enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TRUST SERVICES SECURITY INCIDENTS 2021

Annual Report

JULY 2022

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been 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 practices 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. Since 2019 it has been drafting cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

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

AUTHORS

Apostolos Malatras, Edgars Taurins, Marnix Dekker

ACKNOWLEDGEMENTS

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

LEGAL NOTICE

COPYRIGHT NOTICE

Catalogue Number: TP-AK-22-001-EN-N ISBN: 978-92-9204-581-4 ISSN: 2599-9435 DOI: 10.2824/16330

TABLE OF CONTENTS

1. INTRODUCTION 6

1.1 SCOPE 6

1.2 TARGET AUDIENCE 6

1.3 CONTENT 6

1.4 DISCLAIMER 6

2. INCIDENT REPORTING FRAMEWORK 7

2.1 OVERVIEW OF INCIDENT REPORTING PROCESS 7

2.2 INCIDENT REPORTING TOOL 7

2.3 ANONYMISED EXAMPLES OF SECURITY INCIDENTS 8

3. INCIDENT ANALYSIS 12

3.1 ROOT CAUSE CATEGORIES 12

3.2 DETAILED CAUSES 13

3.3 TYPES OF TRUST SERVICES AFFECTED 14

3.4 QUALIFIED SERVICES VERSUS NON-QUALIFIED SERVICES 17

4. MULTI-ANNUAL TRENDS 2016-2021 18

4.1 MULTI-ANNUAL TREND IN ROOT CAUSE CATEGORIES 18

4.2 MULTI-ANNUAL TREND IN SEVERITY OF IMPACT 20

4.3 MULTI-ANNUAL TREND IN IMPACT ON SERVICES 20

5. CONCLUSIONS 22

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 reporting of security breaches for TSPs in the EU. The reporting obligation consists of 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 2021*, provides an aggregated overview of the notified breaches for 2021, 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 46 incidents.

The key findings from the 2021 incident reports are summarised as follows.

- **A steady increase in notified incidents:** in 2021 notified incidents increased by around 18%, same as the growth observed in 2020. This suggests that authorities and TSPs are becoming more familiar with the process for reporting breaches and their obligations under eIDAS.
- **The number of incidents with a large impact has increased:** in 2020 only 3 incidents were characterised as having had a 'large impact' as opposed to 2021 when 11 such incidents were reported (translating into approximately a quadruple increase). Compared to previous years, it is evident that the numbers for 2020 were outliers and that the norm is a ratio of circa 25% for incidents with large impacts.

The **ratio of reported incidents concerning qualified trust services over non-qualified ones remains high**. In 2021, 80% of total incidents had an impact on qualified trust services when compared with approximately 29% of incidents reported on non-qualified trust services.

Although non-qualified trust services are widely used, not 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.

HIGHLIGHTS 2021

The number of notified incidents is steadily increasing.

The number of incidents with minor and large impacts has increased.

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

System failures account for almost half of incidents and have been the dominant root cause for the last five years of incident reporting.

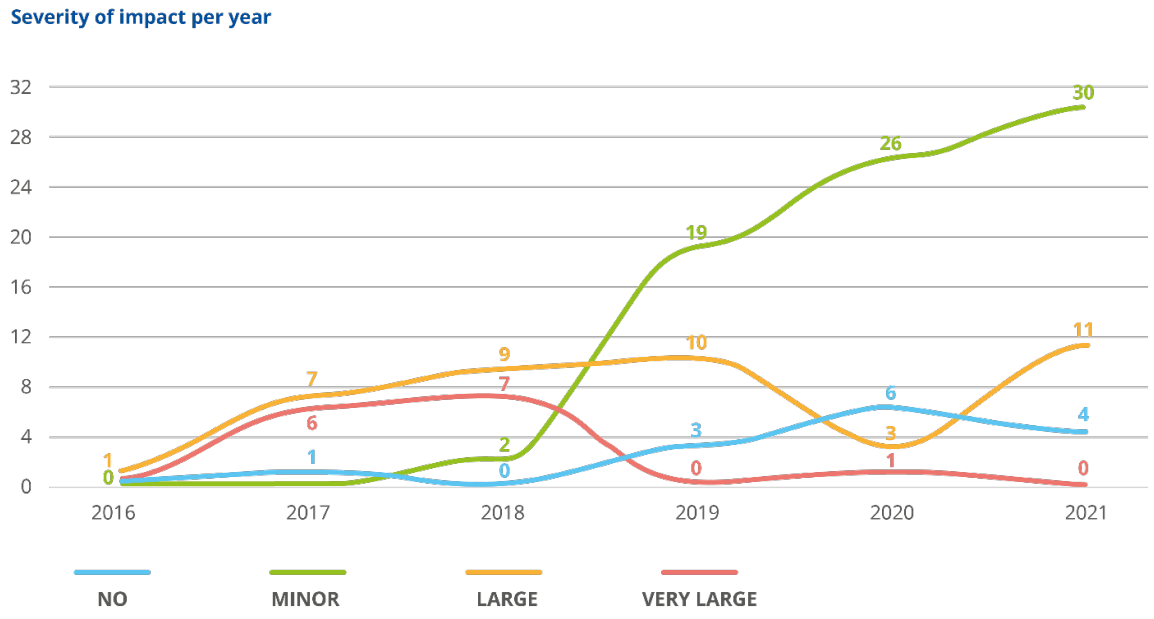
2021 witnessed an increased in incidents caused by malicious actions (20%).

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. 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.

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 2020, 2021 witnessed an improvement in this direction with 9 incidents affecting solely non-qualified services being reported.

