EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ANNUAL REPORT TRUST SERVICES SECURITY INCIDENTS 2023

DECEMBER 2024

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) is working to make Europe cyber secure since 2004. ENISA works with the EU, its Member States, the private sector and Europe's citizens 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 content queries about this report, please email incidentreporting@enisa.europa.eu
For media enquiries about this paper, please email press@enisa.europa.eu

AUTHOR

Marie-Laure Lulé, ENISA

ACKNOWLEDGEMENTS

We are grateful for the review and input received from ENISA European Competent Authorities for Trust Services. ECATS Expert Group comprises experts from 30 national supervisory bodies in the EU Member States, EFTA, EEA and EU candidate countries. The group is currently chaired by a representative of RTR Austria.

LEGAL NOTICE

COPYRIGHT NOTICE

TP-01-24-007-EN-N, ISBN: 978-92-9204-684-2, DOI: 10.2824/9574029

TABLE OF CONTENTS

1. INTRODUCTION 5

1.1 SCOPE 5

1.2 EIDAS REGULATION 5

1.3 DISCLAIMER 5

1.4 STRUCTURE 5

2. INCIDENT REPORTING FRAMEWORK 6

2.1 OVERVIEW OF INCIDENT REPORTING PROCESS 6

2.2 INCIDENT REPORTING TOOL 7

2.3 ANONYMISED EXAMPLES OF SECURITY INCIDENTS 8

3. INCIDENT ANALYSIS 10

3.1 ROOT CAUSE CATEGORIES 10

3.2 DETAILED CAUSES 11

3.3 TYPES OF TRUST SERVICES AFFECTED 12

3.4 QUALIFIED SERVICES VERSUS NON-QUALIFIED SERVICES 16

4. MULTIANNUAL TRENDS 2016–2023 17

4.1 MULTIANNUAL TREND IN ROOT CAUSE CATEGORIES 17

4.2 MULTIANNUAL TREND IN SEVERITY OF IMPACT 19

4.3 MULTIANNUAL TREND IN IMPACT ON SERVICES 20

5. CONCLUSIONS 22

EXECUTIVE SUMMARY

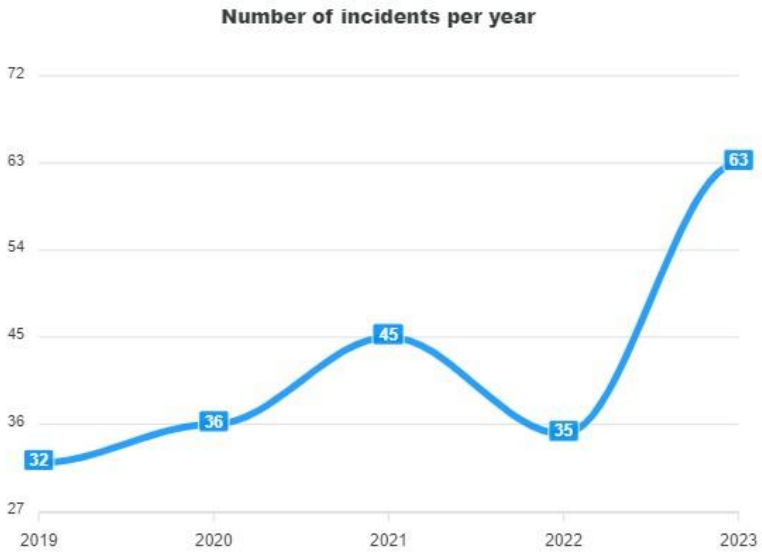
Every year national supervisory bodies must send annual summary reports about the notified breaches to ENISA and the Commission.

ENISA's 2023 report on trust services security incidents provides the seventh round of security incident reporting for the EU's trust services sector, analysing root causes, statistics and trends. It is an aggregated overview of the reported breaches for 2023 as conveyed to ENISA and the Commission by 27 EU Member States and 3 EEA countries.

In 2023, a total of **63 incidents** were reported and analysed (1).

Key findings from the 2023 incident reports are summarised in the following list of points.

- Two thirds of EU supervisory bodies (SBs) – **18** out of 27 – sent their respective reports with 0 incidents reported (2).
- Reported incidents **increased by 80 %** to a total of 63 incidents, compared with 35 in 2022 (3).
- The number of incidents caused by **malicious actions** – 9 – has increased since 2022 – 5 –, reaching the same level as in 2021. However, with **14 %** of the total, it remains a constant percentage since 2022 for this root cause.
- The overall impact of the incidents amounted to **3 184 million user hours lost**, compared with 405 million in 2022. **3 140 million hours were lost due to malicious actions, amounting to 98 % of the total** (4). One million hours were lost due to system failures and 43 million hours due to human errors (5).



Highlights 2023

The number of reported incidents increased by 80 %.

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

As in previous years, most reported incidents concern qualified certificates (95 %).

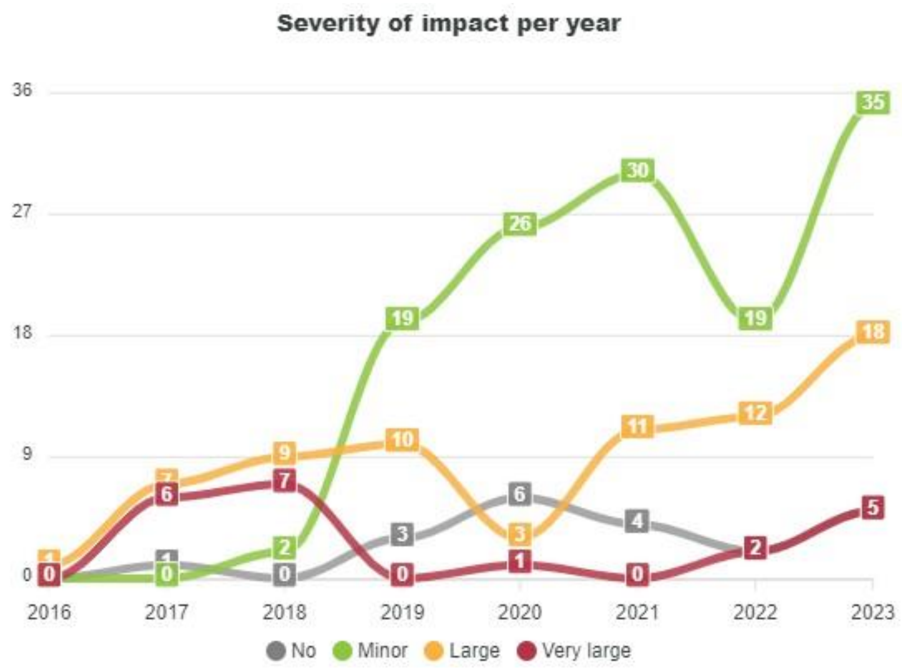
System failures account for more than half of incidents and have been the dominant root cause for the last 8 years of incident reporting.

2023 witnessed an increase in the number of incidents caused by malicious actions affecting, in particular, the number of user hours lost (98 %).

(1) One type D incident, which is not analysed here, was reported under eIDAS in 2023. Type D: threat or vulnerability. For instance, the discovery of a cryptographic weakness would be categorised as a type D incident.
(2) 2022:13/27; 2021: 17/27; 2020: 19/27; 2019: 17/27; 2018: 18/27; 2017: 17/27; 2016: 26/27.
(3) Among them, 46 incidents occurred in 9 EU SBs and 21 in SBs from EEA countries.
(4) In 2022 it was 0 million.
(5) In 2022 it was 34 million and 371 million, respectively.

- In terms of **impact**, in all four categories – no impact, minor, large, very large – the number of incidents almost **doubled**:

    - in 2023, 5 incidents with no impact were reported, 35 with minor impact, 18 large incidents and 5 very large incidents;
    - the number of incidents with minor impact has almost doubled compared with 2022, but remains in line with data from previous years;
    - the number of large and very large incidents has continued to increase.



