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

Annual Report Trust Services Security Incidents 2017

OCTOBER 2018

www.enisa.europa.eu European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups 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 contacting the authors please use resilience@enisa.europa.eu.
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

For the completion of this report ENISA has worked closely with a group of experts from Supervisory Bodies from across Europe. Listing the organizations (in no particular order): ILNAS (LU), CERT LV(LV), Bundesnetzagentur (DE), MCA (MT), NKOM (NO), ANSSI (FR), Austrian Regulatory Authority for Broadcasting and Telecommunications RTR (AT), Ministry of Digital Affairs (PL), GNS (PT), Agency for Digitisation (DK), Radiocommunications Agency (NL), FPS Economy (BE), EETT (GR), RRT (LT), FICORA (FI), Communications Regulation Commission CRC (BG), Agenzia per l'Italia Digitale (IT), National Media and Infocommucations Authority (HU), ICO (UK), Ministry of Communications and Informational Society (RO), National Security Authority NSA (SK), Ministry of Energy, Tourism and Digital Agenda (ES), Swedish Post and Telecom Authority PTS (SE), Ministry of Economy, Entrepreneurship and Crafts (HR), Ministry of the Interior (CZ), Estonian Information System Authority RIA (EE), DCCAE (IE), Ministry of Transport, Communications and Works (CY), Ministry of Public Administration, Information Society Directorate (SI), National Authority for Electronic Certification and Cyber Security (AL), MINGO (HR), Office for Communications AK (LI), European Commission (as observer)

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, 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 526/2013. 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

ISBN: 978-92-9204-258-5, DOI: 10.2824/835041

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[1], 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 the eIDAS regulation sets security requirements for trust service providers. National supervisory bodies have to supervise the trust service providers in their country to ensure that they fulfil these requirements. Cooperation and agreement on how to do this in practice is important not only to create a level playing field for providers operating out of different EU countries, but also to protect transactions based on these services. If there is, for instance, a cyber-attack on a trust service provider in one Member State, then this could have an impact on organizations in other parts of the EU who rely on the provider's trust services.

An important part of Article 19 is the *mandatory security breach notification requirements*: Trust service providers must *notify* the national supervisory body about security breaches, if there is a significant impact on the trust service(s) they provide. Article 19 requires national supervisory bodies to *inform* each other and ENISA if there is cross-border impact. Annually, the national supervisory bodies send *annual summary reports* about the notified breaches to ENISA and the European Commission. This document, the Annual Report Trust Services Security Incidents 2017, marks the second round of security incident reporting for the EU's trust services sector

For 2017, the national supervisory bodies reported 13 security breaches with a significant impact on trust services. We can draw the following conclusions:

- **Notification increase:** The number of notified security breaches increased significantly, in comparison to the previous year. This is not a sign of decreasing security, but rather shows that the implementation of the breach reporting requirements is maturing. Trust service providers are more aware of their breach reporting obligations and are becoming more familiar with the procedure. This leads to more notifications to the supervisory bodies.
- **E-signatures and e-seals most affected:** Almost half of the notified breaches, 43%, involve certificates for electronic signatures and electronic seals.
- **Most common causes are system failures, third party failures:** System failures, third party failures are both responsible for 36% of the breaches. Human errors are more rare (21%). Only 7% of the breaches are caused by malicious actions.
- **Many security breaches had cross-border impact:** Almost half of the notified breaches, 46%, had an impact across borders. This shows that indeed the EU trust services sector is cross-border. Many providers (and their suppliers) are offering services across the EU. Half those were severe, i.e. 50% the cross-border incidents had the highest severity rating (5- disastrous).
- **A third of the breaches were due to ROCA:** A number of notified breaches had the same underlying cause (the ROCA case).

The general conclusion is that, particularly for security supervision of trust services, cross-border collaboration and information exchange between EU Member States are very important and are starting to produce concrete results

[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

that are of value to the community. The eIDAS regulation, and Article 19 in particular, provides the legal basis for collaboration and information exchange between the supervisory bodies. Detailed discussions about security issues and supervision of the sector take place inside 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.

