EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ANNUAL REPORT TRUST SERVICES SECURITY INCIDENTS 2024

JUNE 2025

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

Rossen Naydenov, ENISA

Nuno Rodrigues Carvalho, ENISA

Edgars Taurins, 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

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or ENISA bodies unless adopted pursuant to the Regulation (EU) 2019/881. This publication does not necessarily represent the state-of the-art and ENISA may update it from time to time.

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

This publication is intended for information purposes only. It must be accessible free of charge. 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.

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2025

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 appropriate credit is given and any changes are indicated.

For any use or reproduction of elements that are not owned by the European Union Agency for Cybersecurity, permission may need to be sought directly from the respective rightsholders.

ISBN 978-92-9204-707-8 DOI: 10.2824/2144753, ISSN: 2599-9435

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Every year national supervisory bodies must send annual summary reports about the notified breaches to ENISA and the Commission according to art 19 of the eIDAS[1] regulation.

This is the eighth round of reporting produced by ENISA, for the EU's trust services sector, analysing root causes, statistics and trends. It is an aggregated overview of the reported breaches for 2024 as reported to ENISA by 21 EU Member States and 3 EFTA countries.

In 2024, a total of **44 incidents** were reported by these countries.

Key findings from the 2024 incident reports are summarised in the following list of points.

- Half of the EU supervisory bodies (SBs) – **12** out of 24 – sent their respective reports with 0 incidents reported.
- Reported incidents **decreased to 44**, compared to 63 in 2023. However, it should be noted that in 2023 there were 6 more MS reporting incidents.
- The distribution of incidents remains similar percentage-wise compared to 2023 with system fail taking the major cut at 63% (64% in 2023), human error 23% (same for 2023) and malicious actions 14% (same for 2023).
- The overall impact of the incidents amounted to **618 million** user hours lost which is a decrease of 5 times compared to **3 184 million user hours lost in 2023**[2].
- **Malicious actions** are the most impactful root cause with 571 million user hours lost with over 92% of all hours lost, which is a decline compared to 2023 where we had 98% of all hours lost (3140 million).

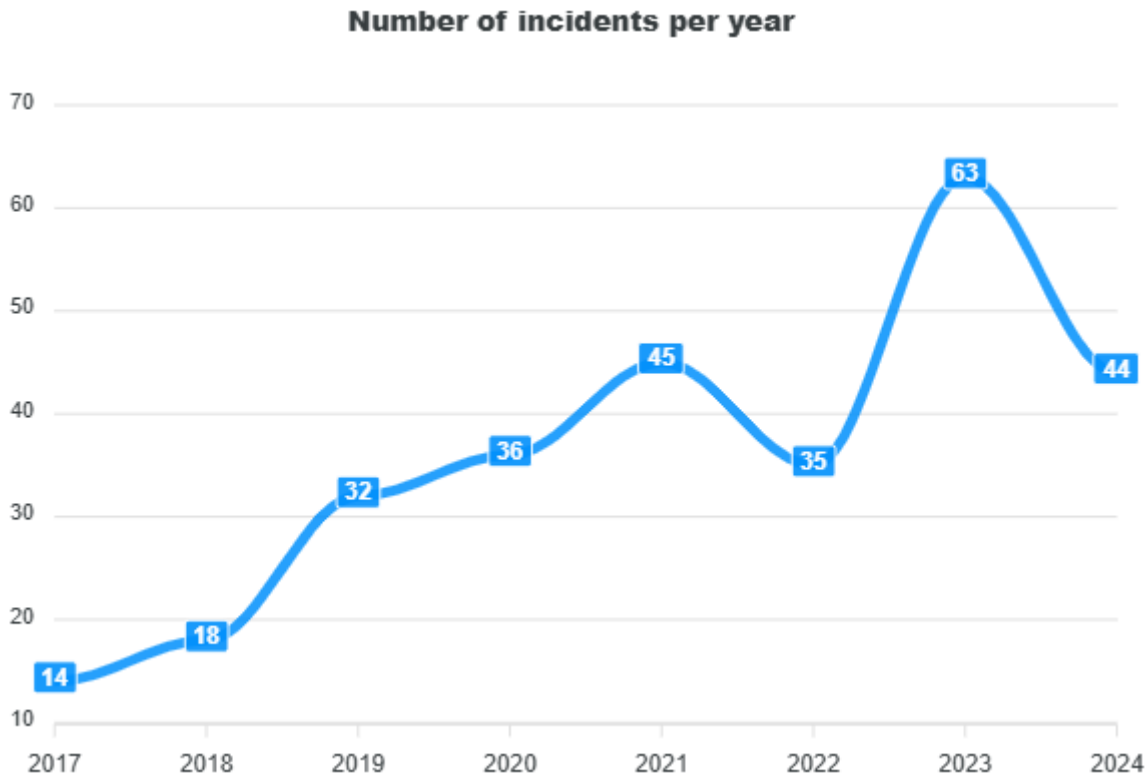
Highlights 2024

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

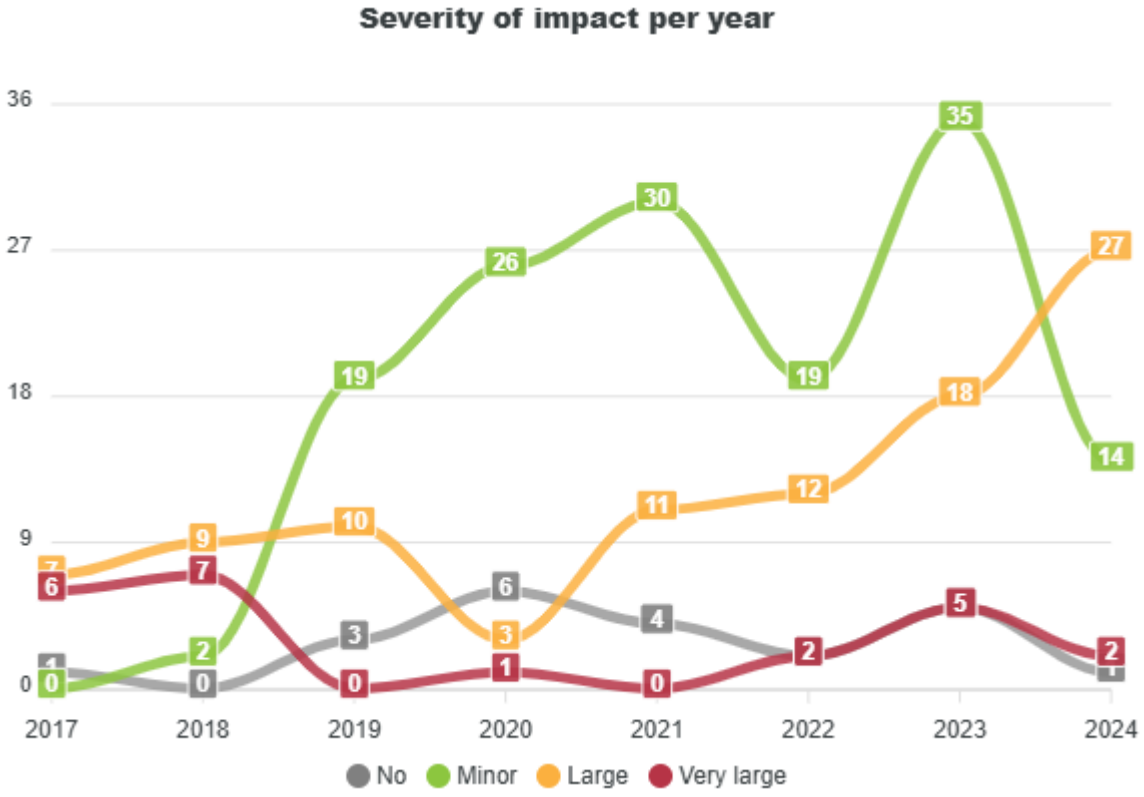
Malicious actions is the most impactful root cause in terms of user hours lost with more than 92% of all user hours lost attributed to this root cause.

(1) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910

(2) Please, take into consideration that we have 6 member states less reporting at the time of writing of the report than what was on 2023



- In terms of **impact**, large incidents continue to **raise**



1. INTRODUCTION

1.1 SCOPE

Under Article 19 of the eIDAS regulation, 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 and 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) ([3]). This tool allows for a custom analysis of trends and patterns and supports the quantitative and qualitative analysis of the data collected.

This report gives an aggregate overview of the incidents submitted to ENISA by the supervisory bodies during 2024.

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 2017-2024;
- Section 5 draws conclusions and observations based on the available datasets.

([3]) For more information https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool; website of the tool can be found here: 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.

