enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

SHA256:GLmuOzvG5EGeRV9KE1WK8tRf3nlc41k/5jRgbTZDpTo
security of electronic trust services in europe
eIDAS §19

TRUST SERVICES SECURITY INCIDENTS 2018

Annual Report

JULY 2019

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 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. Since 2019, it has been drawing up 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 resilience@enisa.europa.eu
For media enquires about this paper, please email press@enisa.europa.eu

AUTHORS

Aggelos Koukounas, Eleni Vytogianni, Marnix Dekker

ACKNOWLEDGEMENTS

We are grateful for the review and input received from the experts in the ENISA Article 19 Expert Group which comprises national supervisory bodies (SBs) from all EU and EFTA 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 the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881.
This publication does not necessarily represent 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

Catalogue Number: TP-AK-19-001-EN-N, ISBN: 978-92-9204-299-8, DOI: 10.2824/540225

TABLE OF CONTENTS

EXECUTIVE SUMMARY

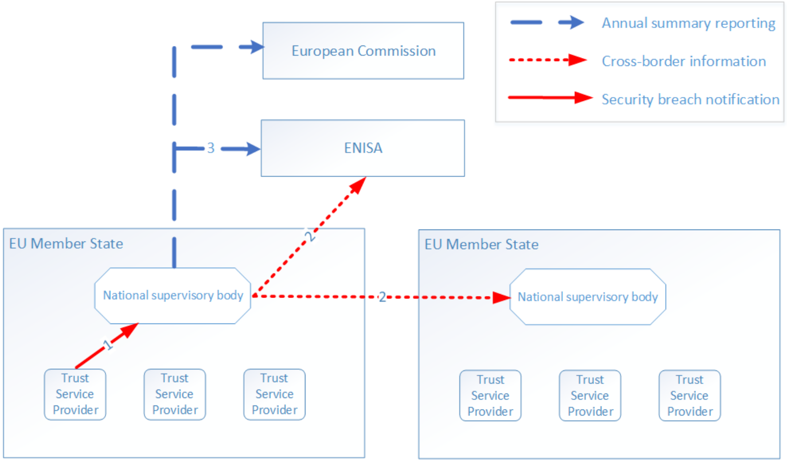
Electronic trust services are a range of services around digital signatures, digital certificates, electronic seals, timestamps, etc. which are used in electronic transactions, to make them secure. eIDAS, an EU regulation, is the EU wide legal framework ensuring interoperability and security of these electronic trust services across the EU. One of the goals of eIDAS is to ensure that electronic transactions can have the same legal standing as traditional paper based transactions. eIDAS is important for the European digital market because it allows businesses and citizens to work and use services across the EU. The eIDAS regulation was adopted in July 2014 and came into force in 2016.

Article 19 of eIDAS introduces *mandatory security breach notification* requirements for TSPs in the EU:

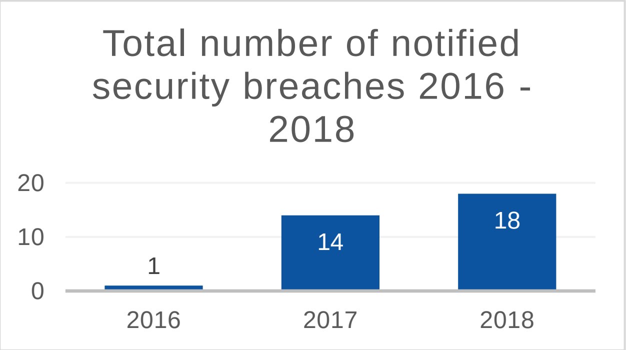
- Trust service providers notify the national supervisory body about security breaches with significant impact.
- National supervisory bodies inform each other and ENISA if there is cross-border impact.
- National supervisory bodies send *annual summary reports* about the notified breaches to ENISA and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

MALICIOUS ACTIONS

Malicious actions have been increasing rapidly since last year (7% of the total in 2017) and now account for almost two fifths of the reported incidents (39% of the total).