The impact on subservices is mainly divided between certificate management (63% of the incidents) and certificate generation (65% of the incidents), with a notable (more than 50%) increase compared to 2020.

Approximately 66% (30 incidents) of the reported incidents were rated as minor, showing stabilisation compared to 2020. No disastrous incidents were reported in 2021, whereas a significant increase was observed for incidents with a large impact, which quadrupled compared to 2020 and returned to 2018-2019 values. Furthermore, relative stability in the number of minor incidents has been observed, indicating that the incident reporting mechanism has become more familiar to the providers and they are reporting more incidents regardless of their severity.



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

Currently the European Commission, Member States and the European Parliament are discussing policy changes. Last year the Commission proposed to integrate Article 19, the

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

security requirements for TSPs into a revised NIS (Network and Information Security) Directive. The goal of this Commission proposal, the NIS2 proposal, is to simplify EU cybersecurity legislation and to ensure that there is a similar approach across the various sectors, including the telecom sector and the trust services sector, which are currently addressed under separate pieces of legislation. This year the Commission will also make a proposal for a new eIDAS regulation.

ENISA will continue to support national supervisory bodies with the implementation of breach reporting under Article 19 of eIDAS and to work towards making this process more 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. 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 2021. This annual report marks the sixth round of security incident reporting in the EU's trust services sector, covering security incidents during 2021.

1.1 SCOPE

This report covers incidents reported by authorities under Article 19 of the eIDAS regulation.

1.2 TARGET AUDIENCE

The audience for this report includes experts in national authorities and experts in the sector.

1.3 CONTENT

This document is structured as follows: in section 2, the policy context is briefly summarised as is the underlying eIDAS reporting framework and an overview of the types of incidents reported is provided using anonymised 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 2016-2021 are highlighted. In Section 5, conclusions and observations based on the available data are drawn.

1.4 DISCLAIMER

This document only contains aggregated and anonymised information about incidents and does not include details about individual countries or individual trust service providers.

Detailed discussions about the reported security incidents take place in the ENISA Article 19 expert group, which is an informal group of experts from national supervisory bodies focusing on the practical implementation of Article 19. The group is currently chaired by a representative from RTR, the Austrian regulatory authority. ENISA acts as the secretariat and supports the group with analysis, drafting, logistics, etc.

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, can be consulted at https://eur-lex.europa.eu/eli/reg/2014/910/oj

2. INCIDENT REPORTING FRAMEWORK

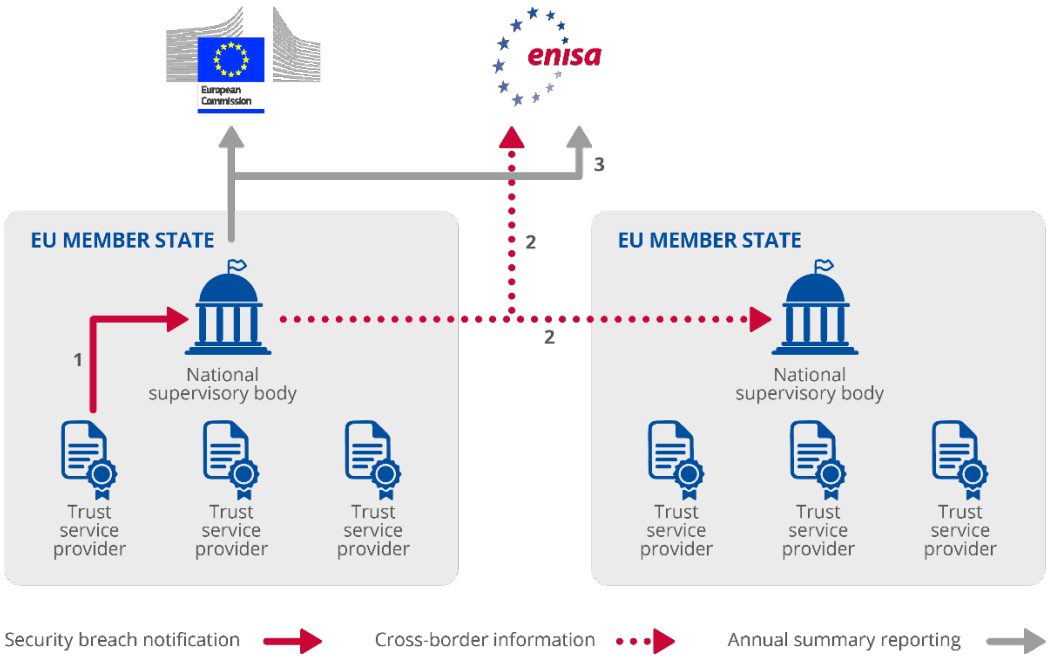
In this section, we give an overview of the formats and procedures for the reporting of incidents (breaches) under Article 19 of the eIDAS regulation.

2.1 OVERVIEW OF INCIDENT REPORTING PROCESS

The mandatory notification process for security breaches has three steps as shown in the figure below:

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

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.