1. INTRODUCTION

1.1 SCOPE

Under Article 19 of the eIDAS regulation ([6]), trust service providers (TSPs) in the EU have to notify their national supervisory bodies of any security incidents. The supervisory bodies send summaries of these incident reports to the European Union Agency for Cybersecurity (ENISA) on an annual basis. Subsequently, ENISA publishes an aggregated overview of the reported security incidents.

ENISA publishes detailed statistics about trust services security incidents in an online visual tool, ENISA's cybersecurity incident reporting and analysis system (CIRAS) ([7]). This tool allows for a custom analysis of trends and patterns and supports the quantitative and qualitative analysis of the data collected.

This document gives an aggregate overview of the security incident reports submitted by the supervisory bodies during 2023. This annual report marks the seventh round of security incident reporting in the EU's trust services sector, covering security incidents that occurred in 2023.

1.2 EIDAS REGULATION

The EU Regulation 910/2014 (eIDAS) sets rules for electronic identity schemes and trust services in Europe, national electronic identification schemes, cross-border interoperability and recognition. Article 19 sets the obligation for qualified and non-qualified trust service providers (TSPs) to report 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.

The eIDAS regulation **aims** to:

- ensure that electronic signatures can have the same legal standing as traditional signatures;
- remove barriers to electronic commerce and all types of electronic transactions in the EU, with a view to building 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.

1.3 DISCLAIMER

As per Article 19, this document only contains aggregated and anonymised information about incidents and does not include details about individual countries or individual TSPs.

1.4 STRUCTURE

This document is structured as follows:

- Section 2 briefly reviews the processes, incl. CIRAS tool and describes anonymised examples of reported incidents;
- Section 3 presents the categories of root causes, the detailed causes and the affected services;
- Section 4 describes the multiannual trends in incidents from 2016-2023;
- Section 5 draws conclusions and observations based on the available datasets.

(6) 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
https://eur-lex.europa.eu/eli/reg/2014/910/oj
(7) https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool
https://ciras.enisa.europa.eu/

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 TSPs in the EU to:

1) assess risks;

2) take appropriate security measures to mitigate security breaches; and

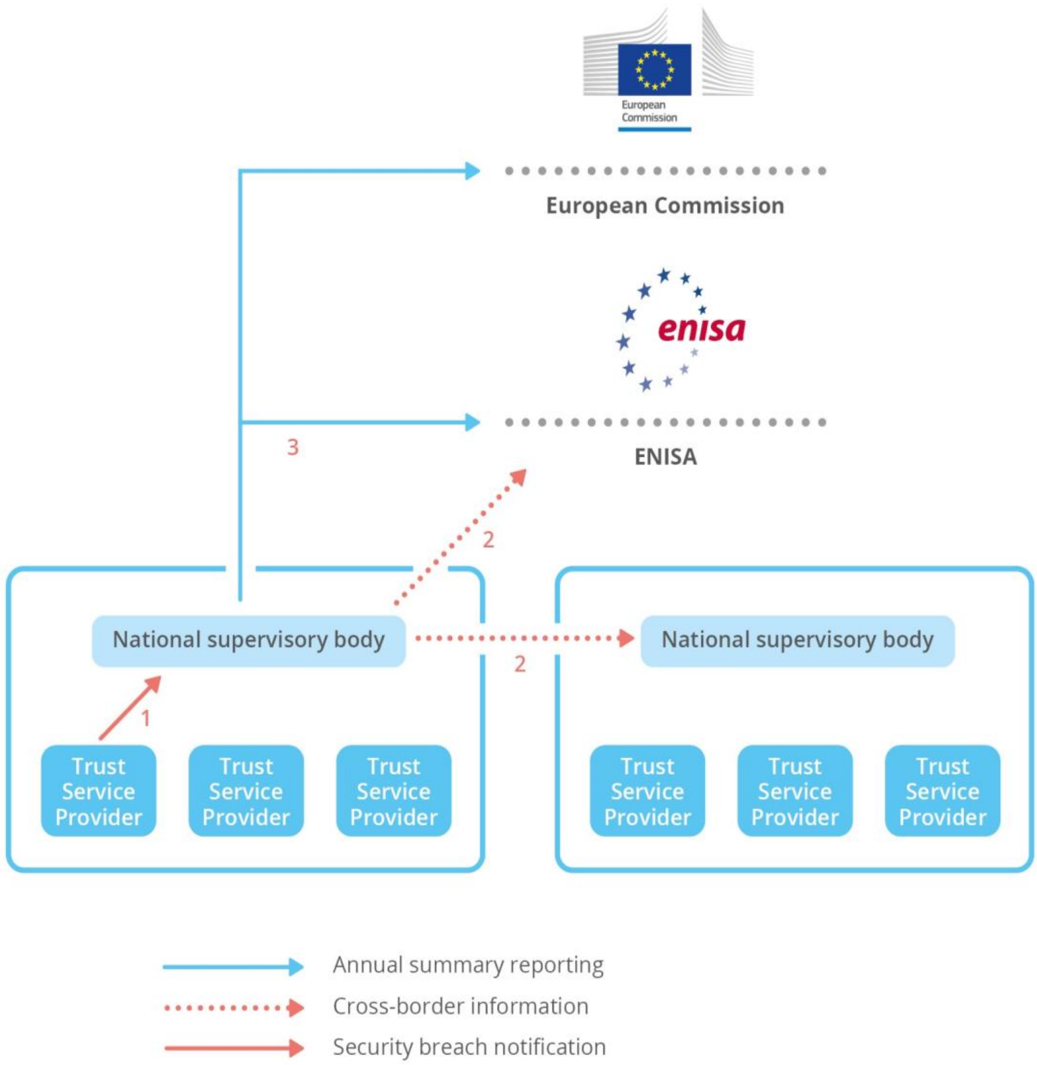
3) report breaches to national supervisory bodies.

2.1 OVERVIEW OF INCIDENT REPORTING PROCESS

The mandatory security breach notification process has three steps, as displayed in **Figure A**.

1. TSPs 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 reported breaches to ENISA and the Commission.

Figure A. Security breach notification process



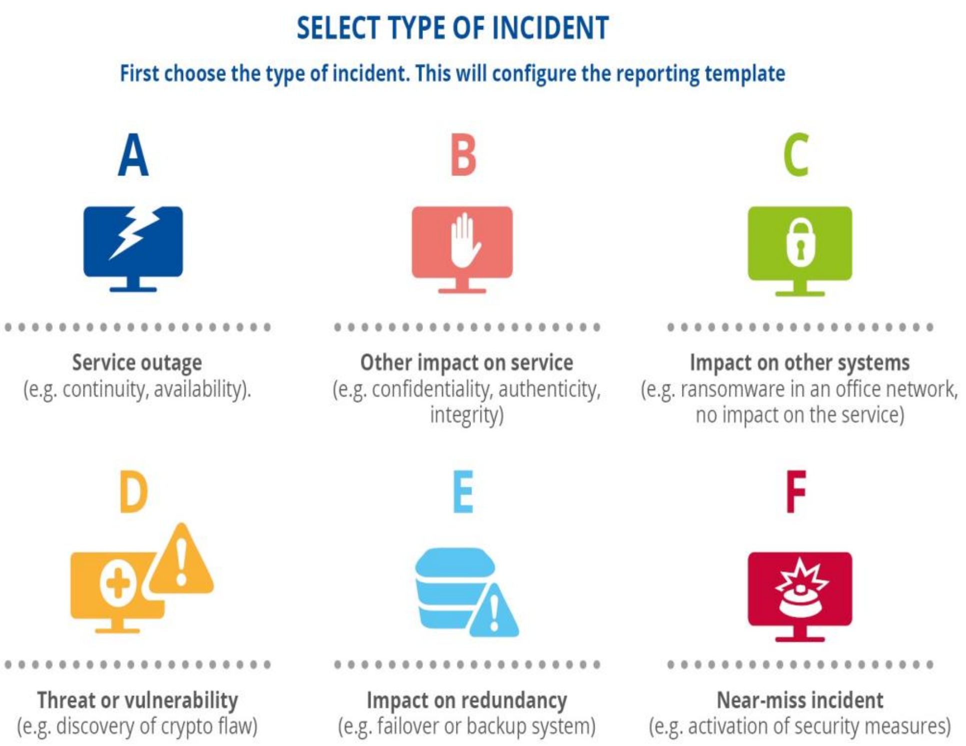
2.2 INCIDENT REPORTING TOOL

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

ENISA reporting 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: short description, types of services and assets, severity level, etc.