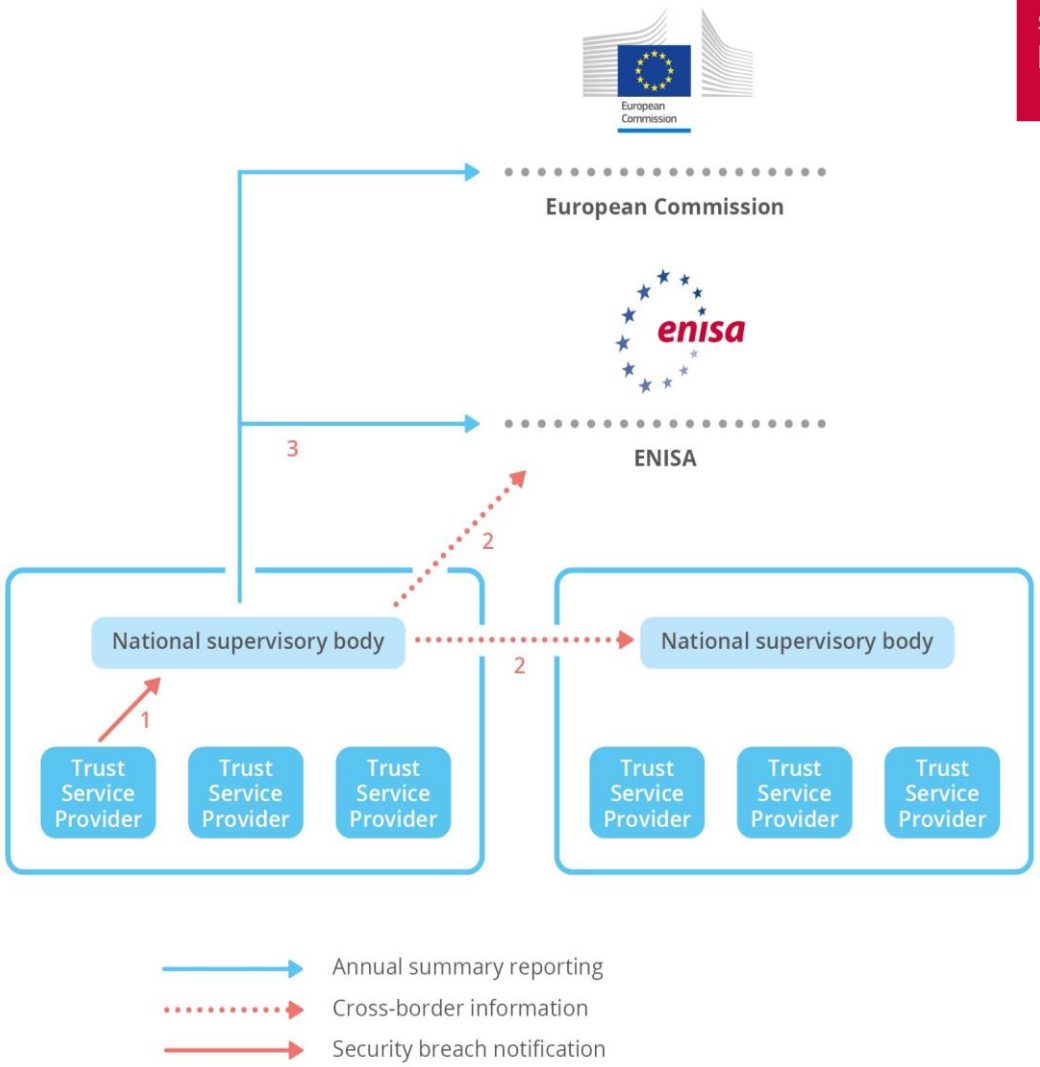


Figure A. Security breach notification process

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.

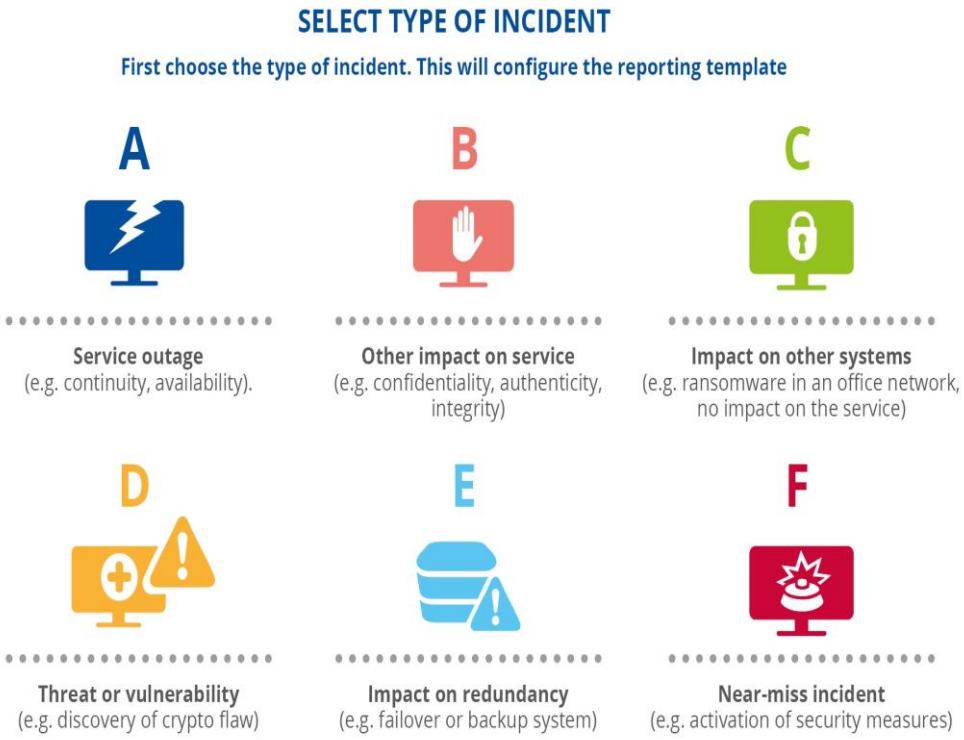


Figure B. Incident reporting tool

- **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 2024 annual summary reporting, by the 21 EU Member States and 3 EEA countries participating in this process, included in total 44 security incidents.

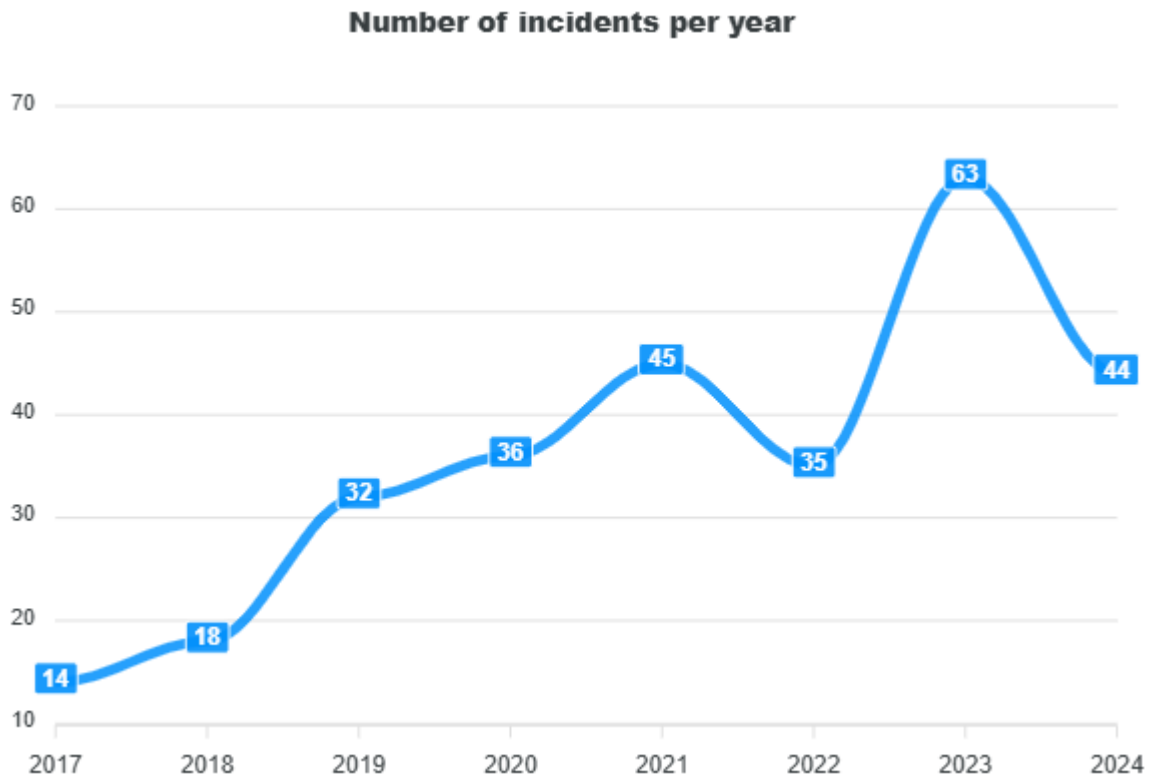


Figure 1. Number of reported incidents from 2017–2024

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 **618 million user hours lost**, 42 million hours of which were for system failures, 4 million hours human errors and **571 million hours malicious actions**. In comparison for 2023 we had 3184 million user hours lost, with system failures having 1 million, human errors 43 million and malicious actions with **3140 million.**

Incidents are divided into four categories of root causes.