2.2 INCIDENT REPORTING TOOL

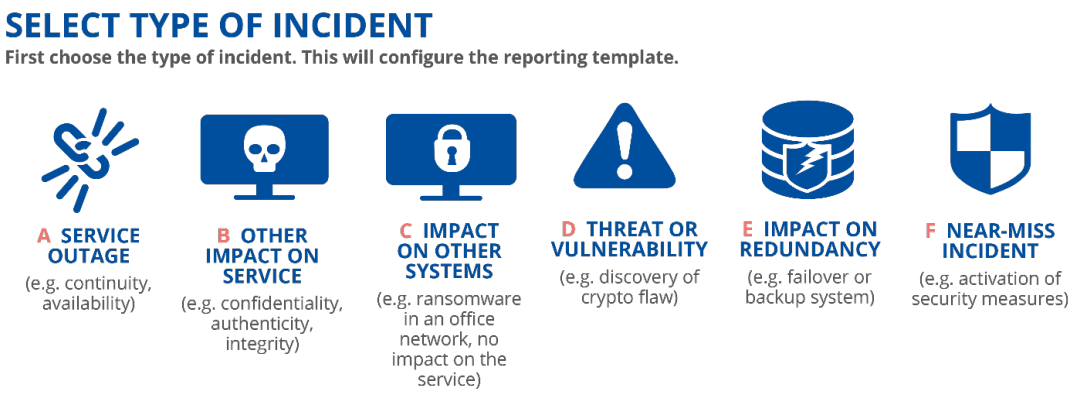
Experts from the national authorities have access to the ENISA CIRAS (Cybersecurity Incident Reporting and Analysis System) incident reporting tool[3], where they can upload incident reports and search for and study specific incidents.

We briefly introduce the reporting template. The template starts with a 'type' selector and has 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] See https://ciras.enisa.europa.eu/

3. Details about the incident: detailed information about the incident, a short description, the types of services, the types of assets, the severity level etc.



- 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 a shared session. This leads to the interception of the media (voice, pictures, video, files, etc.) through a man-in-the-middle attack*. This incident would be categorised as a type B incident.

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

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

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

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

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

2.3 ANONYMISED EXAMPLES OF SECURITY INCIDENTS

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

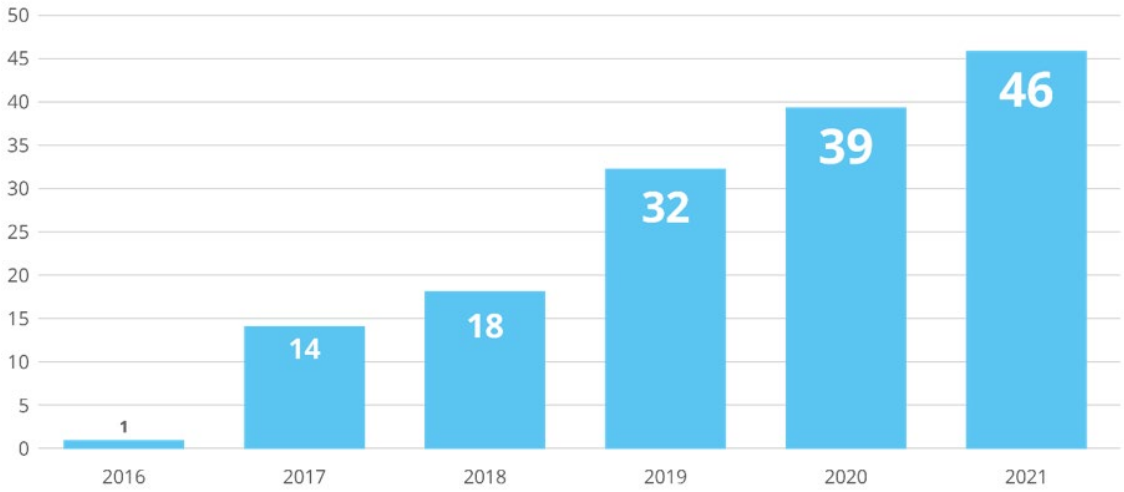
Incident example 4	
Incident type	B-Other impact on core service
Service affected	eSignature
Root cause	Malicious action
Technical causes	Malware and viruses
Assets affected	Generation and validation of signatures/seals platform
Comment	The incident concerns the leak of credentials for qualified signatures. 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 2021 annual summary reporting by the 27 EU Member States and 3 EEA countries participating in this process included 46 security incidents in total[4]. This is the sixth round of annual summary reporting since eIDAS came into force on the 1 July 2016.

Figure 1: Number of reported incidents from 2016 - 2021 under Article of the eIDAS regulation



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

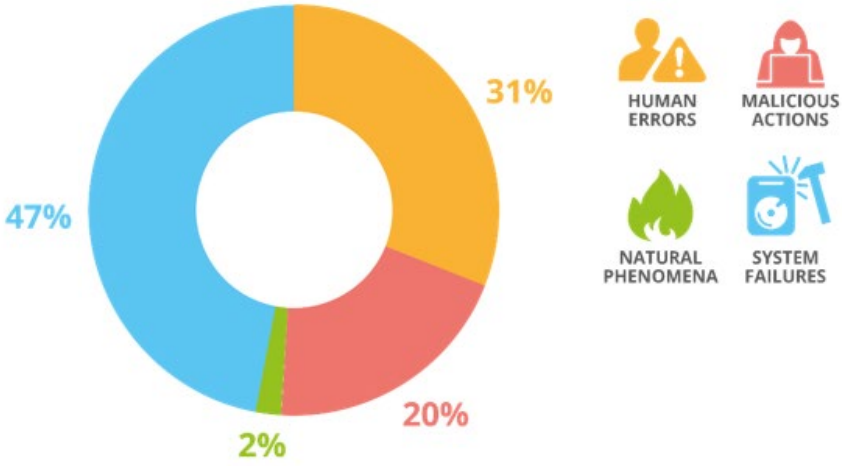
3.1 ROOT CAUSE CATEGORIES

Figure 2 below shows the distribution of the incidents according to their underlying root cause. We categorise 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 almost half of the total reported trust services incidents (47%, around 22 incidents). Typically, system failures are due to either hardware failures or software bugs.
- Almost 31% of incidents were categorised as human errors.
- Around 20% of the incidents were flagged as malicious actions.
- Natural phenomena accounted for 2% of the reported incidents.