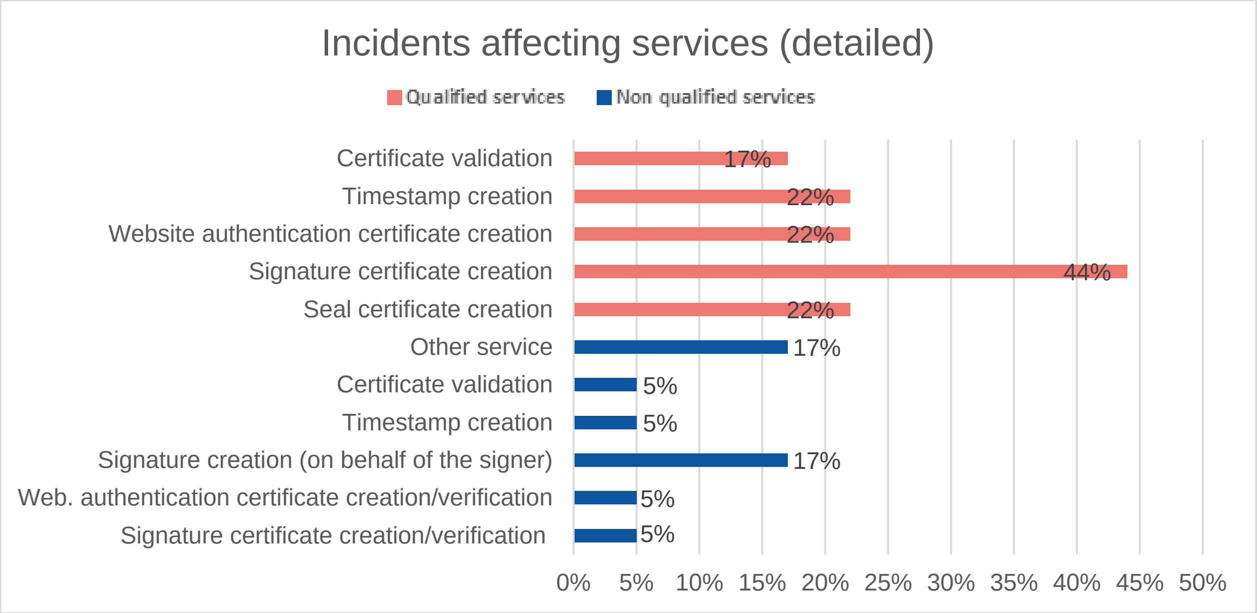
This document, the Annual Report Trust Services Security Incidents 2018 gives an aggregated overview of these breaches, showing root causes, statistics and trends. It marks the third round of security incident reporting for the EU's trust services sector. The annual summary reporting for 2018 totalled 18 incident reports, i.e. incidents with significant impact on the trust services. A total of 28 EU countries and one 1 EFTA country take part in annual summary reporting. We expect a further increase of notified incidents, due increased adoption of trust services market and growing familiarity with this breach reporting process:



The key statistics relating to the 2018 incidents are:

- **Malicious actions and system failures are the dominant root causes of reported incidents**: In the case of system failure, the corresponding percentage (39% of the total) is consistent with the previous year (36% of the total in 2017). Malicious actions have been increasing rapidly since last year (7% of the total in 2017) and now account for almost two fifths of the reported incidents (39% of the total).

- **A few but critical security breaches with cross border impact**: Just under a quarter of the reported incidents had a cross border impact. Although the ratio is small, the seriousness of the incidents was high as 75% of them were classified as level 4 (severe) and 5 (disastrous) in terms of severity. The latter highlights the importance of cross-border collaboration and information sharing among the MS.
- **Qualified e-signatures certificates creation the most affected service**: Roughly, half of the incidents reported affected the qualified creation of qualified certificates for e-signatures.
- **Most of incidents had significant impact, just one was disastrous**: Half of the incidents were submitted as "severity level 3" (significant impact) but only a minor 5% of the total incidents reported (one incident) was characterized as disastrous.



ENISA will provide advice and input on the upcoming eIDAS review by the Commission, due mid-2020. The Agency will also continue to support the national supervisory bodies with implementing the breach reporting under Article 19 eIDAS and to work towards making this process efficient and effective, yielding useful data, for the supervising bodies, for the authorities of other sectors, as well as for the trust service providers and the organisations relying on these trust services.

1. INTRODUCTION

According to Article 19 of the eIDAS Regulation[1], Electronic Trust Service Providers in the EU have to notify the national supervisory bodies in their country about security incidents. Annually the supervisory bodies send summaries of these incident reports to ENISA. Subsequently ENISA publishes an aggregated overview of these security incidents. This document gives an aggregate overview of the security incident reports submitted by the supervisory bodies over 2018.

This annual report marks the third round of security incident reporting in the EU's trust services sector, covering the security incidents of 2018.