- **System failures** continue to be the dominant root cause in 2024, accounting for 64% out of 28 incidents compared to 63% with 40 incidents in 2023. Typically, system failures are due to either hardware failures or software bugs.
- **Human errors** accounted for 23% with 10 incidents, which is similar in percentage for 2023 with 22% albeit with more incidents - 14.
- **Malicious actions** with 6 incidents got a share of 14%, which is the same percentage in 2023, with 9 incidents.
- **Natural phenomena** did not account for any of the reported incidents, which is a trend for the last three years.

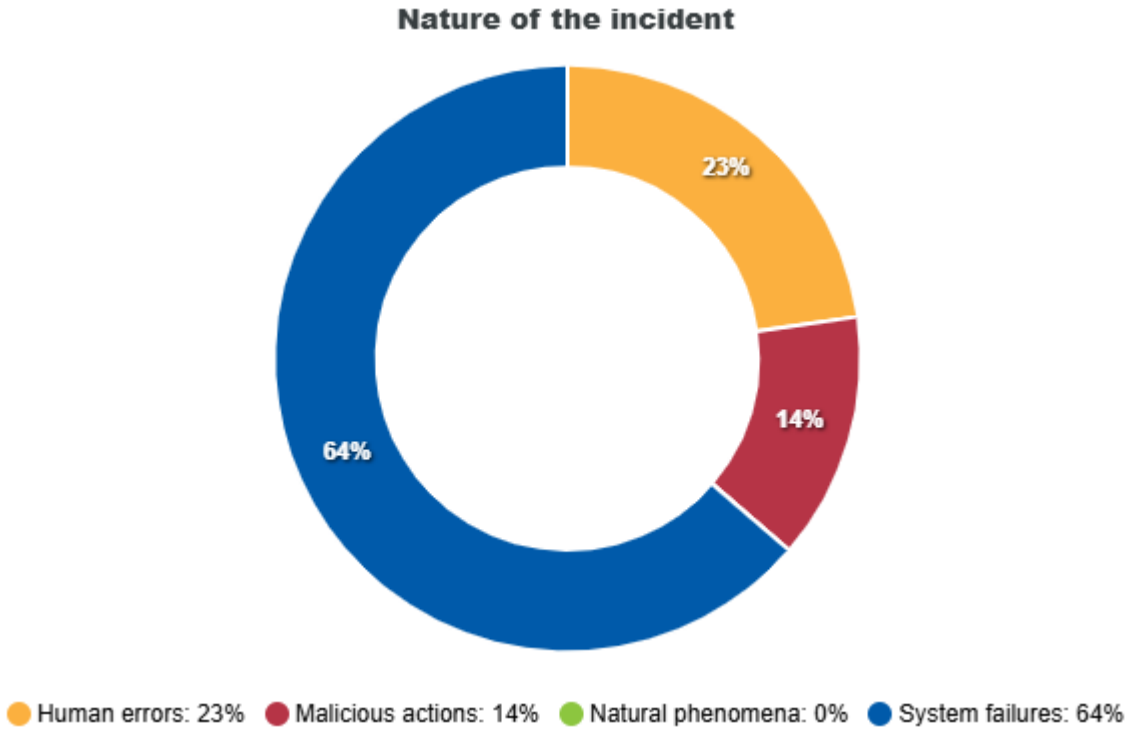


Figure 2. Root causes of TSP security incidents – 2024

We also keep track of **third-party failures**, i.e. when the incident originated from a third party, with a view to assessing the impact on the supplier or the provider.

In 2024, out of 44 reported incidents 7 are marked as third-party failures, compared to 19 incidents out of 63 were flagged as third-party failures for 2023.

Out of those reported in 2024:

- **6** were categorised as **system failures** and
- **1** were categorised as **malicious actions**.

3.1.1 System Failures

System failures account for 28 of all 44 incidents resulting in 64% share for 2024. The most impacted services by system failures are the eSignatures with 85% of all system failures. eTimestamp come second with 17% and webCertificates with 14%.

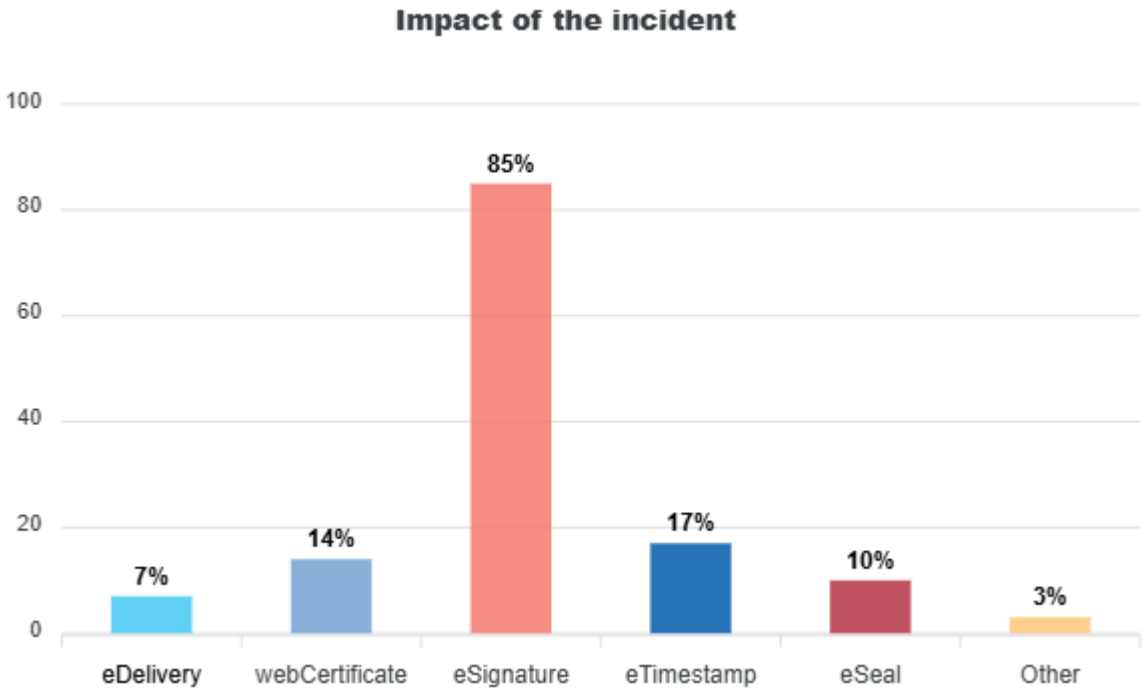


Figure 3. System failures impact on services – 2024

The top three technical causes for system failures are hardware failure with 32%, Software bugs with 28% and policy procedure flaw with 14%. The top two causes are similar to 2023 the difference being that policy procedure was last in the score with 5% while faulty software changes were third with 25%.

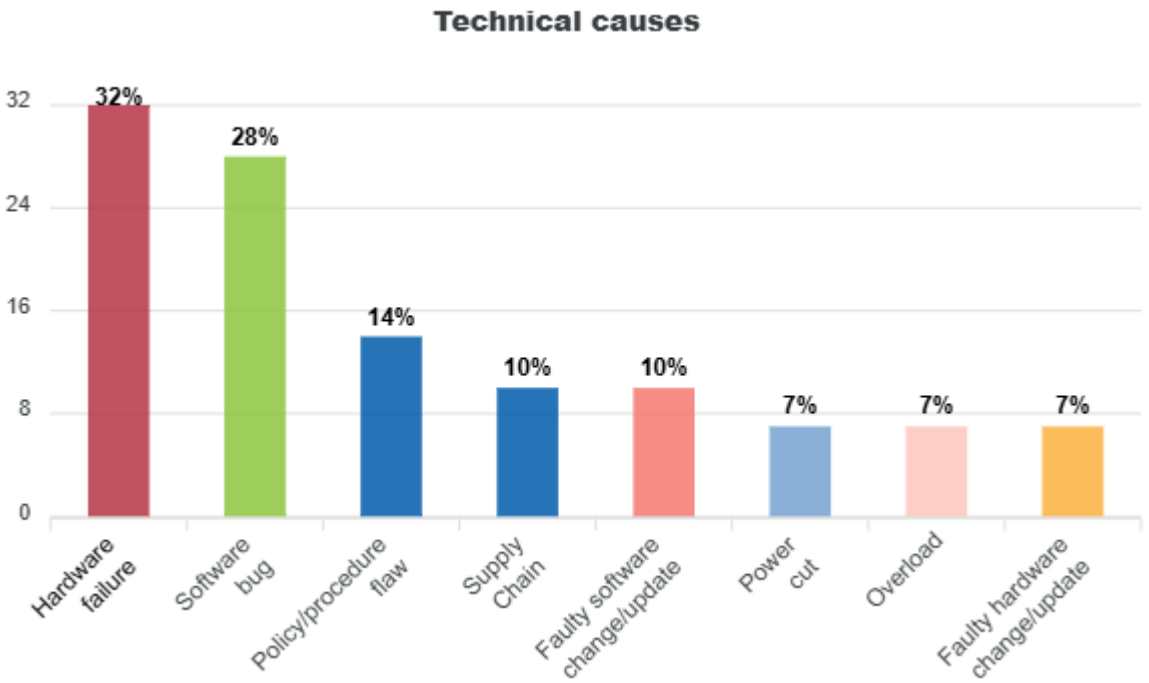


Figure 4. Technical causes for System failures– 2024

The top three technical assets affected by the system failures in 2024 are Certification authority platform (32%), registration authority (32%) and generation and validation of signatures/seals platform with 29%. The difference with 2023 is in the changes in second and third place, where we had generation and validation of signatures/seals platform second with 30% and network platform third with 25%.