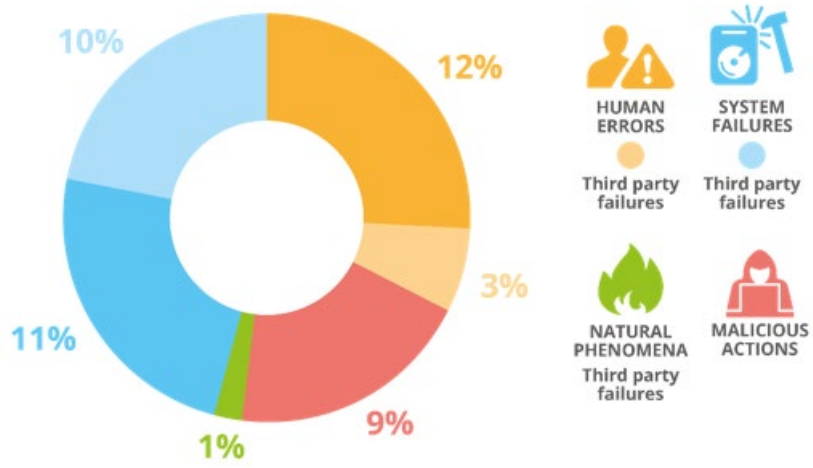
[4] Note that one of the reported incidents was indicated as type D-Active threats or vulnerabilities and is not included in the analysis.

Figure 2: Root causes of TSP security incidents – 2021



We also keep track of third-party failures, i.e. when the incident really originated at a third party. For 2021, 14 incidents out of 45 were flagged as third-party failures (31.11%), well above the 14% of incidents flagged as third-party failures in 2020. This finding further 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. Out of the 14 third-party failures reported in 2021, 10 were categorised as system failures, 3 as human errors and 1 as natural phenomena (arguably a natural phenomenon should not be not classified as third-party failure). Figure 3 provides the full picture.

Figure 3: Root causes – third party failures – 2021



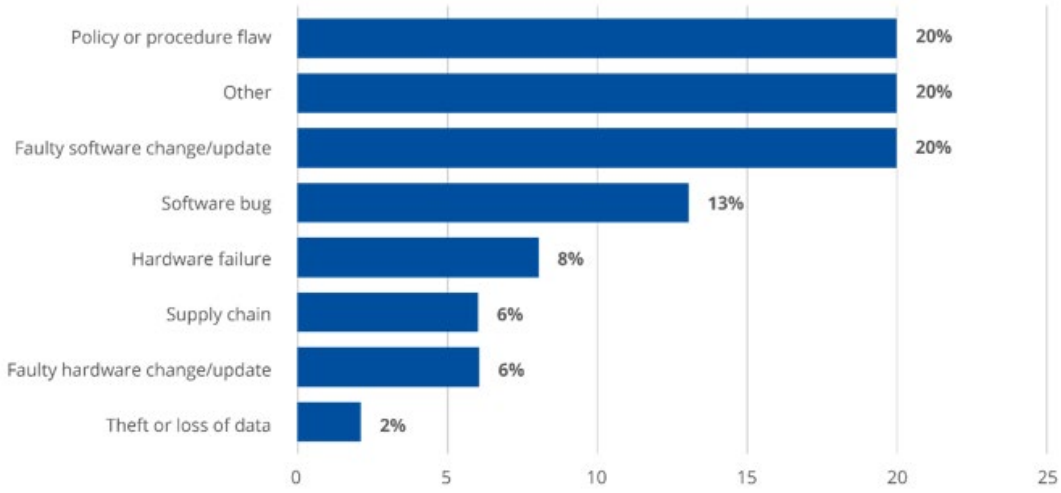
3.2 DETAILED CAUSES

The two most common detailed causes of incidents were flaws in an organisation's policy or procedures and faulty software changes/updates, with each one accounting for 20% of the incidents, followed by other undefined causes (20%) and software bugs (13%).

It is important to note that an incident is often not triggered by only one cause but can involve multiple detailed causes (i.e. a chain of events). Interestingly, supply chain causes that were first introduced in 2021 accounted for 6% of reported incidents, highlighting the increasing threat caused by supply chains as underlined in the ENISA Threat Landscape for Supply Chain[5] that was published in 2021.

The full breakdown of detailed causes[6] for reported incidents may be seen in Figure 4.