1. Introduction

According to Article 19 of the eIDAS Regulation, 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 reported security incidents.

This annual report marks the second round of security incident reporting in the EU's trust services sector, covering the security incidents of 2017.

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.

2. Background

In this section, we explain in more detail the background and policy context of this annual report.

2.1 The eIDAS regulation and Article 19

The eIDAS regulation was adopted in July 2014 and came into force in 2016. It is a legal framework that ensures interoperability of electronic trust services across the EU, creating a single market for such services. One of the goals of eIDAS is to ensure that electronic transactions have the same legal standing as traditional paper based transactions, allowing organizations to move away from expensive and cumbersome paper-based processes.

eIDAS is important for the European digital market because it allows businesses and citizens to use online and digital services across the EU, without the need to obtain a new electronic identity or trust service product each time. The idea is that, for example, a digital signature from a Spanish citizen, created with an Austrian smartcard, can be validated and accepted by, say, a Greek company.

Article 19 of the eIDAS regulation, contains the security requirements for trust service providers and the security breach notification requirements. In a nutshell, Article 19 requires that trust service providers assess risks, take appropriate security measures, and notify security incidents to the supervisory body. Article 19 also puts information sharing obligations on supervisory authorities vis-a-vis other supervisory bodies in the EU. Cooperation and agreement between EU member states on how to implement Article 19 and how to do security supervision is very important not only to create a level playing field across the EU, but also to avoid fraud and cyber-attacks. The Diginotar case of 2011[2] offers a good example of how a single security incident at one European certificate authority had an impact across borders, even globally.

2.2 Legal text of eIDAS Article 19

We include the text of Article 19 verbatim for the sake of reference:

> ***Article 19: Security requirements applicable to trust service providers***
>
> *Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.*
>
> *2. Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of 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. Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.*

[2] https://www.enisa.europa.eu/media/news-items/operation-black-tulip

> *Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA.*
>
> *The notified supervisory body shall inform the public or require the trust service provider to do so, where it determines that disclosure of the breach of security or loss of integrity is in the public interest.*
>
> *3. The supervisory body shall provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers."*

We also quote a part of Article 17 (6) of the eIDAS regulation, which asks supervisory bodies to provide the Commission with a summary of the notified breaches:

> *By 31 March each year, each supervisory body shall submit to the Commission a report on its previous calendar year's main activities together with a summary of breach notifications received from trust service providers in accordance with Article 19(2).*

Finally we report preamble 39 of the eIDAS regulation which explains that one of the reasons for annual summary reporting to ENISA and the Commission is to assess the effectiveness of the breach reporting mechanism itself:

> *To enable the Commission and the Member States to assess the effectiveness of the breach notification mechanism introduced by this Regulation, supervisory bodies should be requested to provide summary information to the Commission and to European Union Agency for Network and Information Security (ENISA).*

2.3 Incident reporting flows in Article 19

Article 19 requires trust service providers to assess risks, take appropriate security measures to mitigate and notify the supervisory bodies of security breaches with a significant impact on the trust services. It requires the supervisory body to inform other Member States and ENISA when a breach concerns other Member States. Moreover, each year supervisory bodies have to provide ENISA and the European Commission with a summary of breach notifications of received from their trust service providers. The diagram below shows the full picture and the different reporting flows. We explain the arrows step-by-step:

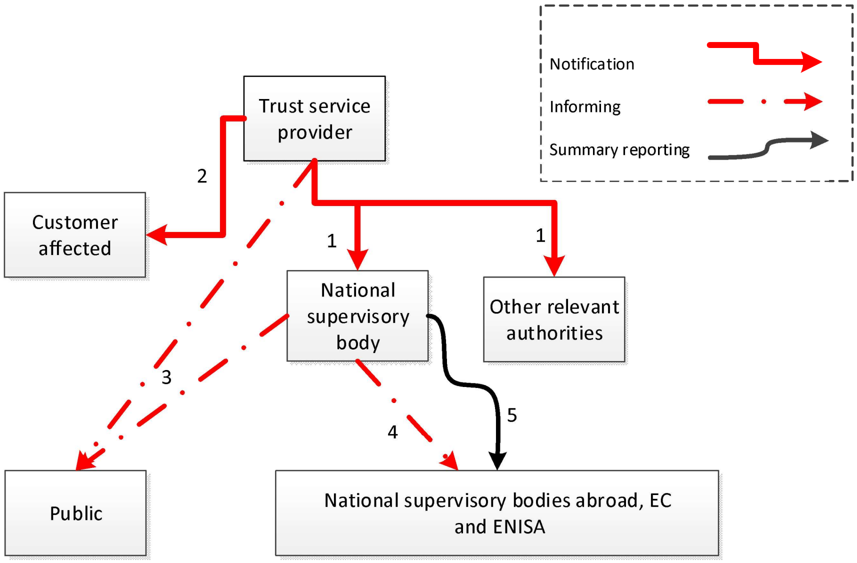

Notification
Informing
Summary reporting
Trust service provider
Customer affected
National supervisory body
Other relevant authorities
Public
National supervisory bodies abroad, EC and ENISA
1
1
2
3
4
5

Figure 1: Overview of reporting flows in Article 19

1. At step 1 (see arrow 1 in the diagram) the trust service provider notifies the national supervisory body of a security breach with a significant impact on the trust service provided or on the personal data maintained therein. This must happen without *undue delay*, and within 24 hours after the trust service provider became aware of the security breach. The provider needs to notify also to other relevant authorities, such as e.g. the national data protection authority (DPA), the national competent authority for information security, etc., where applicable.
2. The trust service provider also notifies the natural or legal person to whom the trust service was provided, i.e. the customer affected by the security incident, without undue delay (arrow 2).
3. If disclosure of the breach is in the public interest then the supervisory body may decide to Inform the public or require the trust service provider to do so (arrow 3).
4. The national supervisory body informs relevant supervisory bodies abroad and ENISA, when a security incident involves two or more Member States (arrow 4).
5. Annually the national supervisory body sends a summary reporting to ENISA and the Commission (arrow 5).

2.4 Security incident reporting

In 2014, after eIDAS was adopted, and under the auspices of the European Commission, ENISA formed an expert group with experts from competent authorities and national supervisory bodies to agree on the technical and practical details of implementing Article 19. In 2015 this group reached agreement about a non-binding technical document describing an incident reporting framework implementing Article 19 in practice[3]. The group also agreed to use the reporting tool (called CIRAS-T) developed by ENISA to facilitate the annual summary reporting. Below we briefly explain the key parts and terminology of the overall incident reporting framework.

2.4.1 Services in scope of reporting

In scope of reporting are qualified and non-qualified trust-service providers offering the following services:

- creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services
- creation, verification and validation of certificates for website authentication
- preservation of electronic signatures, seals or certificates related to those services, as defined in Article 3 of the eIDAS regulation, as an electronic service normally for remuneration

2.4.2 Security incidents

eIDAS and Article 19 mentions *security incidents*, *breaches of security*, *loss of integrity, breach notifications*. In the rest of this document, in line with the terminology used in the above-mentioned incident reporting framework, we abbreviate and use the term security incident to encompass both breaches of security and loss of integrity:

Security incident: A breach of security or loss of integrity with an impact on the security of the trust service provided.

For instance, the flooding of a server room due to heavy rains, causing downtime of an online validation service offered by the trust service provider, would be a security incident.

2.4.3 Reportable security incidents

Security incidents, which have to be notified to the supervisory body are those incidents, which had a *significant* impact on the trust service provided or on the personal data maintained therein. Each country takes a different

[3] The "Incident reporting framework for eIDAS Article 19" is available at https://www.enisa.europa.eu/publications/article19-incident-reporting-framework

national approach to this, based on national circumstances, depending on national circumstances, the sector, the size of the population, etc.

2.4.4 Annual summary reporting threshold

While national reporting thresholds are different in each country, the Article 19 expert group agreed on a threshold for annual summary reporting, to ensure consistency in the annual summary reporting across the EU. The agreed threshold is based on the severity scale, which is introduced in the incident reporting framework. This severity scale has 5 levels:

1. No impact
2. Insignificant impact: provider assets were affected but no impact on core services
3. Significant impact: part of the customers/services is affected
4. Severe impact: large part of the customers/services is affected
5. Disastrous: the entire organisation, all services, all certificates are affected

The members of the Article 19 expert group agreed that security incidents rated at level 3 or higher should be included in the annual summary reporting to ENISA and the Commission.