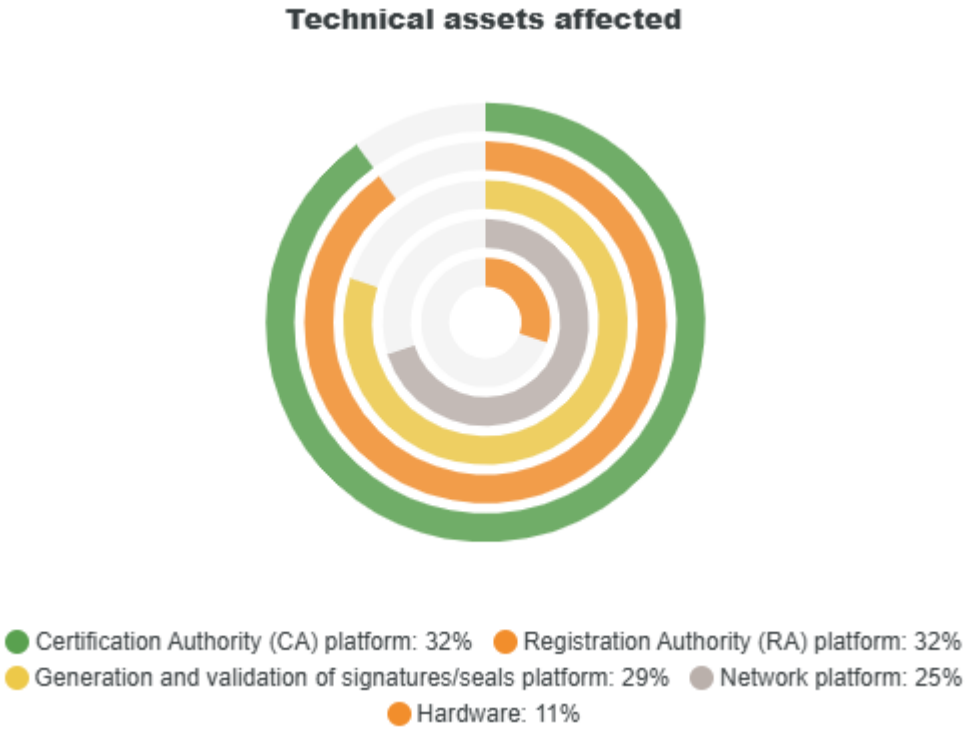


Figure 5. Technical assets affected by System failures– 2024

3.1.2 Human errors

The human errors incidents are 10 in total, representing a 23% share of all incidents in 2024.

The human errors have a limited impact in terms of services affected for 2024, compared to system failures. Only three were affected with eSignature being the top with 80%, which is similar as in 2023 where we had 92%. Second and third are the eTimestamp and webCertificate with same results at 10%. For comparison in 2023 we also had eSeal affected with 14%, which made it the second most affected in that year.

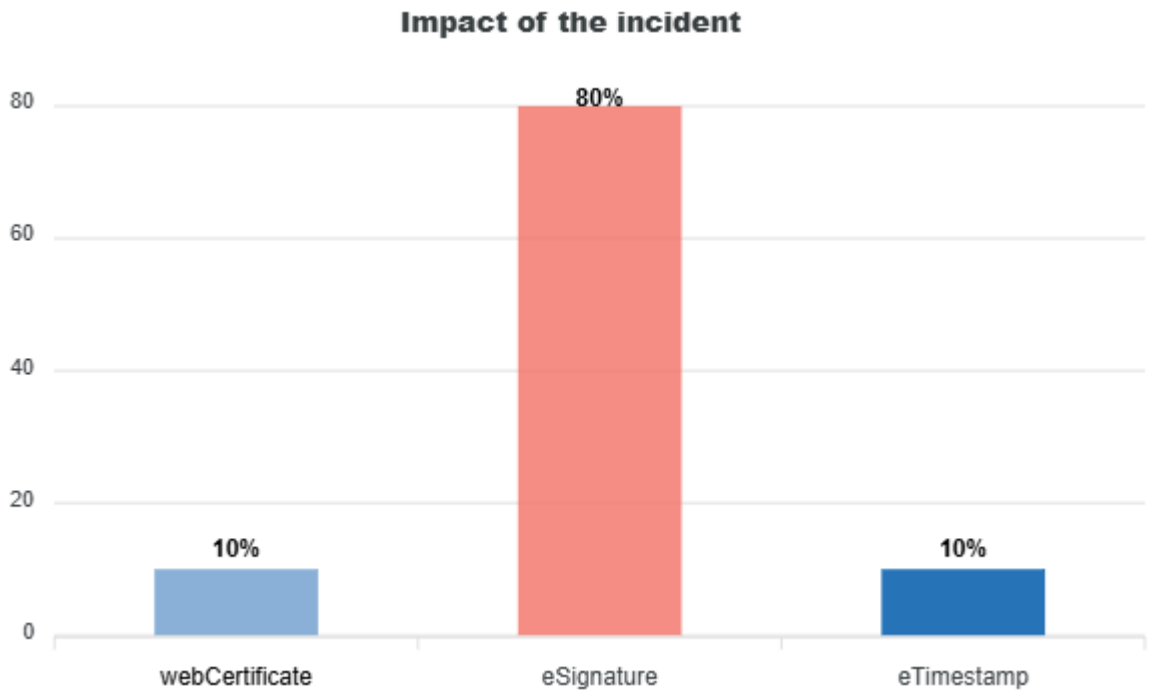


Figure 6. Human errors impact on services – 2024

The top three technical causes for human errors in 2024 were policy/procedure flaw with 60%, similar to 2023 where this cause was with 42%. Second comes faulty software change/update with 30% and last are software bugs with 10%. For comparison in 2023 we also had tampering of personal data standing in last place with 7%.

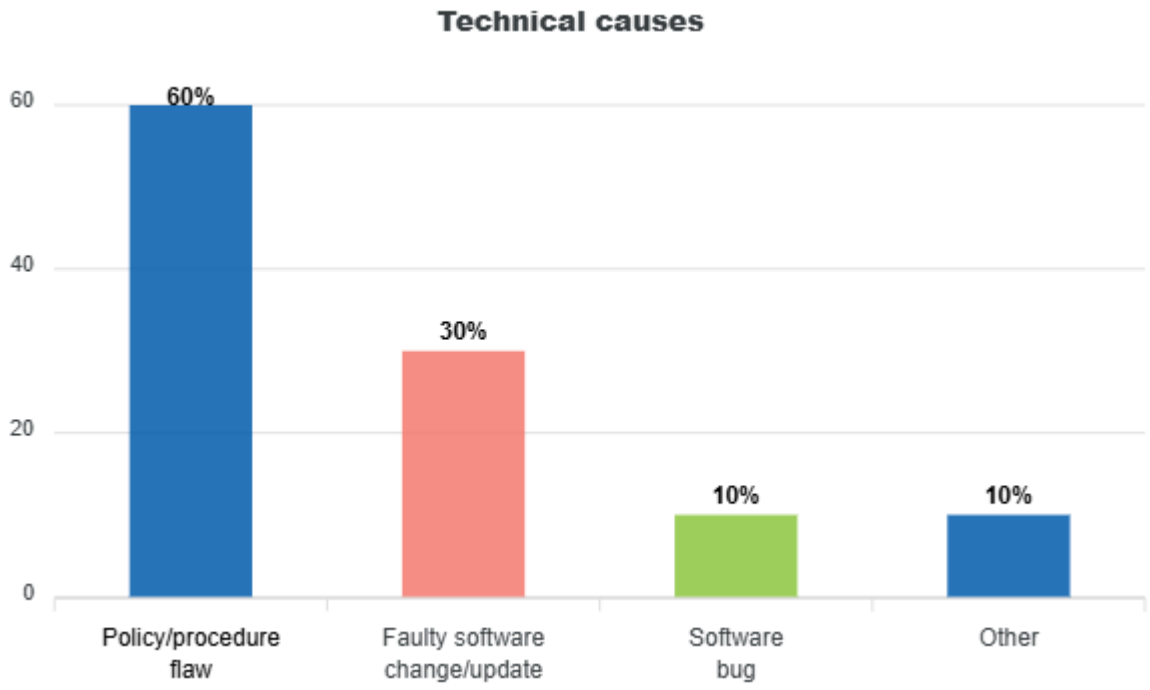


Figure 7. Technical causes **for h**uman errors– 2024

The top three technical assets affected by human errors in 2024 were the generation and validation of signatures/seals platform with 50%, second comes the certification authority with 40% and last are the time stamping and the validation authority with both having 10%. For comparison in 2023 we had certification authority with 29% being top cause, while the rest generation and validation of signatures/seals platform, registration authority and software were all with 21%.