Figure 4: Detailed causes of trust services security incidents - 2021



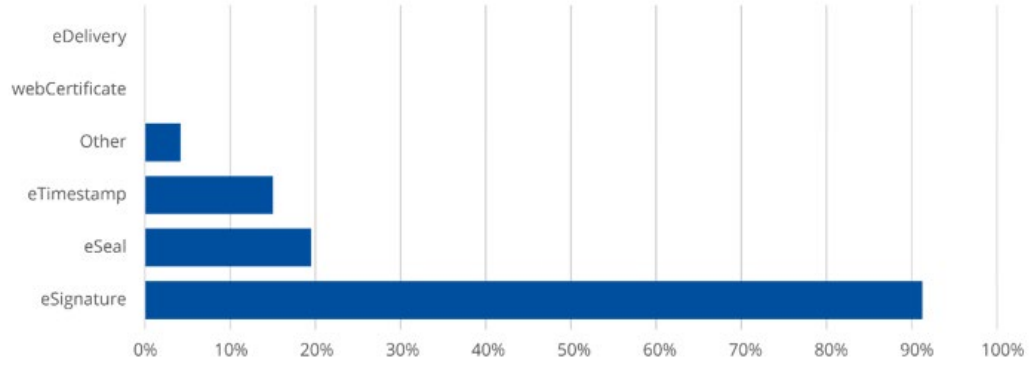
3.3 TYPES OF TRUST SERVICES AFFECTED

Most of the reported incidents (91.3%) had an impact on electronic signatures as can be seen in Figure 5. This is a significant increase compared to 69% recorded in 2020. Interestingly enough, no reported incidents affected web certificates or electronic delivery services. But 19.57% of reported incidents involved electronic seals and 15.22% electronic timestamps, both exhibiting a 50% increase compared to 2020. It needs to be noted that several incidents affected multiple services, hence the numbers in the figure correspond to more than 100%.

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

[5] See https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
[6] The remaining 5% refers to specific detailed causes such as ransomware (~2%), DDoS (~2%) and malware and viruses (~2%).

Figure 5: Impact of incidents on trust services - 2021



For each incident we keep track of the underlying subservices affected. Most incidents have an impact on the generation of signatures/seals/timestamps (65.22% up from 42% in 2020) or certificate management (63.04% up from 47% in 2020) (see Figure 6). The impact on the validation of subservices accounts for 15.22%. Once again, impact on multiple subservices may be reported for incidents, hence the numbers in the figure account for more than 100%.

Figure 6: Impact of incidents on trust subservices – 2021

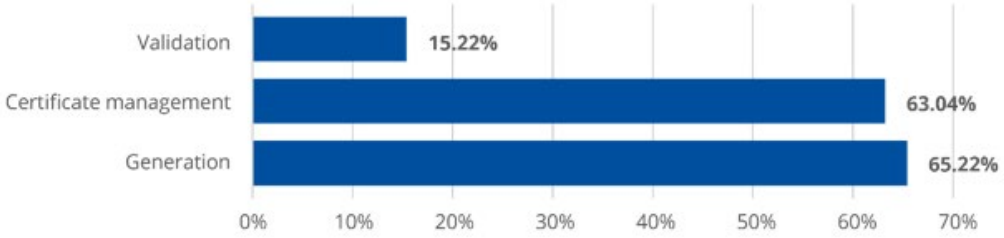
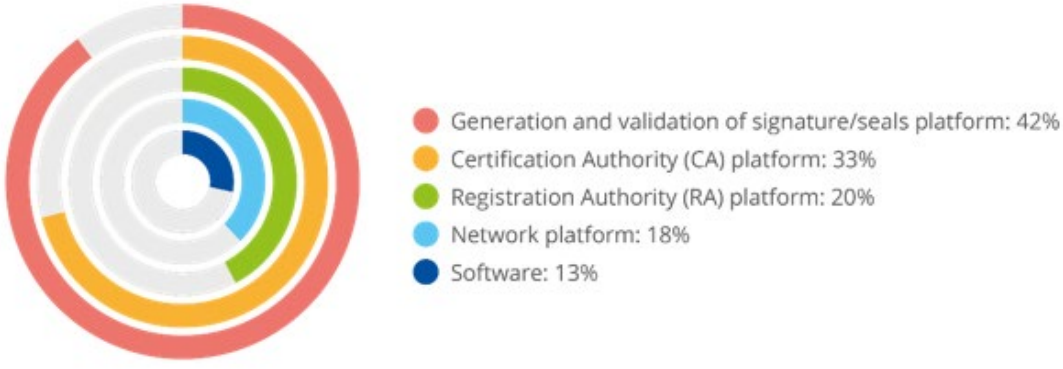


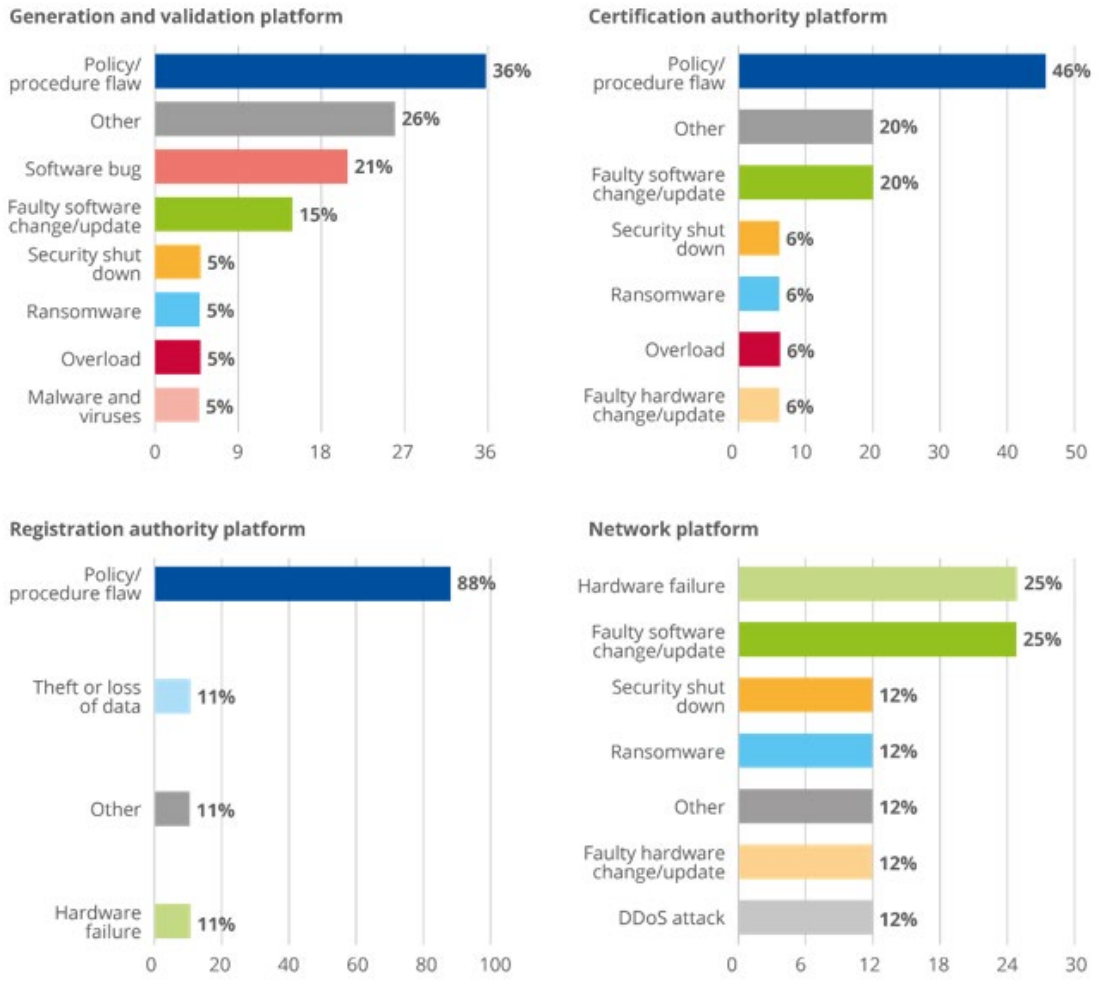
Figure 7: Technical assets affected – TSP security incidents 2021