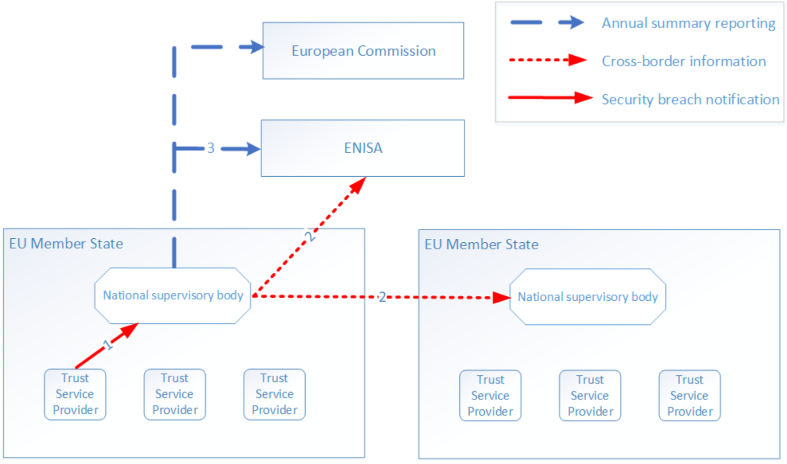
This document only contains aggregated and anonymized information about incidents and does not include details about individual countries or individual trust service providers. Detailed discussions about the reported security incidents take place in the ENISA Article 19 expert group, which is an informal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

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

2. INCIDENT REPORTING FRAMEWORK AND EXAMPLES OF INCIDENTS

Article 19 of eIDAS requires trust service providers in the EU to assess risks and take appropriate security measures to mitigate security breaches. Article 19 also introduces *mandatory security breach notification* requirements these providers:

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



We give some specific examples of incidents to give an idea of the kind of incidents, which were notified to the national supervisory bodies:

- **A human error in issuing qualified certificates**
  Duration: months
  Services affected: qualified creation of qualified certificates for e-signatures, Cause: human error
  Level of severity: 3 – significant

  A TSP issued two qualified certificates whose subject contained the name of the registration officer instead of the persons to whom the certificates should have been issued. There was no impact on personal data except the registration officer's name. The certificates were revoked and the TSP informed all registration authorities about possible sources of error in the process of issuing a qualified certificate. Moreover, the registration platform was changed so that it is no longer possible that a registration officer issues a qualified certificate to him/herself.

- **Attack by DDoS against hardware provider IP addressing**
  Duration: minutes
  Services affected: qualified creation of qualified certificates for e-signatures, e-seals,

Article 19 of eIDAS requires trust service providers in the EU to assess risks and take appropriate security measures to mitigate security breaches.

website authentication and qualified creation of qualified e-timestamps
Cause: malicious actions
Level of severity: 4 – severe

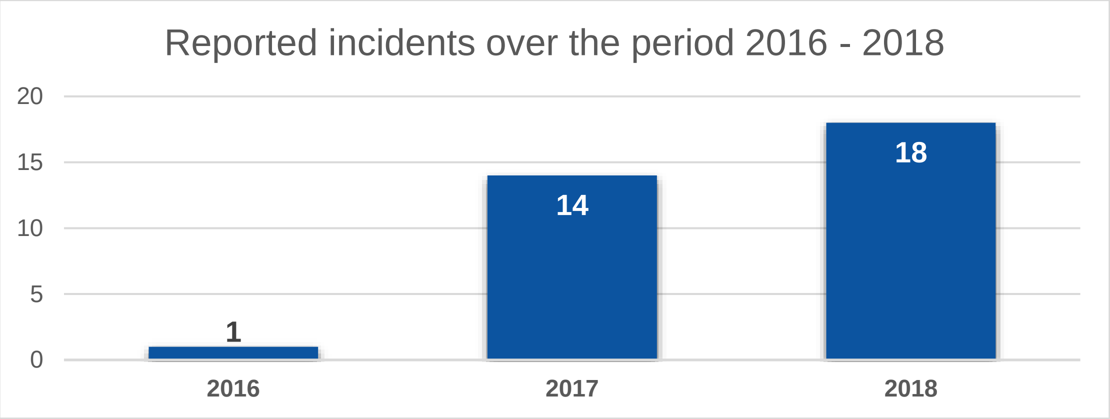
A DDoS attack against hardware provider IP addressing caused saturation phenomena in the links with the international carriers resulting in high use of the links with the national carriers. The incident had a cross border impact. The provider informed all affected customers and afterwards contacted the hardware provider to open a ticket.

- **Network cable damage caused unavailability of trust services for roughly a day**
  Duration: hours
  Services affected: qualified creation of qualified e-timestamps
  Cause: third party failures,
  Level of severity: 4 - severe

  Damage to a network cable, was caused by fire of a nearby electric cable, and led to unavailability of trust services for almost 100 subscribers. The incident had no impact on personal data. Users and internet service providers were informed after incident detection.