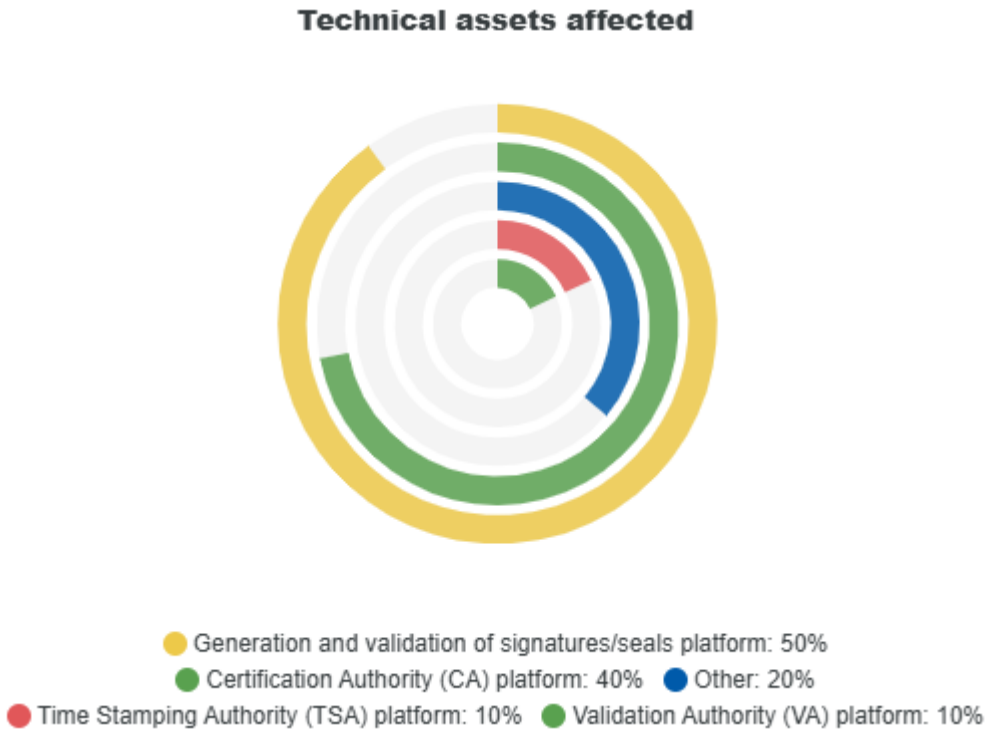


Figure 8. Technical assets affected by Human errors– 2024

3.1.3 Malicious actions

Malicious actions have 14% of the share with 6 incidents for 2024. The malicious actions have a very targeted service for 2024 and this is the eSginature service, with all the incidents reported on this particular service.

The top three technical causes for malicious actions in 2024 are tampering of personal data with 50%, second comes malware and viruses with 33% and last are theft or loss of data and theft or loss of equipment both with 16%.

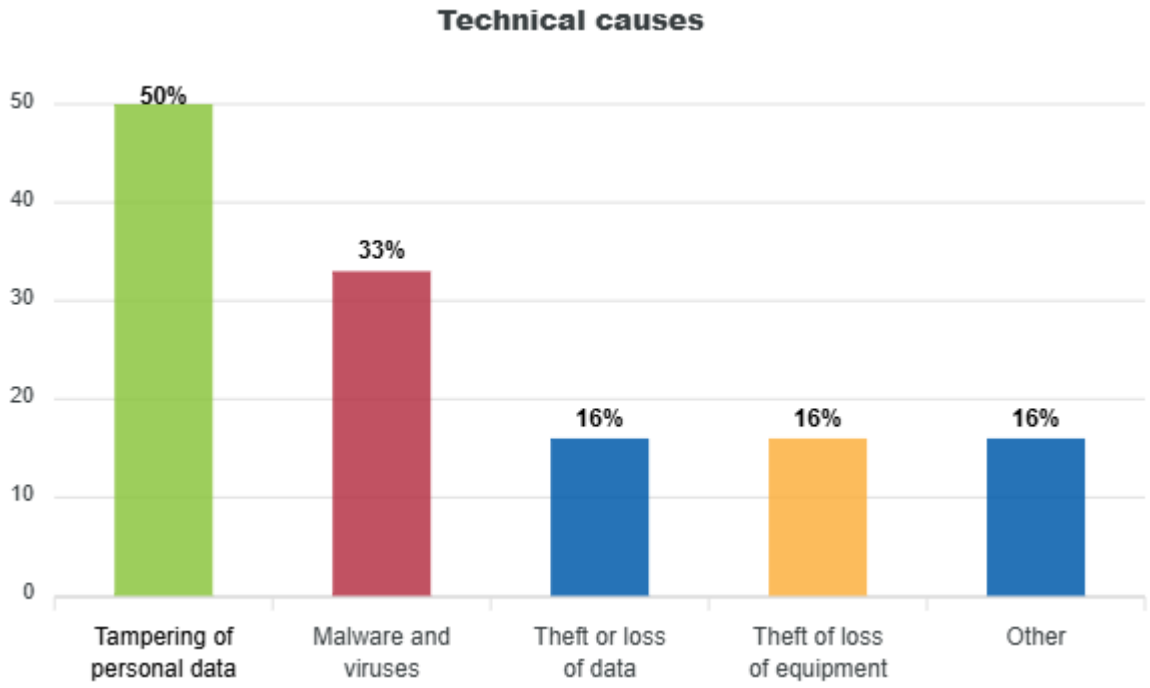


Figure 9. Technical causes for malicious actions – 2024

The top three technical assets affected by the malicious actions in 2024 were Archive with 33%, generation and validation of signatures/seals platform with 33% and certification authority and network platform at 17%. In comparison for 2023 the CA authority was top asset affected with 44%, second comes generation and validation of signatures/seals platform with 33% and third was registration authority with 22%.

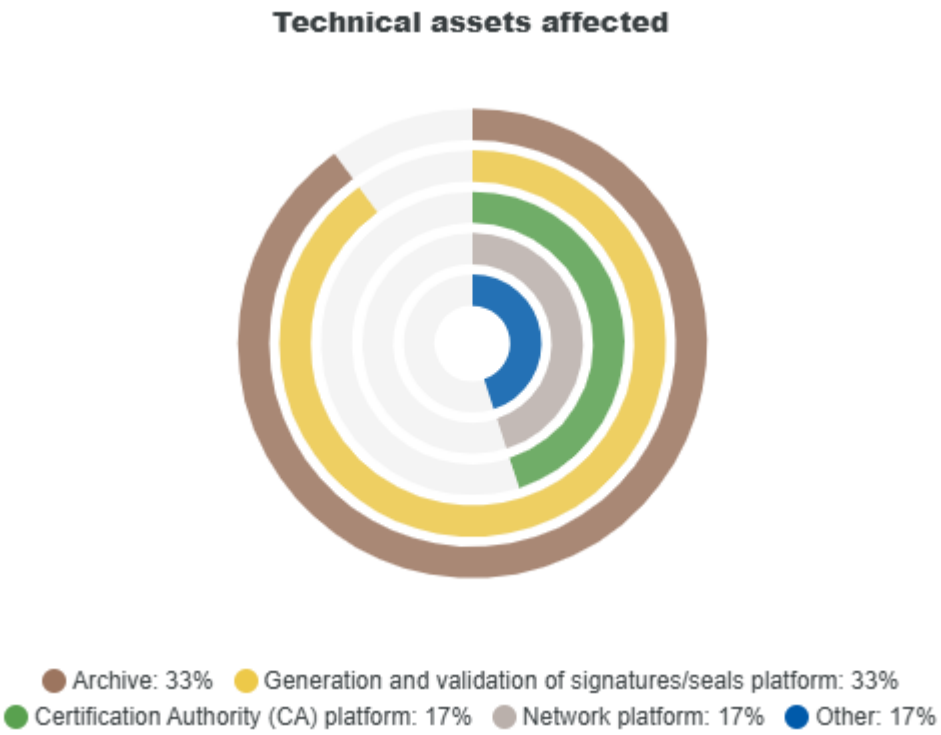


Figure 10. Technical assets affected by malicious actions – 2024

3.2 TECHNICAL CAUSES

It is important to note that an incident is often not only triggered by one cause ([4]) but by multiple detailed causes (i.e. a chain of events).

The top detailed cause of incidents in 2024 was the **policy/procedure flaw**, with 10 incidents accounting for 22% of all incidents. This is an increase compared to 2023 where policy procedure flaw was third technical cause with 13 incidents at 15%.

Software bugs come second overall with 20% and 9 incidents, which is an increase in the share from 2023 where it was 17% with 11 incidents.

Hardware failure comes in third place with 20% share and 9 incidents, which is an increase in the share from 14% in 2023, with the same number of incidents.

Faulty software changes/updates with 13% and 6 incidents are forth, which is a big change compared to 2023, where it was the top cause with 20% and 13 incidents.

The full breakdown of detailed causes for reported incidents can be seen in **Figure 11**.