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 (42%)

and the Certification Authority (CA) platform (33%). It is interesting to note that in 20% of the reported incidents, the affected asset involved the registration authority's platform and in 18% of the cases the network platform. The dispersion of affected assets calls for a holistic approach when it comes to the 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 8: Breakdown of technical causes per affected asset – TSP security incidents 2021



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 or seals, 36% of the incidents report flaws in policies and procedures as the root cause and 21% software bugs. Conversely, in the case of the Certification Authority's platform, the two main root causes are flaws in processes or procedures (46%) and faulty software updates (20%).

The registration platform incidents have an overwhelming 88% of flaws in policies and procedures as their root cause, followed by 11% due to theft of data and 11% due to hardware failures, whereas the network platform has 25% hardware failures, 25% faulty software changes and 12% of ransomware, as well as a 12% of DDoS attacks as root causes. This breakdown is extremely important in order 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 80% of total security incidents affecting trust services had an impact on qualified services (i.e. the creation of qualified signature certificates, the creation of qualified seal certificates, etc.), while only a quarter of the incidents affected a non-qualified service. Again, it is important to note that one incident report could involve multiple trust services, which explains why the percentages in the Figure 9 below add up to more than 100%.

Figure 9: Reported Incidents affecting Qualified v Non-qualified services 2021

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.

4. MULTI-ANNUAL TRENDS 2016-2021

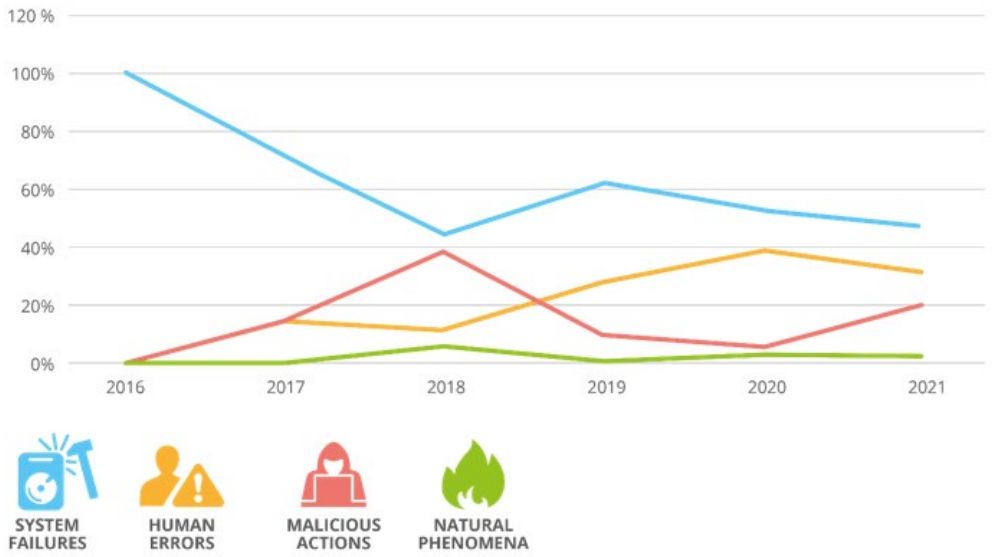
ENISA has been collecting and aggregating incident reports on trust services since 2016. In this section, we look at multi-annual trends over the last six years, covering the period from 2016 to 2021. The total dataset contains 150 reported incidents.

4.1 MULTI-ANNUAL TREND IN ROOT CAUSE CATEGORIES

Over the last few years of reports on security incidents affecting trust services - as displayed in Figure 10 - the most common root cause has been system failures. These add up to 54% as shown in Figure 11, with human errors representing 28% of all reported incidents, 16% involving malicious actions and 2% natural phenomena. One can observe a relative stabilisation in the number of incidents related to system failures over the last 6 years, starting from a peak of 100% in 2016 (first year of trust services annual incident reporting) to 52.8% in 2020 and 46.7% in 2021.

