective; providers are in general reporting more incidents regardless of their severity. In contrast to 2018, there were no very large (i.e. disastrous) incidents during 2019 and 2021 (only 1 such incident reported in 2020), whereas 2 such incidents were reported in 2022.

[9] See http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53646

Figure 13: Severity of impact - Trust services security incidents in the EU [reported over 2016-2022]

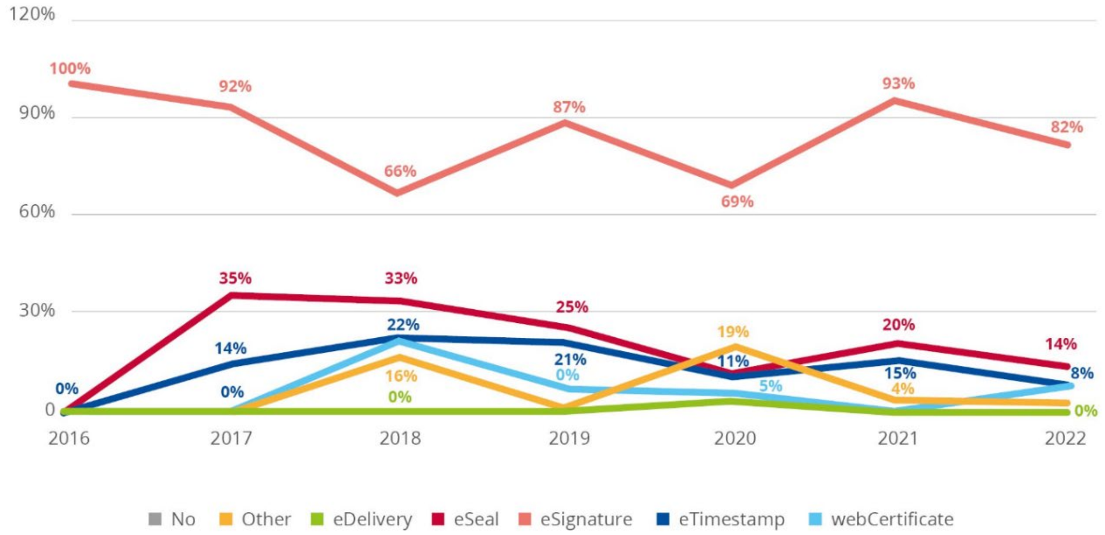


4.3 MULTI-ANNUAL TREND IN IMPACT ON SERVICES

When considering impact per service during the course of 2016-2022 for reported incidents for trust services, Figure 14 provides the overview. It is evident that the majority of reported incidents relate to electronic signatures, with numbers ranging consistently above 66% (2018) and reaching the peak of 100% in 2016 and 82% in 2022.

Electronic seals and electronic timestamps are the services that are affected second and third most respectively, whereas it is interesting to note the consistently low values for web certificates and electronic delivery services. The latter two categories require further attention to explore the reason for the low number of reported incidents, to investigate whether this is due to reduced usage of the services, better security provisions or lack of maturity for reporting of such incidents.

Figure 14: Impact on services - Trust services security incidents in the EU [reported over 2016-2022]



5. CONCLUSIONS

The key takeaways from the 2022 incidents are:

- **The number of incidents with a large impact has slightly increased:** in 2022, 12 incidents with large impact were reported, continuing the trend observed over the past years. By comparison, in 2020 only 3 incidents were characterized as having had a "large impact" as opposed to 2021 when 11 such incidents had been reported (translating into approximately a quadruple increase). Additionally, 2 very large impact incidents were reported in 2022.
- **Qualified trust services versus non-qualified trust services:** In 2022, 75% of total incidents had an impact on qualified trust services when compared with approximately 15% of incidents reported on non-qualified trust services and 10% of incidents having provided no relevant information. 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. It needs to be highlighted that in 2021 significant improvement in this particular area was noted compared to 2020 when the observation was first made, and this trend persists in 2022. This is a testament to the value of the work on incident reporting and the relevant analysis, which had a direct positive impact on the overall process. However, we need to highlight the 10% of reported incidents lacking this very piece of information: providing accurate and complete information on reported incidents is essential for proper analysis and follow-up actions.
- **Root causes for malicious actions are consistent with the findings of the 2022 ENISA Threat Landscape**. Despite the relatively low number of incidents reported in the field of trust services, there is an alignment with the findings of the ENISA Threat Landscape, which illustrates the representative nature of trust services security incident reporting.

We conclude with some other observations:

- **Reporting of threats/vulnerabilities in 2022:** in 2022, authorities reported only one threat/vulnerability, same as in 2021. This threat on video identification of identification providers, which is not under the control of a TSP and therefore can hardly be supervised, was reported as type D-incidents/vulnerabilities. While challenging for authorities to report such threats or vulnerabilities, the importance of information sharing cannot be understated, in particular when it comes to malicious actions. Early warnings and best practices on how to address malicious actions can greatly help mitigate them and thus reduce the impact of potential incidents. It can also serve as a great example of peer learning between authorities, learning from one another on how best to mitigate potential threats.
- **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 very few reports about incidents with non-qualified trust services suggests there is still under-reporting in this area, although 7 purely non-qualified trust services incidents were reported in 2022, thus showing growing maturity.
- **EU policy changes:** eIDAS regulations and eIDAS incident reporting have been in place for more than five years now and eIDAS is currently under review. The Commission is discussion the revision of the eIDAS Regulation. In 2022, with the advent of the revised NIS (Network and Information Security) Directive 2, incident reporting under Article 19 of eIDAS is repealed and relevant incident reporting will follow the guidelines and process of NIS2 as of October 17th 2024. 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 and contributing to consolidated incident reporting under NIS2.

TP-AK-20-001-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

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 978-92-9204-654-5
doi: 10.2824/65720