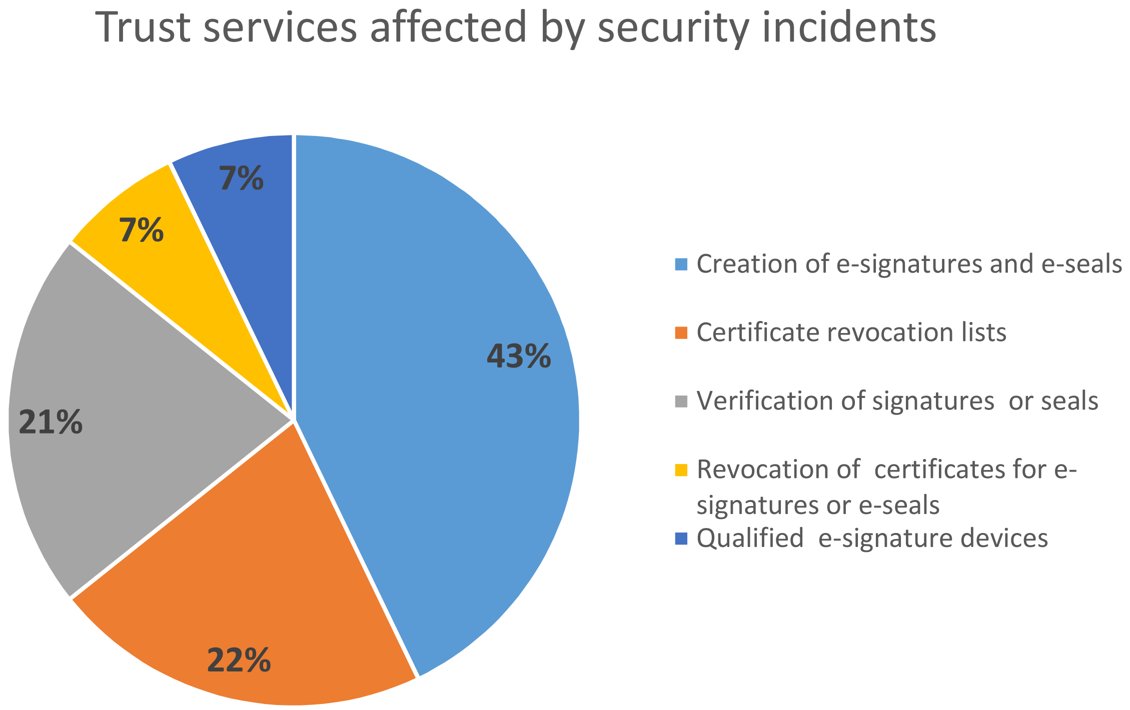
3. Analysis of reported security incidents

For the annual summary reporting for 2017, 13 security incidents with significant impact were reported to ENISA and the Commission[4].

This is only the second round of annual summary reporting, because eIDAS came into force just recently, on the 1st of July 2016. For comparison, in the first year of annual summary reporting, covering (half of 2016), only one incident was reported.

3.1 Trust services affected

Most incidents (43%) affected the creation of certificates for electronic signatures and electronic seals. The second category of services affected were the online certificates revocation services (CRL and OSCP) with 22%, and the online verification services with 21%.