Note that we observe the same pattern in electronic communication services[7], where system failures account for almost two thirds (65%) of total incidents (926 out of 1432 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.

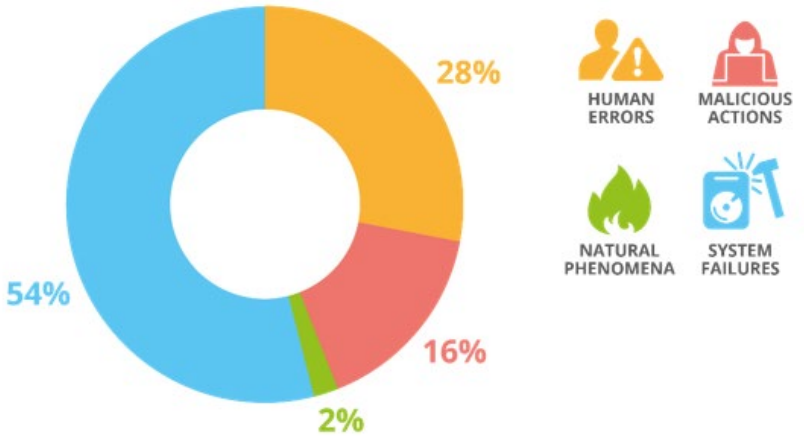
Figure 10: Root cause categories – Trust services security incidents in the EU (reported over 2016-2021)



Moreover, incidents concerning human errors are being reported at an increasing rate, with 28.1% in 2019, 38.9% in 2020 and 31.1% in 2021. Malicious actions vary over the years, with the peak observed during 2018 (38.9%) and a value as low as 5.6% during 2020. During 2021, malicious actions were the root cause for 20% of the reported incidents.

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

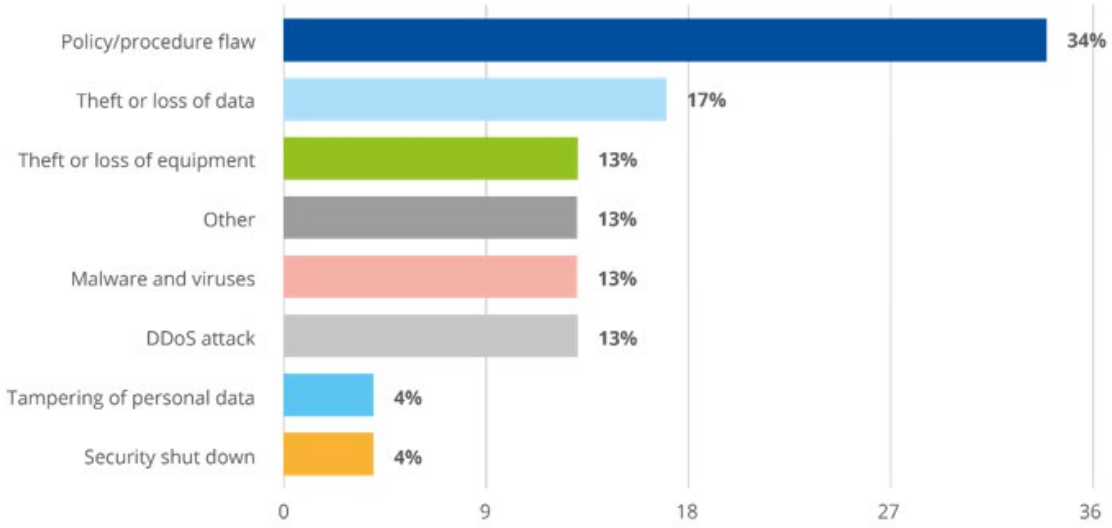
Figure 11: Nature of reported incidents – Trust services security incidents in the EU (reported over 2016-2021)



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 (34%), theft/loss of data (17%), theft/ loss of equipment (13%), malware (13%) and DDoS attacks (13%).

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 the reports of trust services security incidents.

Figure 12: Detailed technical causes – Trust services security incidents in the EU (reported over 2016-2021)



[88] See https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

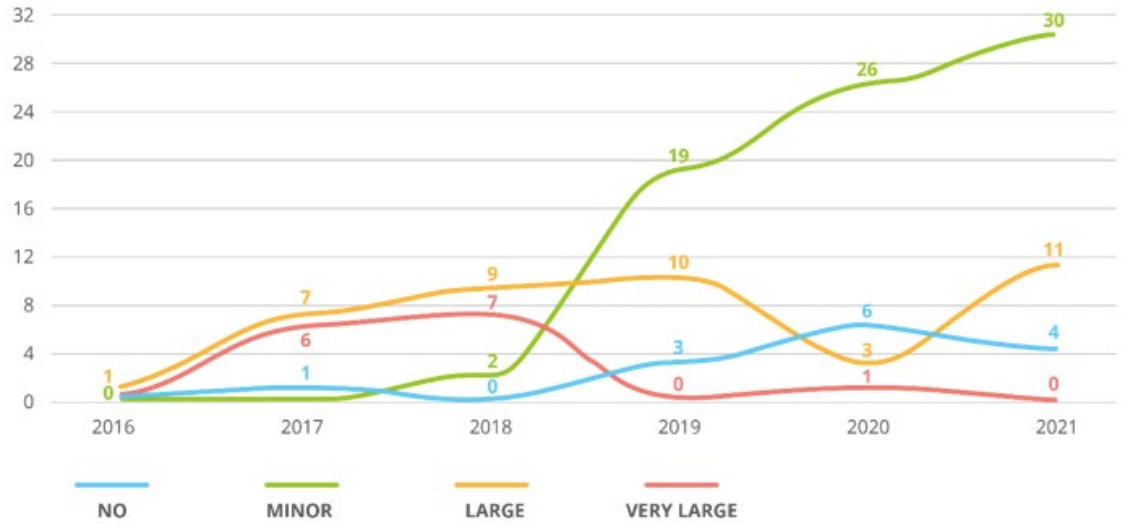
4.2 MULTI-ANNUAL TREND IN SEVERITY OF IMPACT