([4]) 'Other' is not defined here.

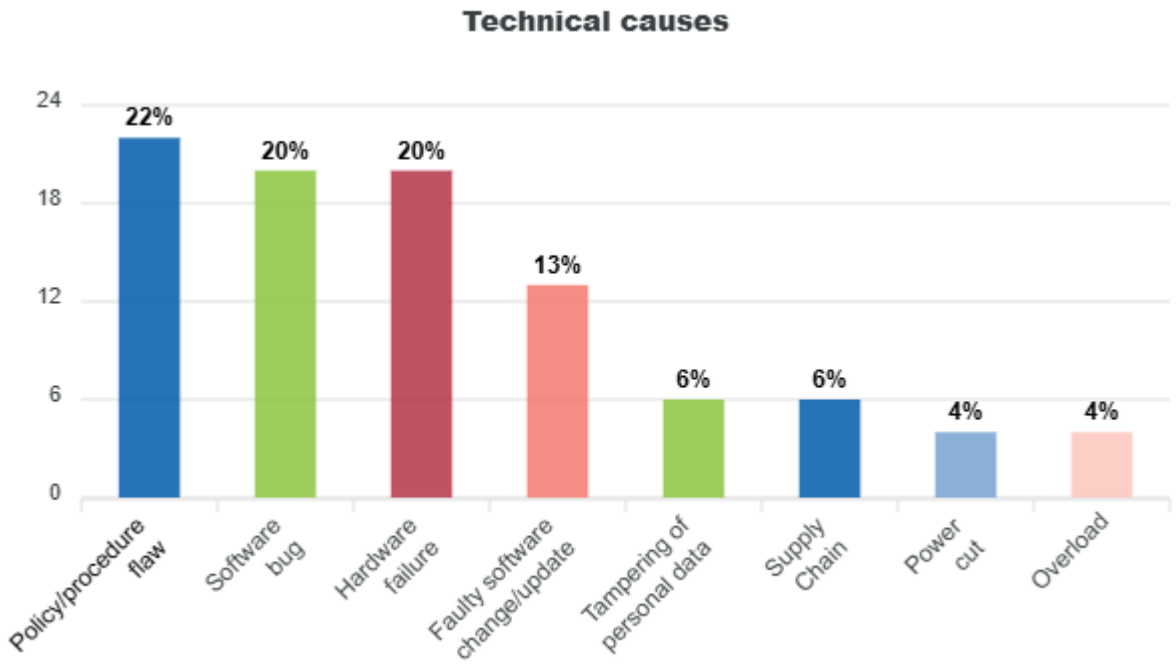


Figure 11. Detailed causes of trust services security incidents – 2024

3.3 SERVICES AFFECTED

The most affected services in 2024 are eSignature, eTimestamp and webCertificate.

Most of the reported incidents (**86%**) had an impact on **electronic signatures** ([5]), as can be seen in **Figure 12**, compared to 95% having an impact on electronic signatures in 2023.

eTimestamps come distant second with just 13% representing 6 incidents, which is similar to 12% and 8 incidents in 2023.

The third most impacted services was webCertifcate with 11% and 5 incidents, which is an increase from 2023 where it had 4% and 3 incidents.

eSeal had the biggest decline with 6% and 3 incidents, while in 2023 there were 26% and 7 incidents.

([5]) 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.

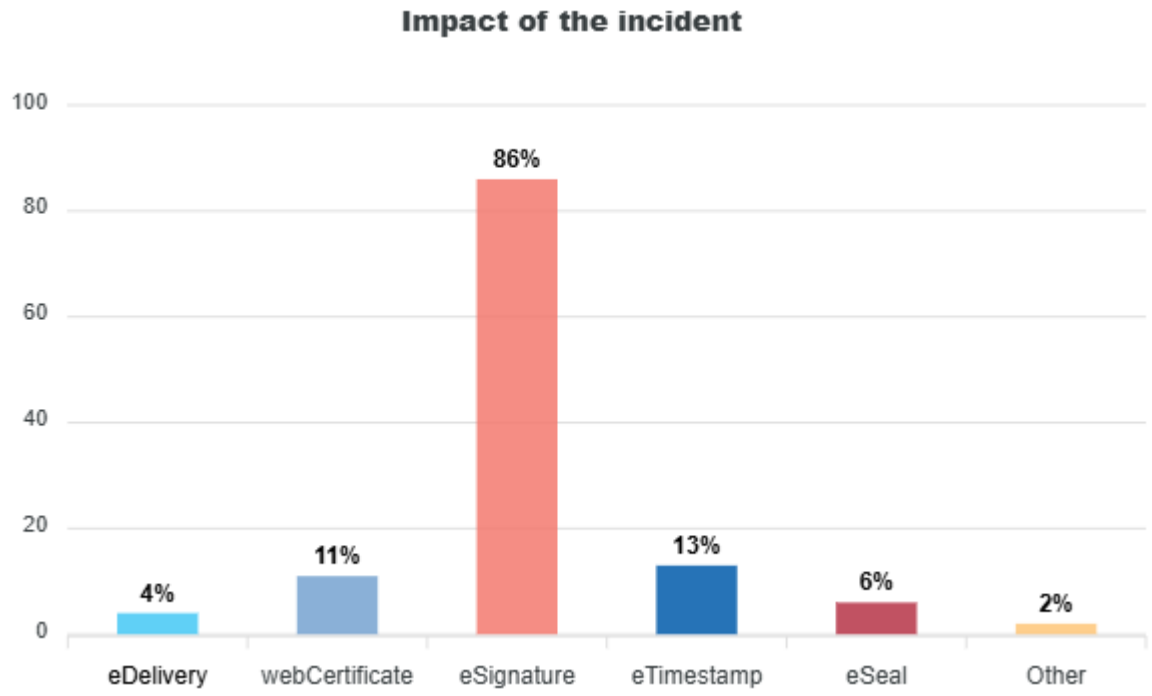


Figure 12. Impact of incidents on trust services – 2024[6]

3.4 ASSETS AFFECTED

Finally, we also keep track of the **underlying assets** affected by incidents, which can be seen in **Figure 13.**

The top affected assets are the generation and validation of signtures/seals platform with 34% and 15 incidents, which is an increase in percentage compared to 2023 with 28% with a bigger number of incidents – 18.

The second most affected asset in 2024 is the certification authority platform with 32% and 14 incidents which is a decrease compared to 2023 where it was top cause with 43% and 27 incidents.

The registration authority platform is the third most impacted asset with 23% and 10 incidents which is similar to 2023 where we had 21% and 13 incidents.

Network platform is forth with 18% and 8 incidents, which is a decrease in share compared to 2023 with 24% and double the incidents to 15.

([6]) Please note that several incidents affected multiple services, hence the numbers in the figure adding up to more than 100%

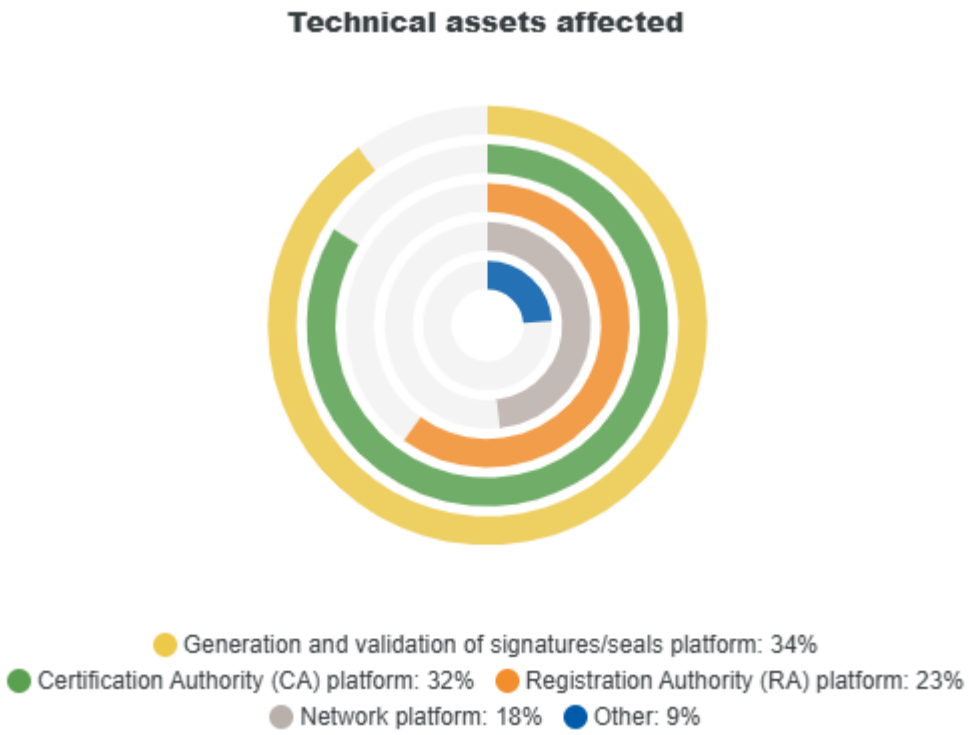


Figure 13. Technical assets affected – TSP security incidents 2024

3.5 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 **37** incidents in qualified services and 7 incidents in non-qualified services. The distribution remains exactly the same to what was in 2023 with the same numbers in terms of percentages.