Figure B. Incident reporting tool



- **Type A**: service outage (e.g. continuity, availability). For example, an outage caused by a cable being cut by 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 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, malware is 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 ANONYMISED EXAMPLES OF SECURITY INCIDENTS

In this paragraph, some kinds of incidents that are reported are presented by providing detailed and anonymised examples.

Incident example 1	
Incident type	A – core service outage
Service affected	e-signature, e-seal, e-timestamp
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 e-signature/e-seal/e-timestamp services due to a backend system overload.

Incident example 2	
Incident type	A – core service outage
Service affected	e-signature, e-seal
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	e-signature, e-timestamp
Root cause	System failure
Technical causes	Software bug; configuration issue
Assets affected	Generation and validation of signatures/seals platform; software
Comment	An issue with the configuration of a supporting system led to the loss of availability of the e-signature and e-timestamp services.

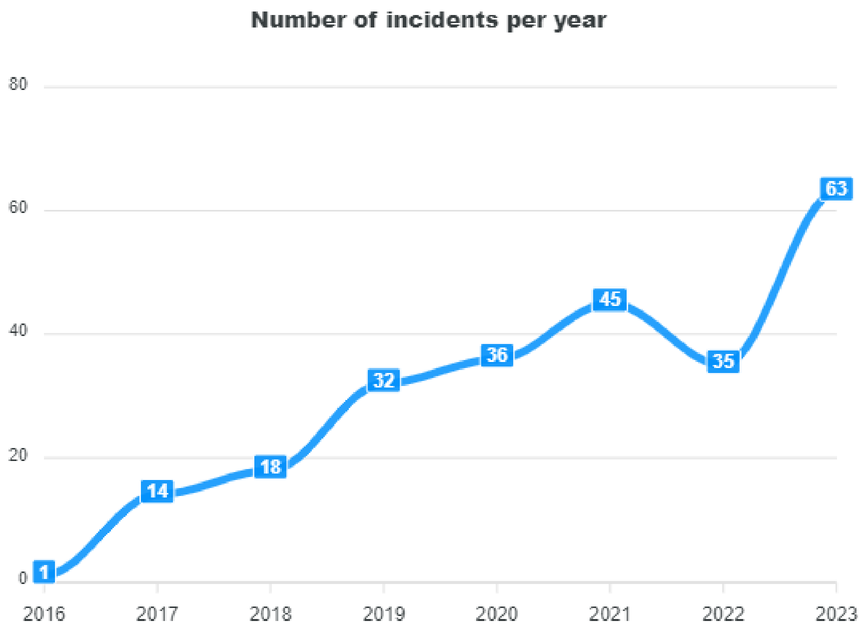
Incident example 4	
Incident type	B – other impact on core service
Service affected	e-signature
Root cause	Malicious actions
Technical causes	Malware and viruses
Assets affected	Generation and validation of signatures/seals platform
Comment	The incident concerns the leak of credentials for qualified 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 2023 annual summary reporting, by the 27 EU Member States and 3 EEA countries participating in this process, included in total 63 security incidents. This is the seventh round of annual summary reporting since eIDAS came into force on 1 July 2016.

Figure 1. Number of reported incidents from 2016–2023



In 2023, the number of incidents increased by 80 %, despite the 25 % decrease in reported incidents in 2022. However, this 2023 data is aligning with the trend observed over the period analysed.

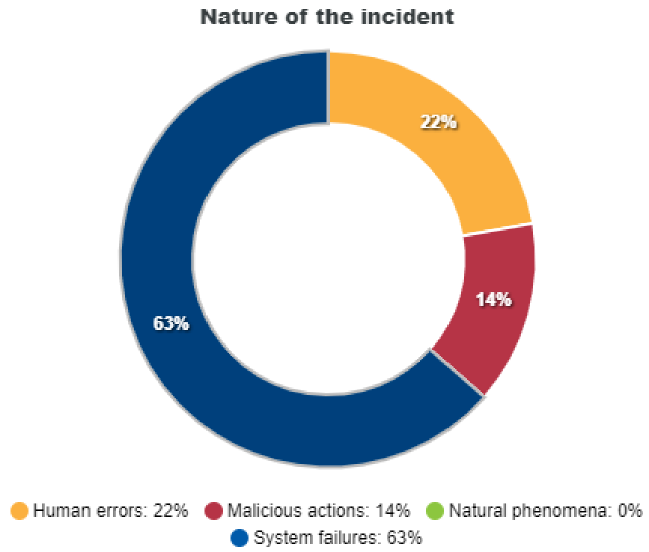
3.1 ROOT CAUSE CATEGORIES

Figure 2 shows the distribution of the incidents according to their underlying root cause.
The overall impact of the incidents amounted to **3 184 million user hours lost**, one million hours of which reflected system failures, 43 million hours human errors and **3 140 million hours malicious actions**.

Incidents are divided into four categories of root causes.

- **System failures** continue to be the dominant root cause, accounting for more than half of total trust services incidents reported (63 %, 40 incidents). Typically, system failures are due to either hardware failures or software bugs.
- With 14 incidents, 22 % of incidents were categorised as being caused by **human errors**.
- With nine incidents, 14 % of the incidents were flagged as **malicious actions**.
- **Natural phenomena** did not account for any of the reported incidents.

Figure 2. Root causes of TSP security incidents – 2023



We also keep track of **third-party failures**, i.e. when the incident really originated from a third party, with a view to assessing the impact on the supplier or the provider. For 2023, 19 incidents out of 63 were flagged as third-party failures (33 %). Out of those reported in 2023:

- **15 out of 19** were categorised as **system failures** (40);
- **2 out of 19** were categorised as being caused by **human errors** (14); and
- **2 out of 19** were categorised as **malicious actions** (9).

3.2 DETAILED CAUSES

It is important to note that an incident is often not only triggered by one cause ([8]) but by multiple detailed causes (i.e. a chain of events).

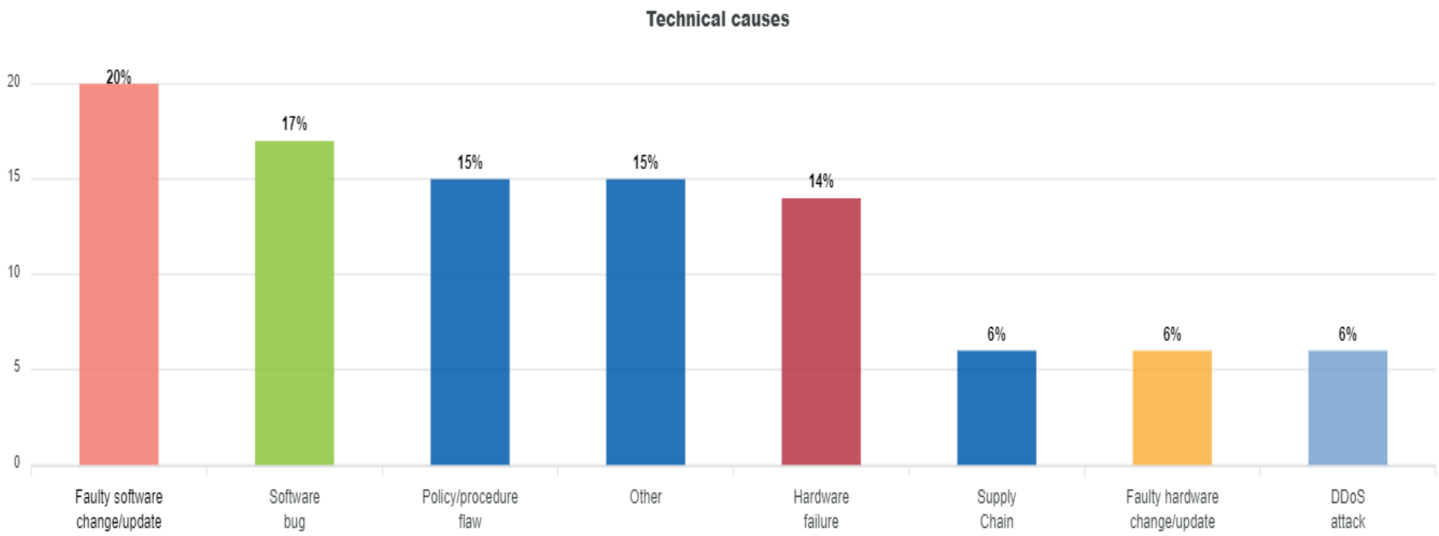
The two most common detailed causes of incidents in 2023 were **faulty software changes/updates** (20 %) and **software bugs** (17 %). Flaws in the organisation's policy or procedures and **faulty hardware changes/updates** each account for around 15 % of the incidents, and **hardware failures** for 14 %. Note that the category 'Other' with 15 % is not defined in the dataset.