3. ANALYSIS OF REPORTED INCIDENTS

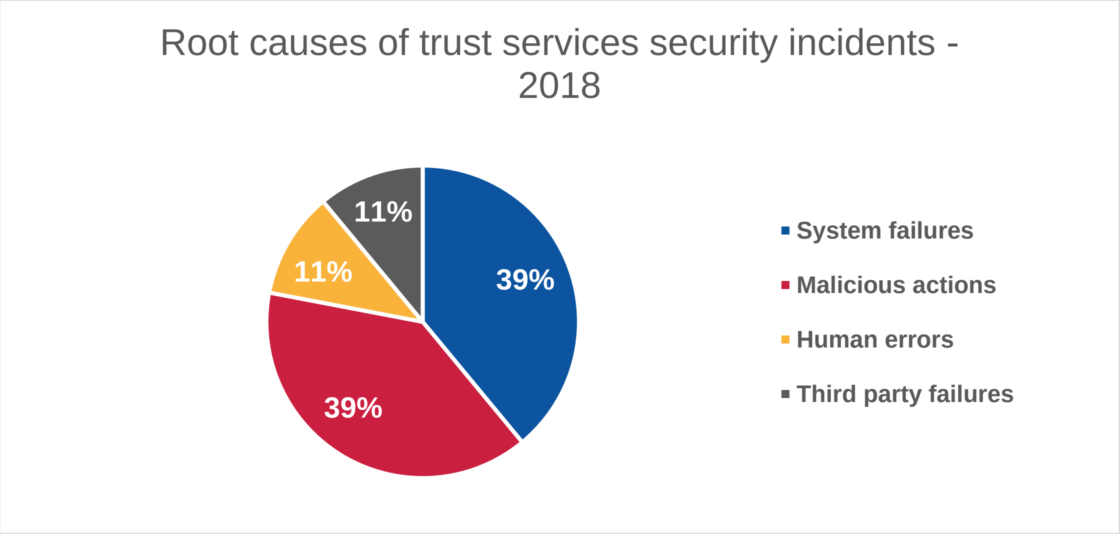
The 2018 annual summary reporting, by the 28 EU Member States and 1 EFTA country participating in this process, included in total 18 security incidents[2]. This is only the third round of annual summary reporting, because eIDAS came into force only recently, on the 1st of July 2016.



We expect the number of notified security breaches to continue to increase as the trust services market continues to grow and providers become more familiar with the breach reporting process.

3.1 ROOT CAUSE CATEGORIES

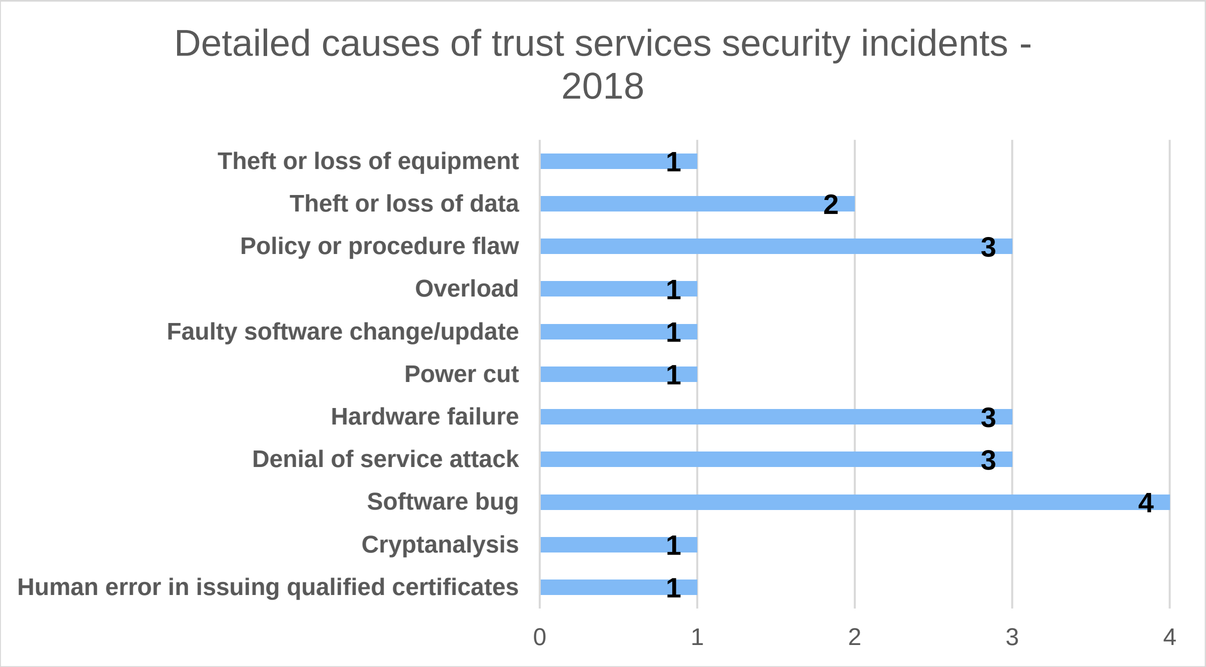
For 2018 the most common root causes of security incidents were system failures (7 incidents, 39% of the total) and malicious actions (7 incidents, 39% of the total). The latter is significantly higher than in 2017 when malicious actions accounted for just one incident. Only a tenth of the incidents are third party failures, another tenth are human errors.