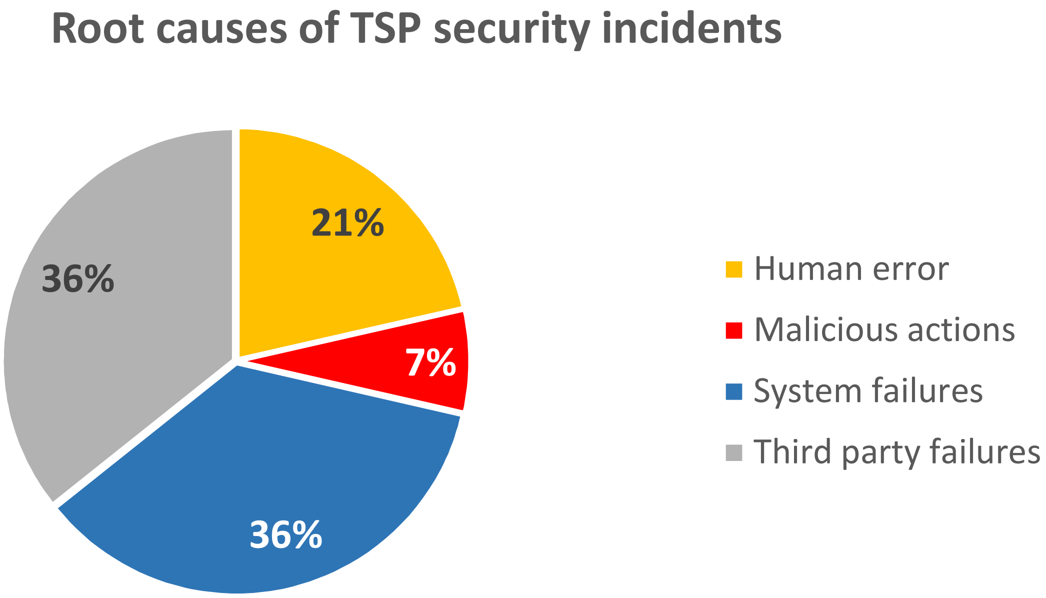


[4] Note that one additional security incident was reported, but excluded from the analysis, because it had no impact.

3.2 Root causes of security incidents

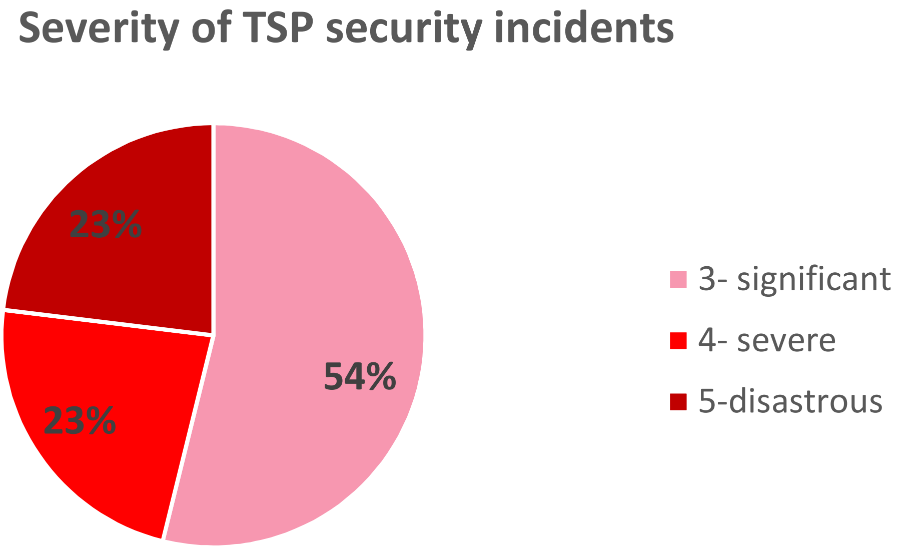
The most common root causes of security incidents were system failures (36%) and third party failures (36%). Malicious actions were rarely the cause of incidents (just 7% of the incidents).

This graph is evidence of a larger trend in the root causes of the security incidents as system failures is the main one in the telecom sector[5] as well.