Moreover, **supply-chain** causes ([9]), which were first introduced 2 years ago, accounted for **6 %** of reported incidents in 2023 (8 % in 2022). A percentage equivalent was found for the faulty hardware change/update and distributed denial-of-service (DDoS) attacks.

The full breakdown of detailed causes for reported incidents can be seen in **Figure 3**.

([8]) 'Other' is not defined here.
([9]) See ENISA Threat Landscape for Supply Chain Attacks (2021) https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.
In 2022 only 8 % of the incidents were denoted as being supply-chain-related (6 % in 2021).

Figure 3. Detailed causes of trust services security incidents – 2023



3.3 TYPES OF TRUST SERVICES AFFECTED

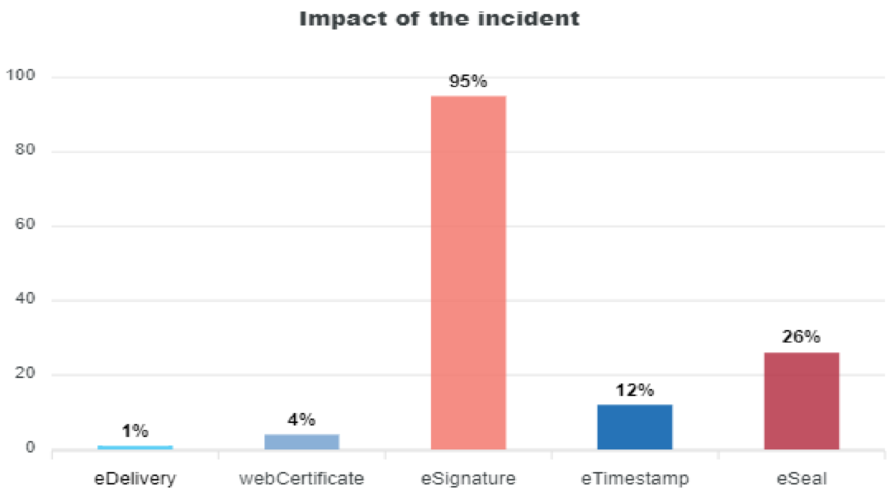
The most commonly affected services are e-signatures, e-seals and e-stamps.

Most of the reported incidents (**95 %**) had an impact on **electronic signatures** ([10]), as can be seen in **Figure 4**, compared with 82 % in 2022. Among them, 65 % were related to system failures, 22 % to human errors and 13 % to malicious actions.

Interestingly, **26 %** of incidents reported affected **electronic seals** ([11]), compared with 14 % in 2022. Among them, 76 % were related to system failures, 12 % to human errors and 12 % to malicious actions.

Electronic timestamps make up **12 %** of the total.

Figure 4. Impact of incidents on trust services – 2023



([10]) Article 3(10) 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.
([11]) Article 1(25) 'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.

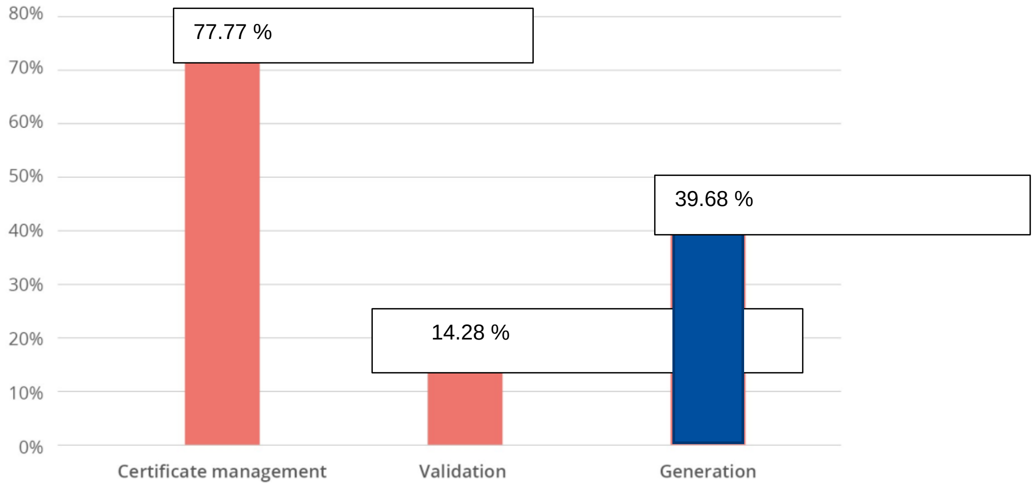
Please note that several incidents affected multiple services, hence the numbers in the figure adding up to more than 100 %.

In **Figure 5**, for each incident we kept track of the **underlying subservices affected** in 2023, i.e. certificate management, validation and generation of signatures/seals/timestamps.

- Incidents most frequently affected **certificate management**: 49 of 63, representing 77.77 % (71.43 % in 2022 and 63.04 % in 2021).
- Incidents affecting the **generation** of signatures/seals/timestamps continued to decrease, reaching 39.68 % (42.86 % in 2022).
- Incidents affecting the **validation** subservice accounted for 14.28 % of the total in 2023 (17.14 % in 2022 and 15.22 % in 2021).

Once again, impact on multiple subservices may be reported for incidents, hence the numbers in **Figure 5** adding up to more than 100 %.

Figure 5. Impact of incidents on subservices – 2023

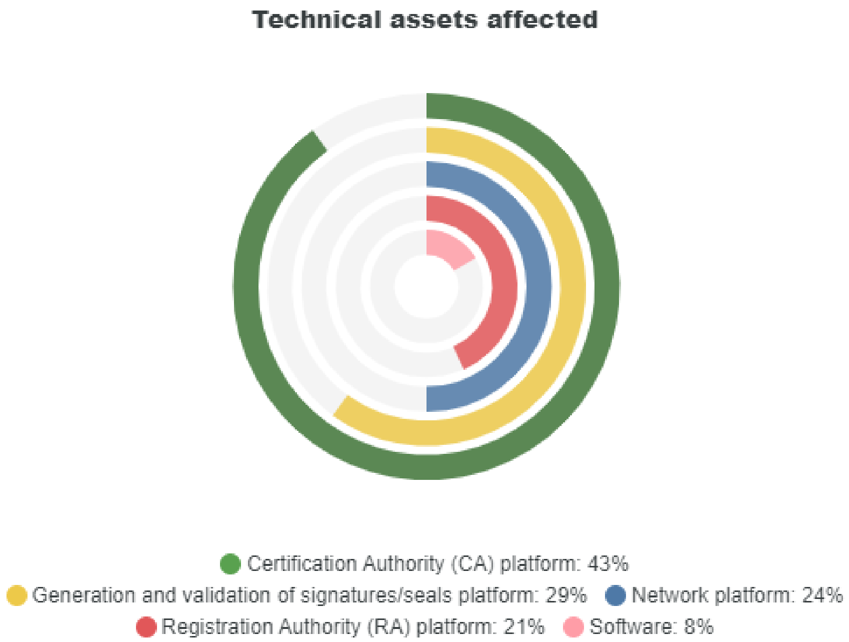


Finally, we also keep track of the **underlying assets** affected by incidents.