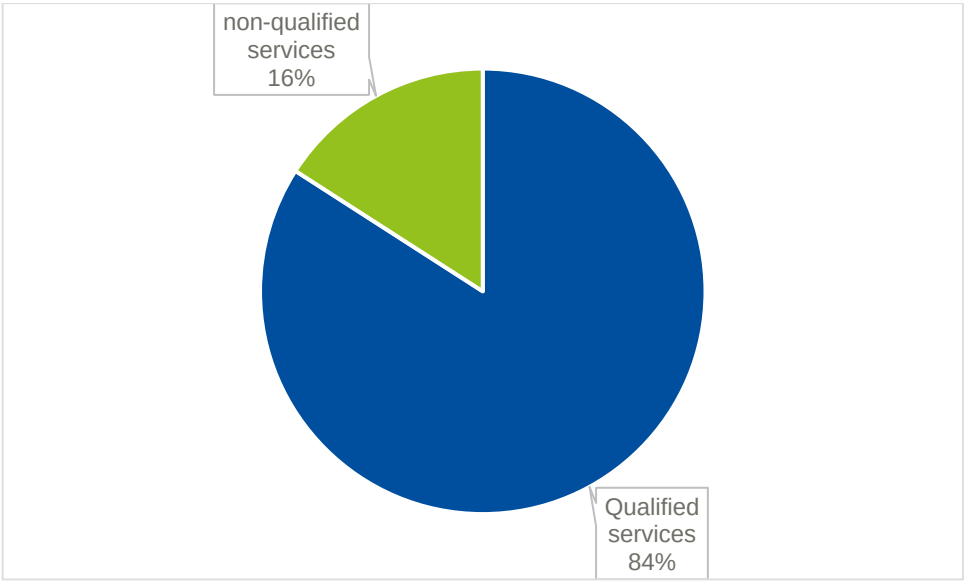


Figure 14. Reported incidents affecting qualified v non-qualified services – 2024

4. MULTIANNUAL TRENDS 2017–2024

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 2017–2024. The dataset contains a total of 287 reported incidents.

4.1 ROOT CAUSE TRENDS

Root-cause categories, i.e., system failures, human errors, malicious actions and natural phenomena, are analysed over the period from 2017 to 2024.

From 2017–2024 system failures represented 58% of all reported incidents, human errors represented 26% of all reported incidents, 15% involved malicious actions and 1% natural phenomena, as displayed in **Figure 15.**

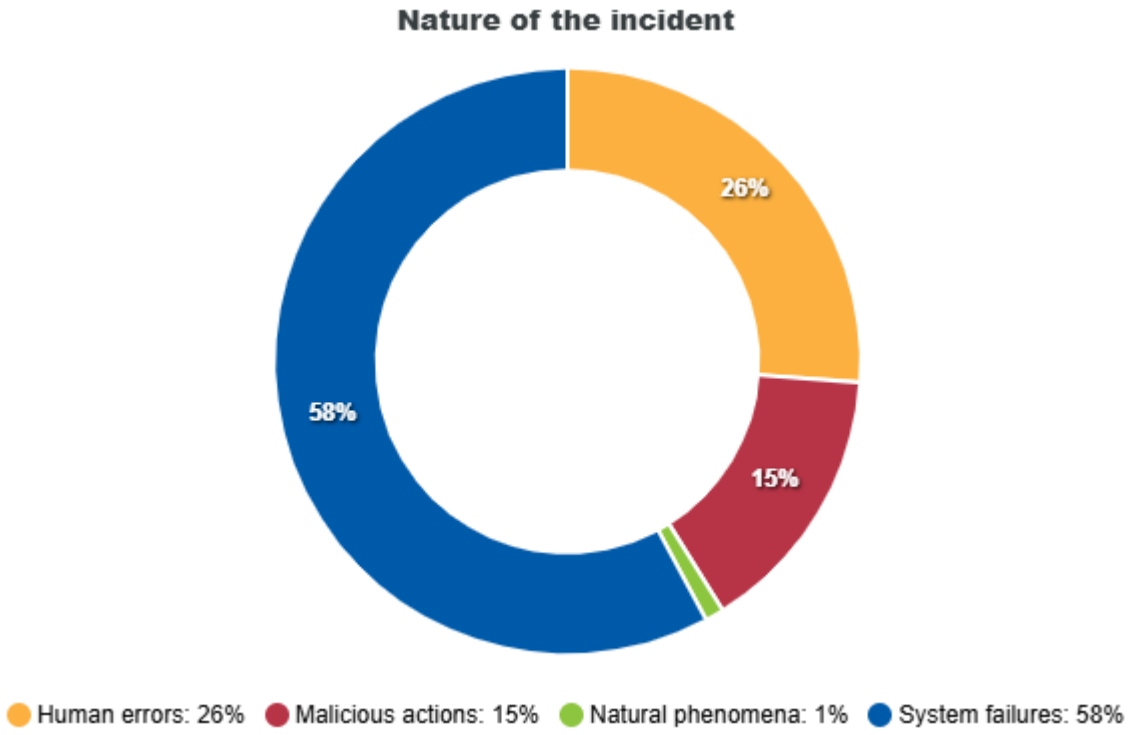


Figure 15. Nature of reported incidents – trust services security incidents in the EU (reported from 2017–2024)

Over the period of reference, out of 287 incidents reported:

- system failures accounted for 166 of all reported incidents,
- human errors accounted for 75 of all reported incidents,
- 43 involved malicious actions, and
- 3 involved natural phenomena.

Percentage trends of related incidents over the last 8 years are displayed in **Figure 16**, arranged by category.

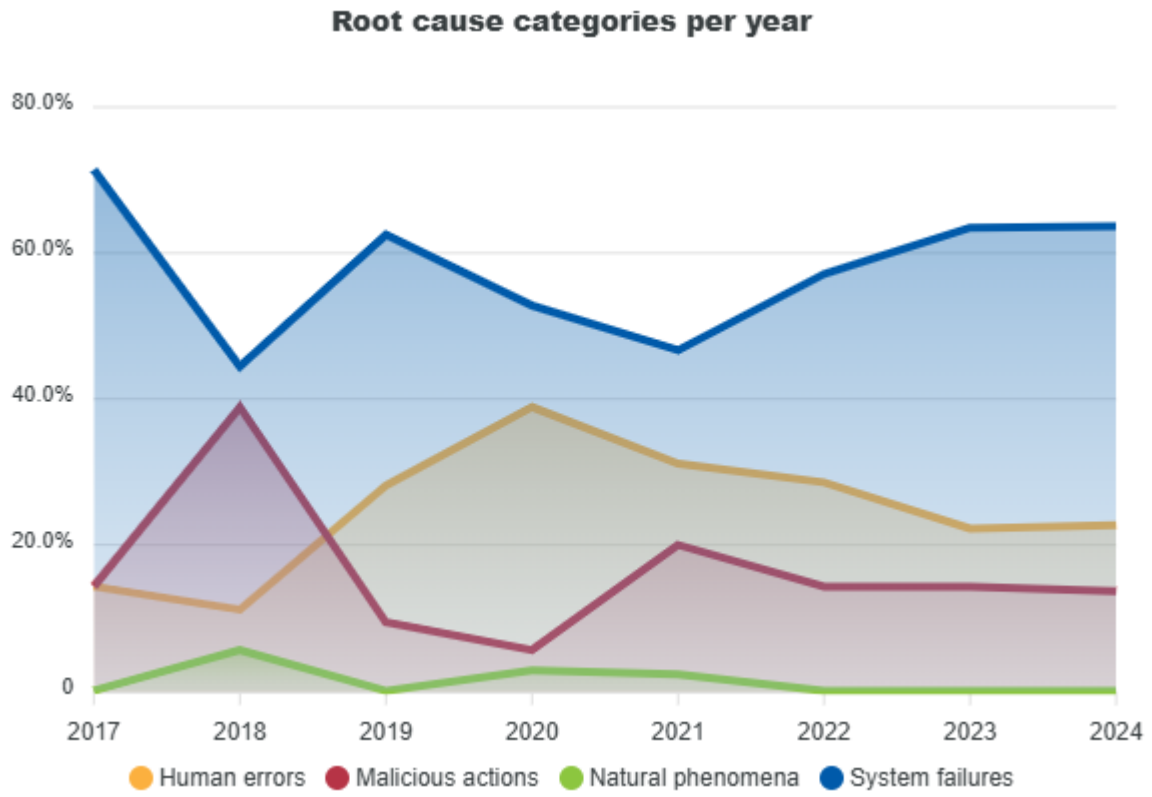


Figure 16. Root-cause categories – trust services security incidents in the EU (reported from 2017–2024)

Over the years of trust services security incident reporting, the most common root cause has been **system failures**, with a total of **166 reported incidents**. The percentage of system-failure-related incidents over the last 5 years has been steadily increasing.

Incidents concerning **human errors** have been steadily decreasing from around 40% in 2020 to 23% in 2024.