[2] Note that two of the reported incidents were indicated as level 2 severity (insignificant impact) and included in the analysis

3.2 DETAILED CAUSES

The four most common causes of incidents are software bugs, hardware failures, DDoS attacks and policy/procedure flaws.

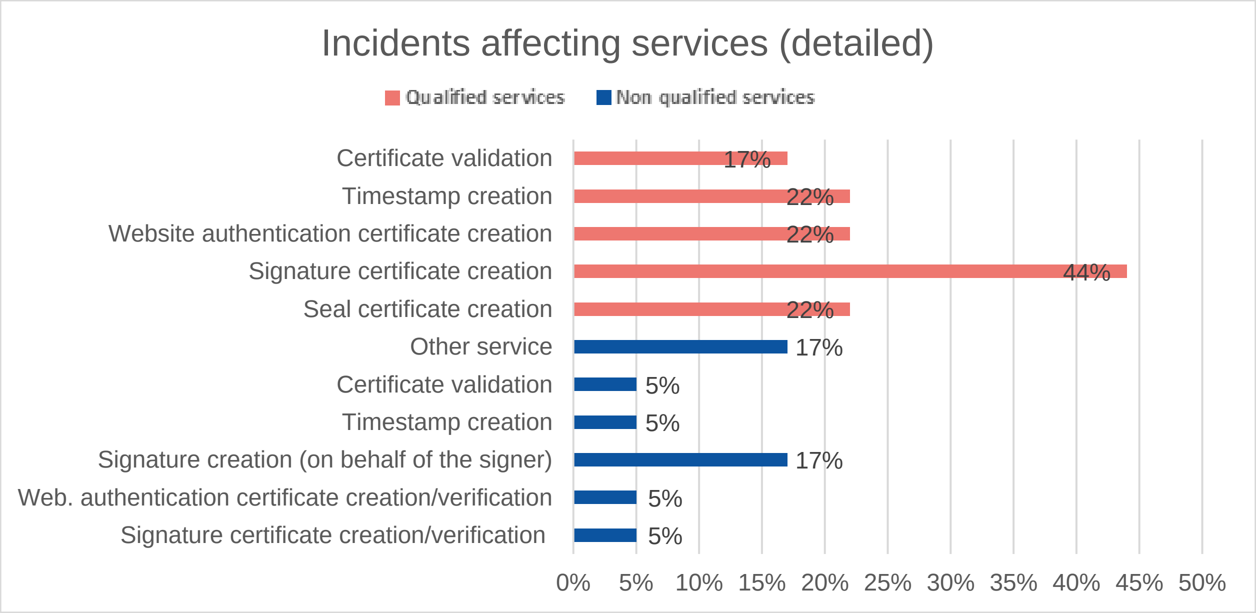


3.3 SERVICES AFFECTED

In this section we look which services were impacted by incidents.