- The CA platform (43 %, compared with 33 % in 2022).
- The generation and validation of the signatures/seals platform (29 %, compared with 45 % in 2022).
- The network platform (24 %, compared with 11 % in 2022).
- The registration authority's platform (21 %, a constant).
- Software assets represented 8 % of affected assets over the reported period.

The dispersion of affected assets calls for a comprehensive approach when it comes to the security of trust services, taking into account assets from across the entire life cycle and supply chain. See the impact on technical assets in **Figure 6.**

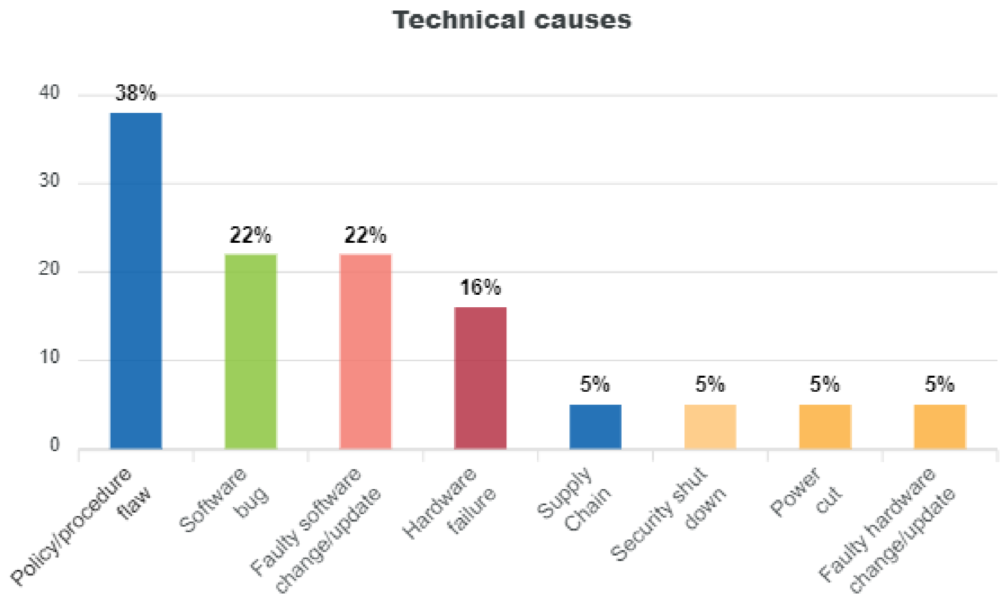
Figure 6. Technical assets affected – TSP security incidents 2023



By looking deeper into the affected technical assets, one can ascertain noteworthy differences between the corresponding technical causes, as detailed in **Figure 7**.

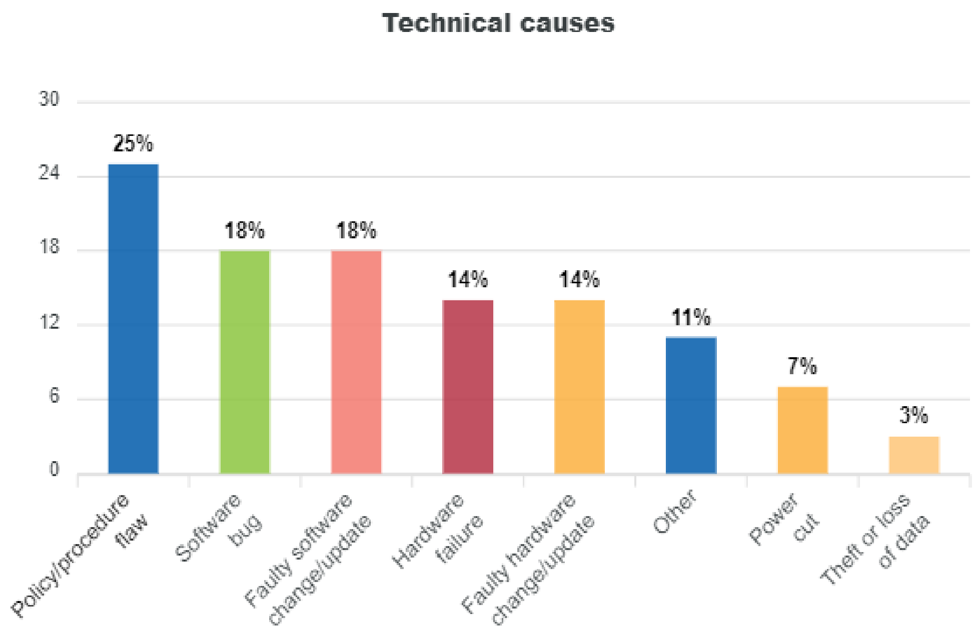
In the case of the platform for the **generation and validation of signatures/seals**, 38 % of the incidents report that flaws in policies and procedures were the main root cause in 2023, compared with 25 % in 2022.
Software bugs account for 22 %.

Figure 7a - generation and validation of signatures/seals



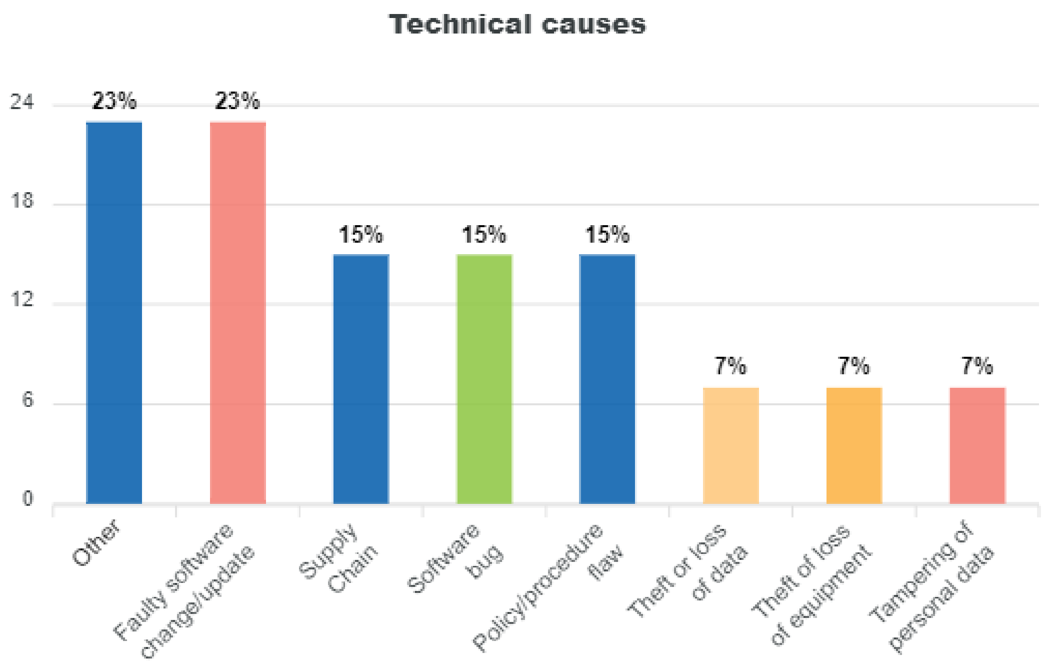
In the case of the **CA's platform**, the three main root causes are flaws in processes/procedures (25 %), software bugs (18 %) an d faulty software changes/updates (18 %).

Figure 7b – CA's platform



The registration platform incidents have a lower percentage (15 %) of flaws in policies and procedures as their root cause, but higher percentages of faulty software changes/updates (23 %) and supply-chain and software bugs related incidents (15 %). Note that the column 'Other' with 23 % is not defined in the dataset.