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 a large impact increased significantly over the course of 2021 compared to the drop that was observed in 2020. It seems that the drop that was observed in 2020 was an outlier, and about 23% of incidents every year are reported as having a large impact. It is interesting to see that there has been a rather linear increase in minor incidents over the course of the last few years.

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

Figure 13: Severity of impact – Trust services security incidents in the EU (reported over 2016-2021)

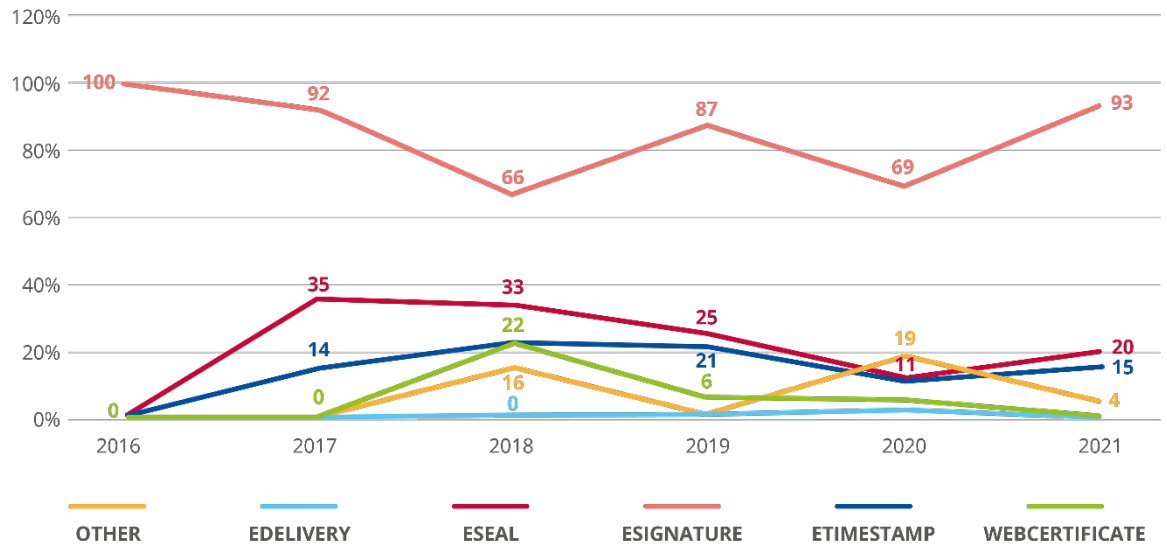


4.3 MULTI-ANNUAL TREND IN IMPACT ON SERVICES

When considering the impact per service during the course of 2016-2021 for reported incidents for trust services, Figure 14 provides an overview. It is evident that the majority of reported incidents relate to electronic signatures, with numbers ranging consistently above 66% (2018) and reaching peaks of 100% in 2016 and 93% in 2021.

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

Figure 14: Impact on services – Trust services security incidents in the EU (reported over 2016-2021)



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

5. CONCLUSIONS

The key takeaways from the 2021 incidents are:

- **A steady** lower level of severity confirms that TSPs are becoming more familiar with the incident reporting process and that they are reporting more incidents, even if they are less severe.
- **Qualified trust services versus non-qualified trust services:** the ratio of reported incidents concerning qualified trust services over non-qualified ones remains high. In 2021, 80% of total incidents had an impact on qualified trust services when compared with approximately 29% of incidents reported as having impacted non-qualified trust services. Although non-qualified trust services are widely used, not 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 improvements in this particular area were noted compared to 2020 when the observation was first made. This is a testament to the value of the work on incident reporting and related analysis, which had a direct positive impact on the overall process.
- **System failures (47%) remain the dominant root cause** and the second most dominant are human errors at 31%. A notable increase in malicious actions (20%) was observed in 2021.
- **Root causes for malicious actions are consistent with the findings of the 2021 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 reporting on security incidents relating to trust services.

We conclude with some other observations:

- **Reporting of threats/vulnerabilities in 2021:** in 2021 authorities reported only one threat/vulnerability. This vulnerability, 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 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 nine purely non-qualified trust services incidents were reported in 2021, 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 working on a proposal for a revised eIDAS regulation. In 2020, the Commission also made a proposal for a revised NIS (Network and Information Security) Directive, i.e. NIS2, which proposes the integration of eIDAS Article 19 with

the NIS Directive and there was a political agreement on the text in May 2022. Both policy proposals are expected to deliver important improvements. These policy changes present an opportunity to address some of the gaps in policy, for example, the issue of supervision of and reporting by the providers of non-qualified services. We look forward to supporting the Commission and the EU Member States with implementing eIDAS security incident reporting in an efficient and effective manner and contributing to consolidated incident reporting under NIS2.

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.

TP-AK-22-001-EN-N

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

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

enisa.europa.eu

ISBN 978-92-9204-581-4
ISSN 2599-9435
DOI: 10.2824/16330