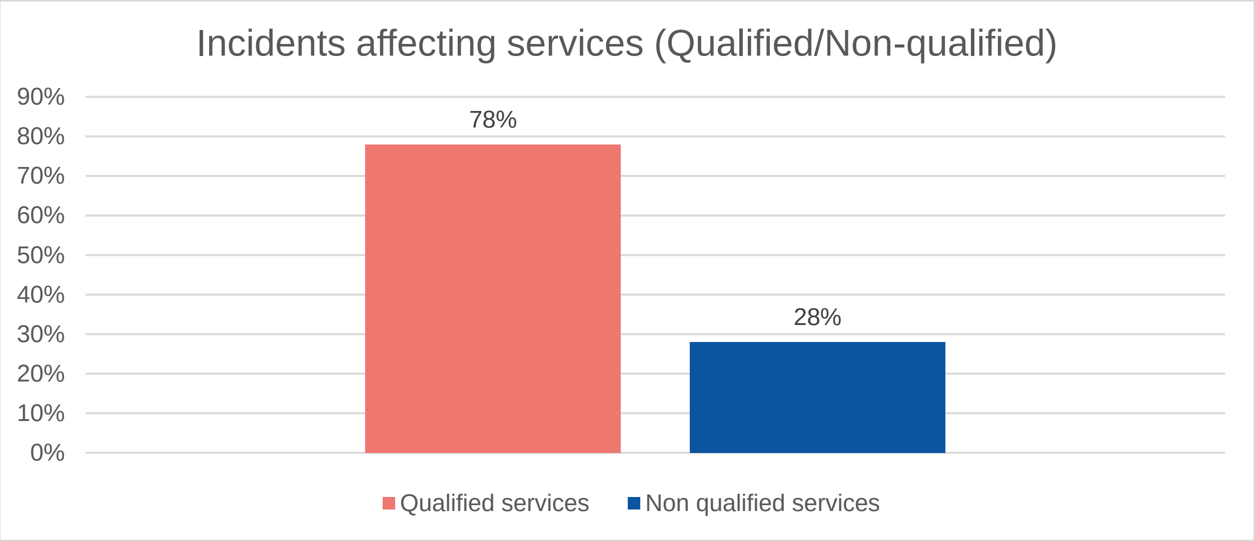
3.3.1 Trust services affected in detail

Most of the reported incidents affected the qualified signature certificate creation (44% of total incidents). This is consistent with last year. Website authentication certificate creation, seal certificate creation and timestamp creation were the second most affected services among the qualified ones. (22% of total incidents for each service). Approximately a fifth of the reported incidents (17% of total) affected the validation of e-signatures/e-seals.



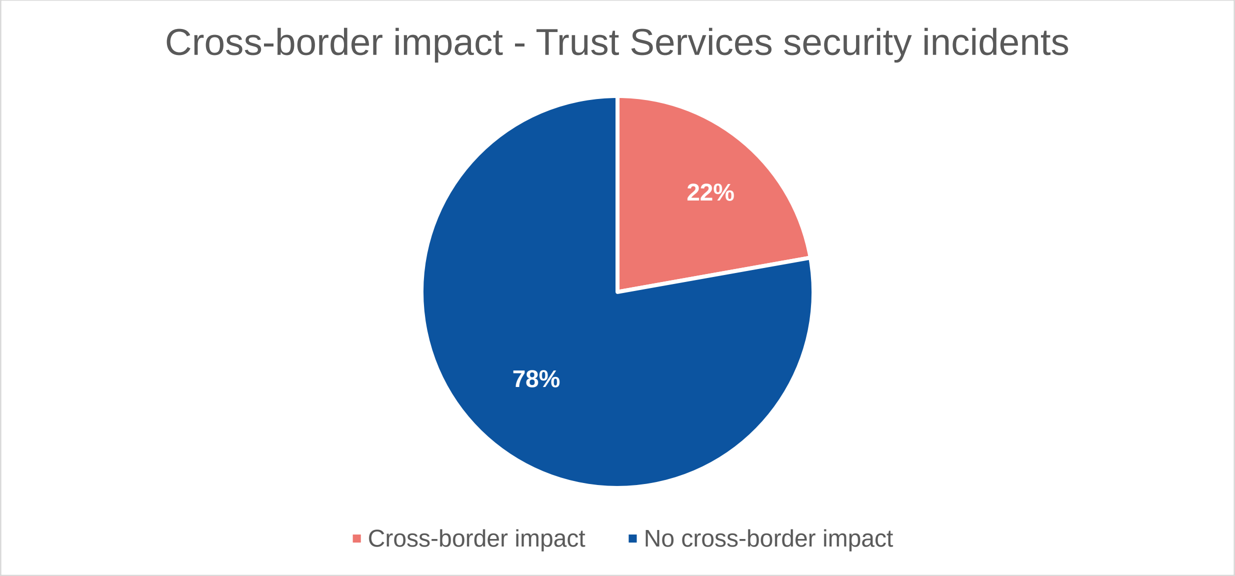
3.3.2 Qualified versus non-qualified

This year, approximately three quarters of the total incidents had an impact on qualified services (i.e. qualified signature certificate creation, qualified seal certificate creation, etc.). The corresponding percentage for non-qualified services is just over a quarter. Note that one incident report could involve multiple trust services, which explains why the percentages in the charts here add up to more than 100%.