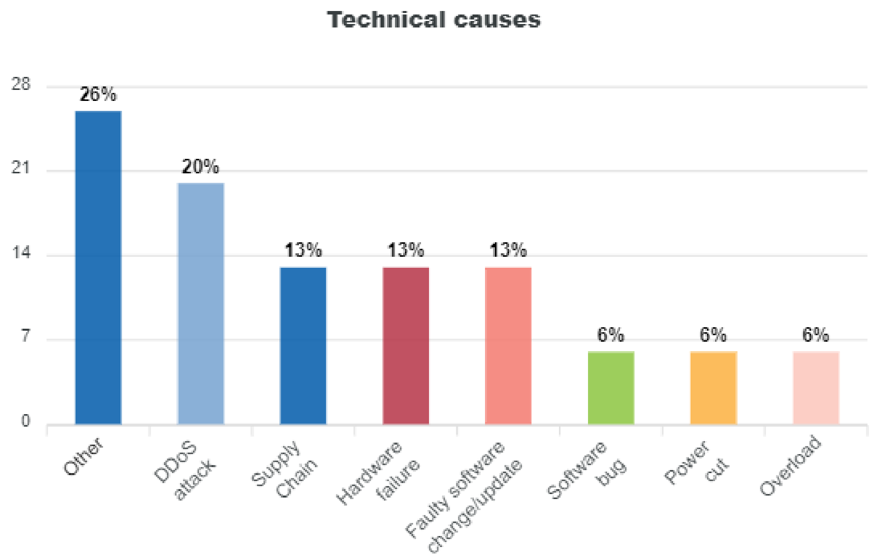
Figure 7c – Registration's platform



The network platform has 20 % of DDoS attacks as a root cause, followed by 13 % of supply-chain attacks.

The category ‘Other’ with 26 % in this table is not defined in the dataset.

Figure 7d. Network platform

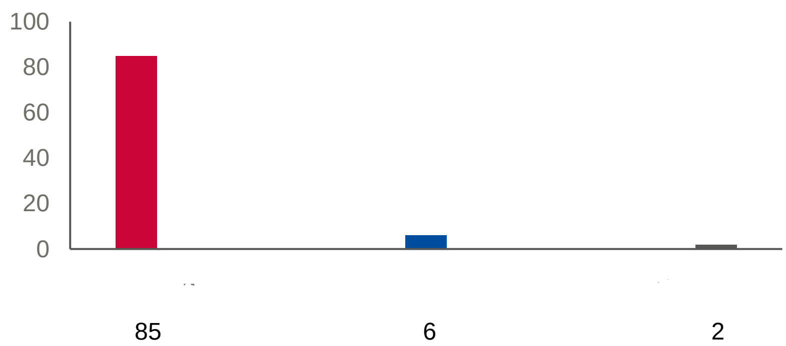


This comprehensive breakdown is extremely important to understand where emphasis should be prioritised when it comes to targeted security controls in the various technical assets of TSPs.

3.4 QUALIFIED SERVICES VERSUS NON-QUALIFIED SERVICES

This year nearly 84 % of total trust services security incidents had an impact on qualified services (i.e. qualified signature certificate creation, qualified seal certificate creation, etc.) with **85** qualified services and **6** non-qualified services. Again, it is important to note that one incident report could involve multiple trust services, which explains why the total number of incidents in **Figure 8** adds up to more than 63 (i.e. the total number of incidents reported in 2023).

Figure 8. Reported incidents affecting qualified v non-qualified services – 2023



Note that, in most cases, the TSP reporting an incident also offers qualified services and that the impact on non-qualified services is usually 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 for incidents that impact qualified services. Moreover, we need to underline a decrease in the number of non-qualified service incidents being reported compared with 2022 (7), which indicates the need to promote the importance of incident reporting to the respective providers.

4. MULTIANNUAL TRENDS 2016–2023

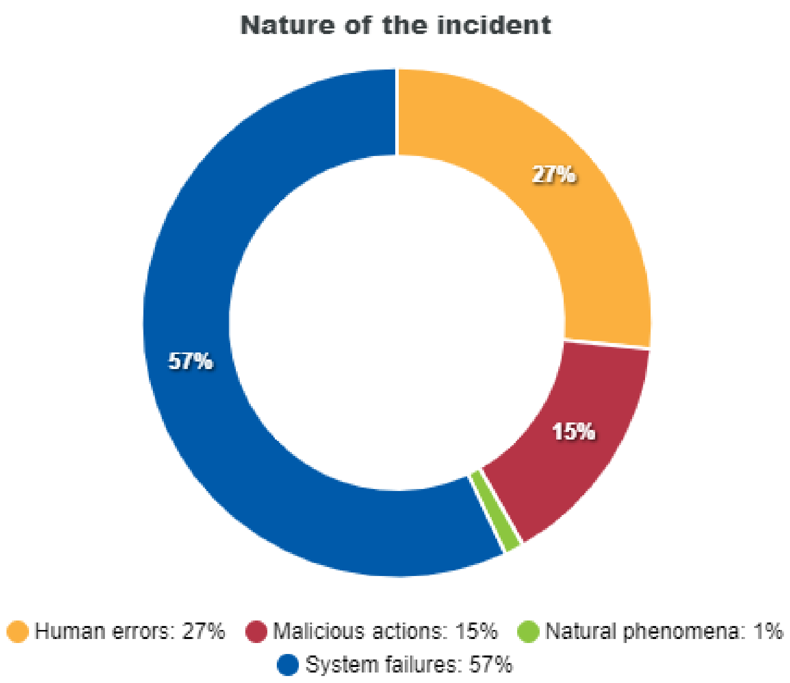
ENISA has been collecting and aggregating trust services incident reports since 2016. In this section, we look at multiannual trends over the last 8 years, covering 2016–2023. The dataset contains a total of 244 reported incidents.

4.1 MULTIANNUAL TREND IN ROOT CAUSE CATEGORIES

Root-cause categories, i.e. system failures, human errors, malicious actions and natural phenomena, are analysed over the period of reference ([12]).

From 2016–2023 system failures represented 57 % of all reported incidents, human errors represented 27 % of all reported incidents, 15 % involved malicious actions and 2 % natural phenomena, as displayed in **Figure 9.**

Figure 9. Nature of reported incidents – trust services security incidents in the EU (reported from 2016–2023)



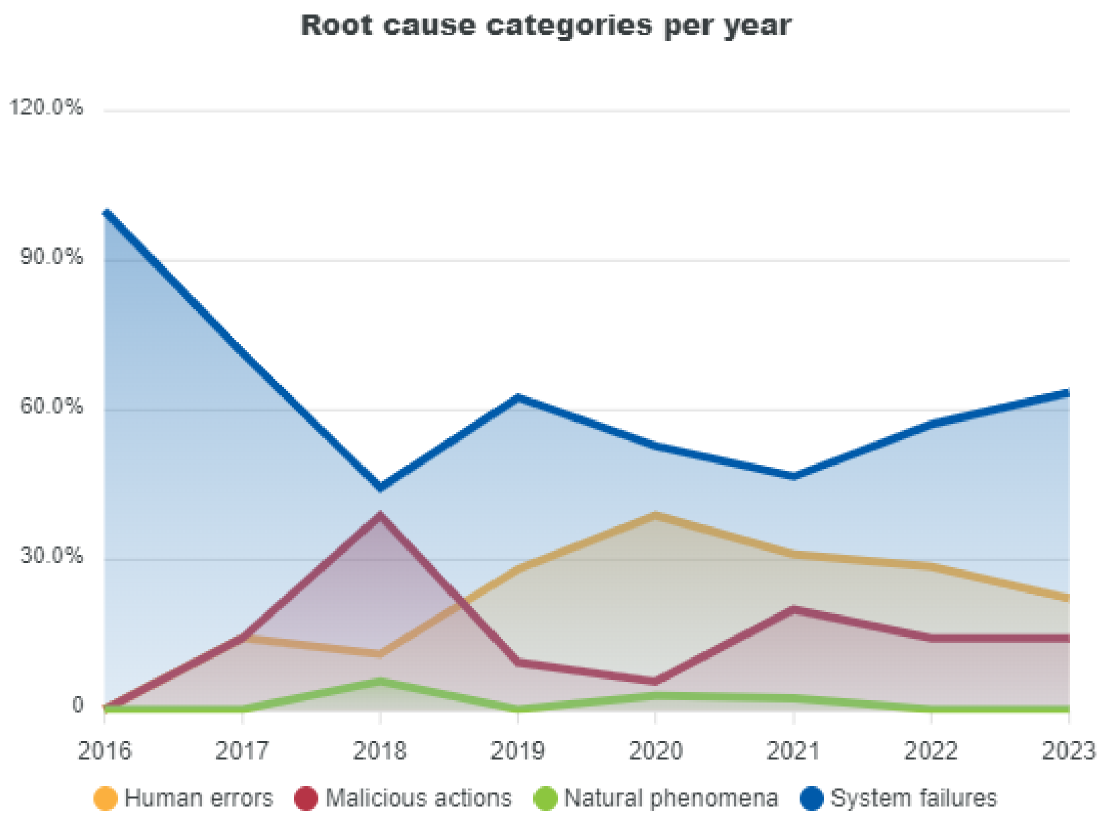
Over the period of reference, out of 244 incidents reported:

- system failures accounted for 139 of all reported incidents,
- human errors accounted for 65 of all reported incidents,
- 37 involved malicious actions, and
- 3 involved natural phenomena.

([12]) Peak of 100 % in 2016, first year of trust services annual incident reporting.

Percentage trends of related incidents over the last 8 years are displayed in **Figure 10**, arranged by category.

Figure 10. Root-cause categories – trust services security incidents in the EU (reported from 2016–2023)



Over the last few years of trust services security incident reporting, the most common root cause has been **system failures**, with a total of **139 reported incidents**. The percentage of system-failure-related incidents over the last 8 years has varied as follows: 100 % in 2016, 71.4 % in 2017, 44.4 % in 2018, 62.5 % in 2019, 52.8 % in 2020, 46.7 % in 2021, 57.1 % in 2022 and 63.5 % in 2023, representing an average of **57 %** over the period analysed.

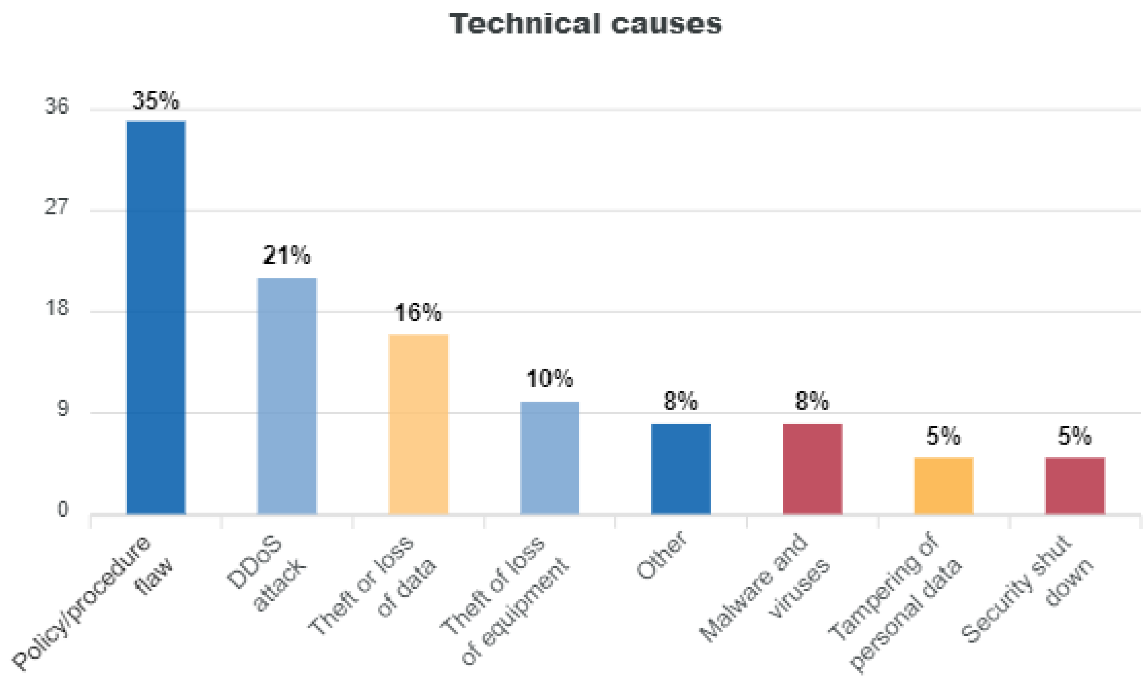
Moreover, incidents concerning **human errors** have remained constant since 2020 with an average of circa **14** incidents per year. In terms of percentage of total incidents, this data has been steadily decreasing over the last few years, from 38.9 % in 2020 to 31.1 % in 2021, 28.6 % in 2022 and 22.2 % in 2023.

In the trust services sector, **natural phenomena** are not a common root cause. From 2016–2023 only **three** incidents were reported, accounting for **1 %** of the total. No such incidents were reported in 2022 or 2023.

Malicious actions vary across the years, with the peak of 38.9 % observed during 2018 and a value as low as 5.6 % recorded in 2020. In 2023, malicious actions were the root cause for 14.3 % of the reported incidents with nine incidents, likewise in 2022 with five incidents, and for 20 % of reported incidents in 2021 with nine incidents.

For the 37 incidents reported under the malicious actions category, the most common technical causes over the years are given in **Figure 11**.

Figure 11. Detailed technical causes – trust services security incidents in the EU (reported from 2016–2023)



It is interesting to contrast these findings with the latest version of the ENISA threat landscape and the identified prime threats (threats against data, malware, threats against availability, non-malicious threats, etc.).

4.2 MULTIANNUAL TREND IN SEVERITY OF IMPACT

In the multiannual trend concerning the severity of impact, the EU cybersecurity incident taxonomy ([13]) is again followed, where the severity of the impact has the following values: no impact, minor, large and very large impact. Over time, TSPs are reporting more incidents regardless of their severity.

The number of incidents with **no impact** was 5 in 2023.

It is interesting to see that there is a mostly linear increase in **minor incidents** (in green) over the course of the last years from 2 incidents in 2018, to 19 in 2019, 26 in 2020 and 30 in 2021, with a drop to 19 in 2022 and a rise to 35 in 2023.

While comparing the statistics for severity since 2016, it is quite clear that **large impact incidents** (in yellow) have continued to increase (by one third) in frequency, reaching 18 incidents this year, despite the drop observed in 2020.