Natural phenomena is not a common root cause in trust services sector. From 2017–2024 only **three** incidents were reported, accounting for **1%** of the total. No such incidents were reported since 2022.

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 2024, malicious actions were the root cause for 14% of the reported incidents with nine incidents. Since 2022 malicious actions remain stable at around 14%.

4.2 IMPACT SEVERITY TRENDS

In the multiannual trend concerning the severity of impact, the EU cybersecurity incident taxonomy ([7]) 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 only difference now being 2024, which for the first time shows a decline[8].

It should be noted that there is a mostly linear increase in **large incidents** (in yellow) over the course of the last 5 years from 3 incidents in 2020 to 27 in 2024.

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

([8]) Here we would like to mention that this might be due to the missing reports from 6 member states at the time of writing

Looking at **large impact incidents** (in yellow) we can clearly see a continued increase, reaching 27 incidents this year, despite the drop observed in 2020.

With respect to the **very large impact incidents** reported over time they seem to settle around 2 incidents per year.

For reference in terms of reported incidents, in 2023 we had reports from 27 member states and 3 EFTA countries, while in 2024 we have reports from 21 member states and 3 EFTA countries. This therefore, has an impact on the incidents we have received and the graphs that are displayed. Furthermore, the impact assessment methodology that supports Member States in evaluating incidents should be streamlined to ensure a consistent and comparable understanding of impact across all MS.

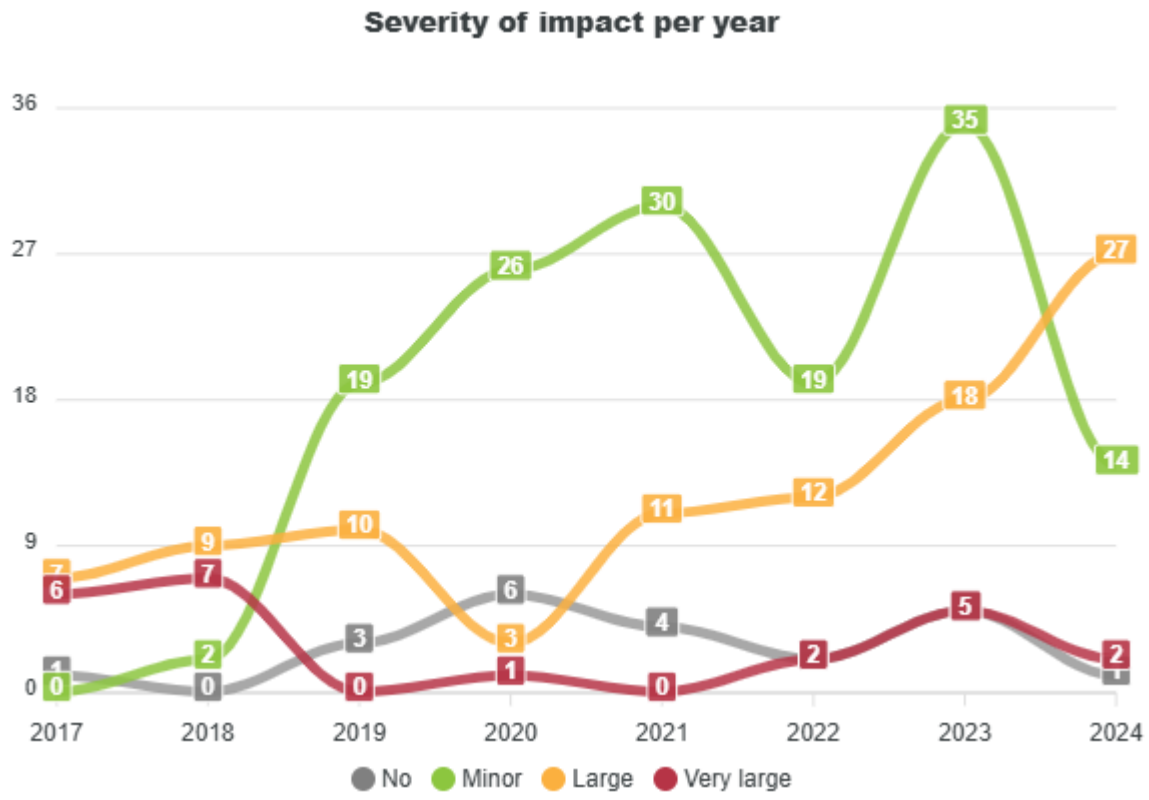


Figure 17. Severity of impact – trust services security incidents in the EU (reported from 2017–2024)

4.3 IMPACT ON SERVICES TRENDS

In this section, the impact per service from 2017–2024 for reported incidents for trust services is detailed in **Figure 18**.

It is evident that the majority of reported incidents relate to **electronic signatures**, with numbers averaging around the 86%. This is probably due to the fact that electronic signatures are used for authorization of transactions, financial or otherwise, while electronic seals are mostly used to ensure integrity of data. Additionally, automation is usually used with electronic seals, while electronic signatures are quite extensively used by humans as well, which leads to more incidents.

Electronic seals show a steady declining trend coming to the lowest share of 6% over the 8 years.

Electronic timestamps seem **to oscillate around the 11%** over the 8 years of incident reporting.

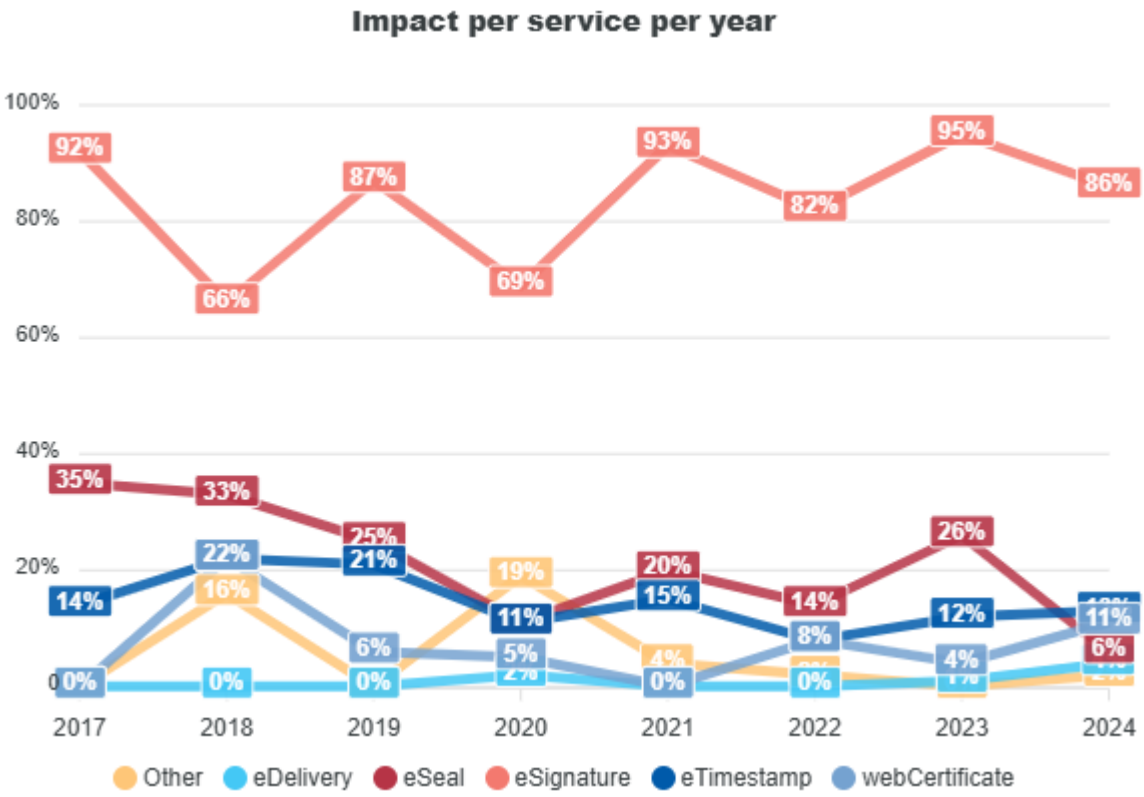


Figure 18. Impact on services – trust services security incidents in the EU (reported from 2017–2024)

5. CONCLUSIONS

The **key takeaways** from the 2024 incident reports are as follows.

- Half of the EU Supervisory Bodies – **12** out of 24 (reported) – sent their respective reports with 0 incidents reported ([9]).
- The overall impact of the incidents accounted for 618 million user hours lost which is 5 times decrease over the 2023 where **3 184 million user hours lost** were reported.
- **Malicious actions** accounted for 92% of all hours lost in 2024 with 571 out of 618 million.
- The number of large incidents continue to increase in the last 5 years.
- **Qualified trust services versus non-qualified trust services** – in 2024, 84% of total incidents had an impact on qualified trust services.

([9]) 2022: 13/27; 2021: 17/27; 2020: 19/27; 2019: 17/27; 2018: 18/27; 2017: 17/27; 2016: 26/27.

TP-01-25-015-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 978-92-9204-707-8
doi: 10.2824/2144753