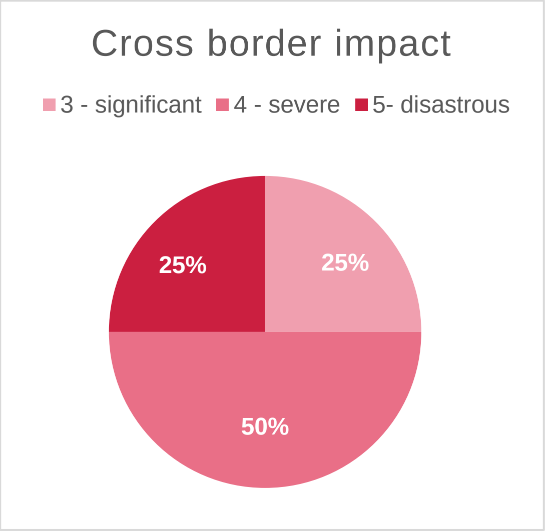


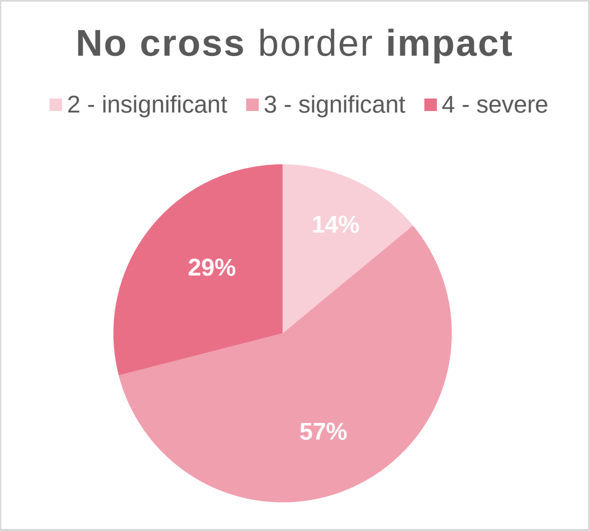
3.4 SECURITY INCIDENTS WITH CROSS BORDER IMPACT

Approximately one quarter of the security incidents (4 incidents, 22%) had an impact across borders, in the other EU Member States. In most cases of cross border impact, supervisory bodies informed other MS by initiating the cross-border incident notification procedure.



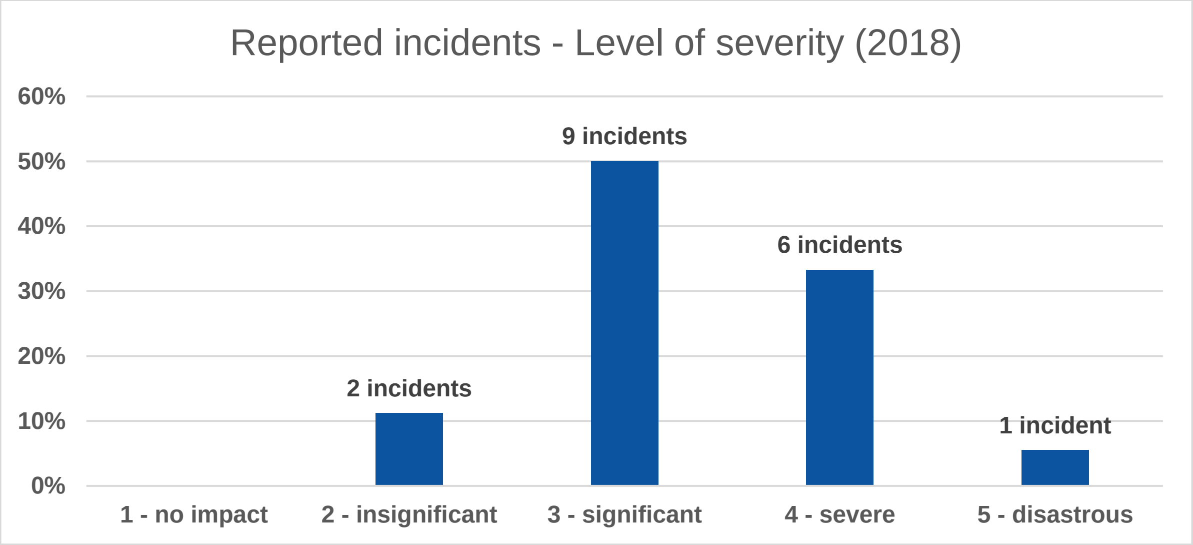
Half of the incidents with cross-border impact were rated as severe (level 4) and a quarter of them were reported as disastrous (level 5) indicating the importance of cross-border collaboration and information sharing. Incidents without cross-border impact were less critical as only 30% of them were submitted as severe while most of them (57%) were classified as level 3 (significant impact) in terms of severity.