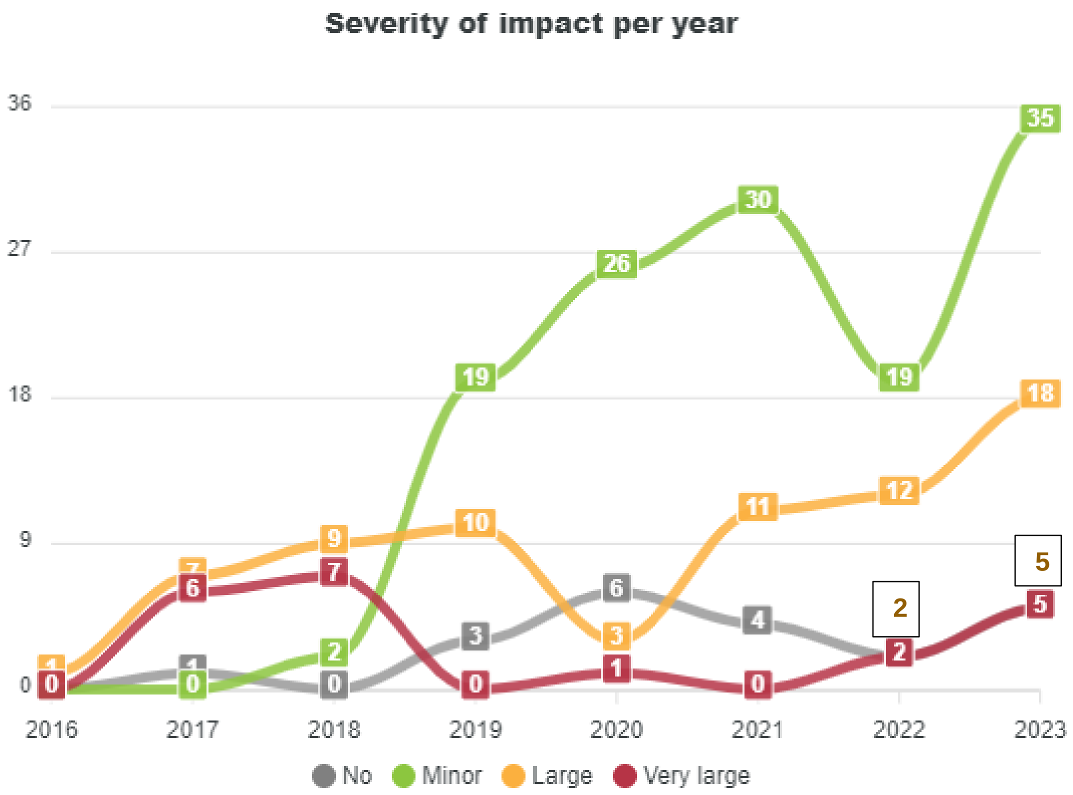
With respect to the five **very large impact incidents** reported this year, the trend since 2021 shows an increase over time.

([13]) See Cybersecurity Incident Taxonomy (2018)
http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53646

In terms of **impact**, in all four categories, the number of incidents almost doubled compared with 2022.

However, looking at the trends, the increase has followed a steady path since 2018, as detailed in **Figure 12**.

Figure 12. Severity of impact – trust services security incidents in the EU (reported from 2016–2023)



4.3 MULTIANNUAL TREND IN IMPACT ON SERVICES

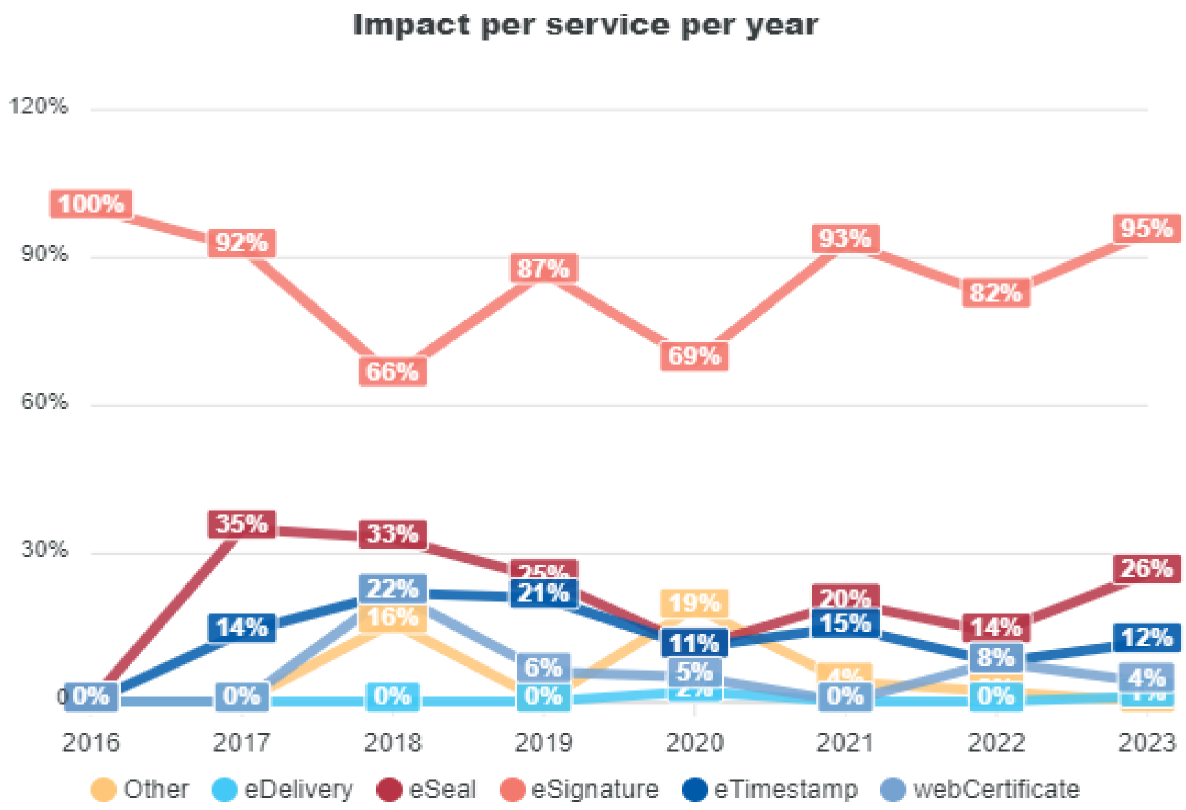
In this section, the impact per service from 2016–2023 for reported incidents for trust services is detailed in **Figure 13**.

It is evident that the majority of reported incidents relate to **electronic signatures**, with numbers ranging consistently between 65 % and 95 % since 2017, reaching 95 % in 2023 to give an average of 85.5 % over the period analysed. This may be attributed to their widespread deployment and uptake in comparison to electronic seals and timestamping services.

For these categories, if we look back at the past years of reporting (2016–2023), we see a similar pattern: 23 % affected **electronic seals** and 14 % affected **timestamping services**.

Web certificates and **electronic delivery services** consistently have low values. 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 a reduced usage of the services, better security provisions or a lack of reporting.

Figure 13. Impact on services – trust services security incidents in the EU (reported from 2016–2023)



5. CONCLUSIONS

The **key takeaways** from the 2023 incident reports are as follows.

- Two thirds of EU SBs – **18** out of 27 – sent their respective reports with 0 incidents reported ([14]).
- Reported incidents **increased by 80 %** to a total of **63 incidents**, compared with 35 in 2022 ([15]).
- The number of incidents (9) caused by **malicious actions** has increased compared with 2022 (5) reaching the same level as in 2021. However, with **14 %** of the total, it remains a constant percentage since 2022 for this root cause.
- The overall impact of the incidents amounted to **3 184 million user hours lost**, compared with 405 million in 2022, among which **3 140 million hours (98 %) were lost due to malicious actions** ([16]). One million hours were lost due to system failures and 43 million hours were lost due to human errors ([17]).
- In terms of **impact**, in all four categories the number of incidents almost **doubled**:
    - in 2023, 5 incidents with no impact were reported, 35 with minor impact, 18 large incidents and 5 very large incidents;
    - the number of incidents with minor impact has almost doubled compared with 2022, but remains in line with data from previous years;
    - the number of large and very large incidents has continued to increase.
- **Third-party failures** continue to be monitored, with a view to assessing the impact on suppliers and providers. For 2023, 19 incidents out of 63 were flagged as third-party failures (33 %).
- **Qualified trust services versus non-qualified trust services** – in 2023, 84 % of total incidents had an impact on qualified trust services.

([14]) 2022: 13/27; 2021: 17/27; 2020: 19/27; 2019: 17/27; 2018: 18/27; 2017: 17/27; 2016: 26/27.
([15]) Among them, 46 incidents occurred in 9 EU SBs and 21 in SBs from EEA countries.
([16]) In 2022 it was 0 million.
([17]) In 2022 it was 34 million and 371 million, respectively.

TP-01-24-007-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 978-92-9204-684-2
doi: 10.2824/9574029