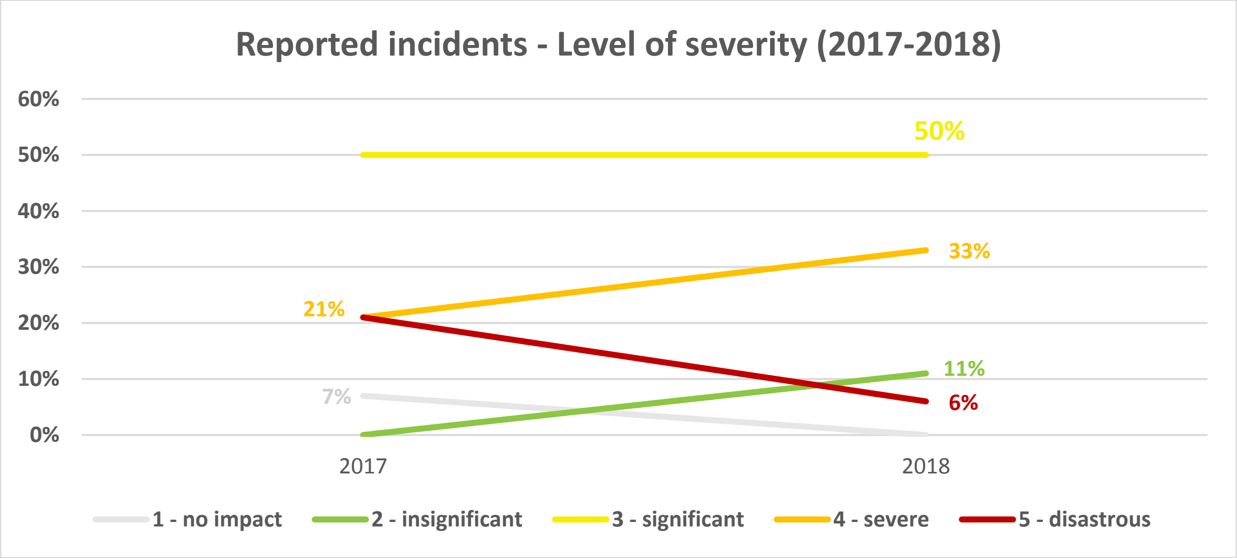
3.5 LEVEL OF SEVERITY

In 2018 half of the reported incidents had severity level 3 (significant impact), while a third of the incidents were severe. Only one incident was reported as disastrous.



3.6 SEVERITY 2017 AND 2018

We compare the statistics for severity with the previous round of reporting, covering 2017. The number of incidents with a significant impact is stable at 50%. There were less disastrous incidents, but more severe incidents.



4. CONCLUSIONS

Two years after the adoption of the eIDAS regulation, the electronic trust services market is growing, as is the number of applications and processes relying on electronic identities. eIDAS is becoming an enabler for the single digital market. Web certificates (for HTTPS, i.e. SSL/TLS) are now the norm, thanks to innovative projects, like ‘Let’s encrypt’, and the joint work of the web browser manufacturers. The collaboration between the supervisory bodies across the EU is delivering results. ENISA looks forward to continuing to support the supervisory bodies across the EU as well as the Commission, with the security aspects of implementing eIDAS.

ENISA looks forward to continuing to support the supervisory bodies across the EU as well as the Commission, with the security aspects of implementing eIDAS

We make some general observations below:

- **Cross eIDAS collaboration and information sharing:** Under eIDAS there is a cooperation network of authorities for national electronic identity systems, and there is a group of national supervisory bodies for the electronic trust services market. But from a security perspective these areas are closely related. Security issues with an electronic identity system, often have an impact on trust services, for example, many certificate authorities use electronic identities for authentication. Similarly, security issues with electronic trust services, often have an impact on eID systems, for example, many eID systems are built with trust services. Collaboration and information sharing related to incidents, threats, good practices, etc. is important.
- **Situational awareness:** We believe situational awareness about vulnerabilities and threats will help the supervisory bodies to do a more effective supervision. ENISA will continue to facilitate information sharing between the relevant authorities and supervisory bodies.
- **Connecting the security supervision of NISD, eIDAS, and European Electronic Communication Code (EECC):** The start of 2019 saw a very successful campaign of cyberattacks. The attack, referred to as DNSpionage, used weaknesses in TLD to poison DNS, to obtain fake web certificates, and subsequently man-in-the-middle traffic between employees and the targeted organizations. Media reports suggest the attackers have been highly successful in capturing large amounts of information from these organizations. This attack touches different areas, under different EU laws. This attack shows why it is so important to establish a close connection with regular information exchange and updates between eIDAS, the EECC and the Digital infrastructures part of the NIS Directive.
- **Security supervision of non-qualified web certificates:** A crucial part of the trust services market are the web certificates, used for HTTPS and other TLS encrypted channels. However, it is not easy to supervise this area. Providers of these certificates are not obliged to register with a national supervisory body and many organizations use providers outside the EU. The ex-post (light-touch) supervision regime for digital service providers, under the NIS Directive, could be an option.

The Commission will be reviewing the eIDAS regulation in 2020. We look forward to supporting this eIDAS review and contributing with advice.

TP-AK-19-001-EN-N

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. Since 2019, it draws up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

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

enisa.europa.eu

ISBN 978-92-9204-299-8
doi: 10.2824/540225