3.3 Severity of security incidents

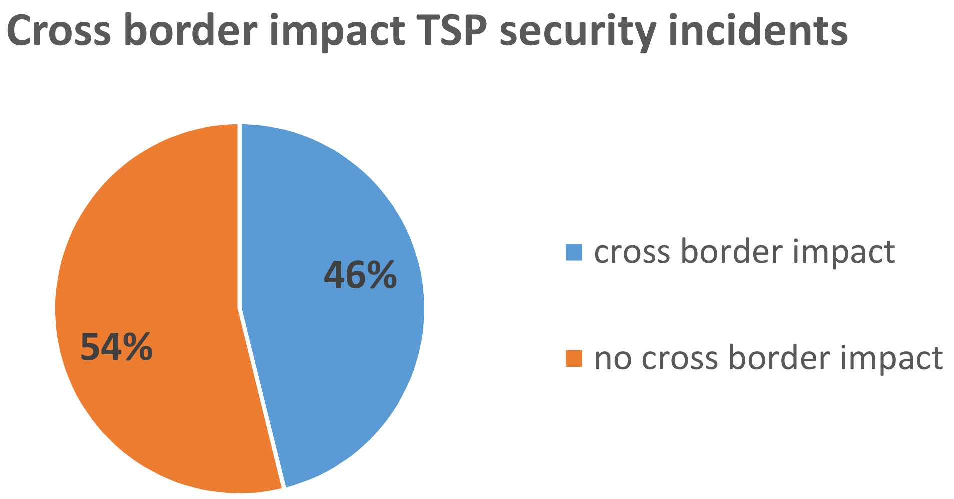
Approximately half of the reported security incidents (46%) were either severe or disastrous.



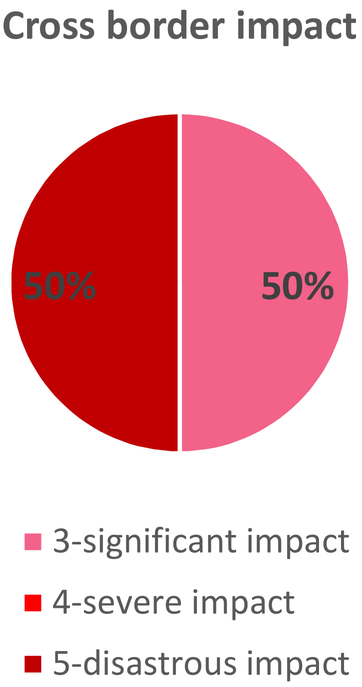
[5] ENISA Annual Report Telecom Security Incidents 2017
https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2017

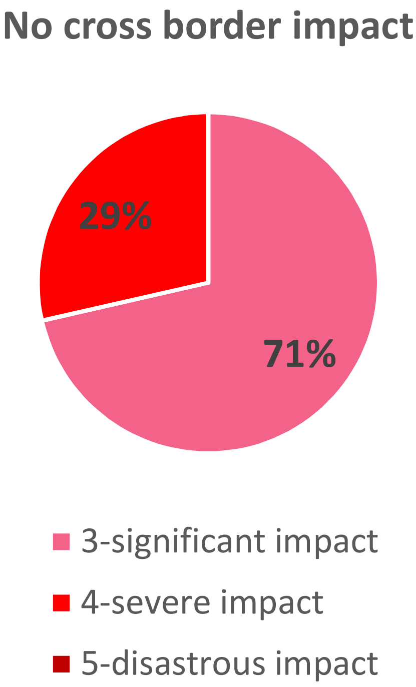
3.4 Security incidents with cross border impact

Almost half of the security incidents (46%) had impact across borders, in other EU Member States. This is not surprising if one considers the nature of the trust services and the single market. Supervisory Bodies (SBs) informed other Member States (MS) by initiating the cross-border incident notification procedure.



Half of the incidents with cross-border impact were rated as disastrous (level 5). This highlights the importance of cross-border collaboration and information sharing. Incidents without cross-border impact were, generally speaking, less severe.





4. Examples of reported security incidents

In this section, we give some specific (anonymized) examples of reported security incidents. We also indicate the severity level that was indicated by the national supervisory body as part of the annual summary reporting to ENISA and the European Commission.

- ***Malware compromised email addresses (severity level 3- significant):*** *The computer of an employee of a trust service provider was infected by malware, via an email attachment. The malware used a word document containing a macro. The attacker downloaded a list of account email addresses and tried to retrieve authentication information from the provider's customers via spear-phishing. The provider reacted by resetting the passwords of all employees, improved the authentication process for employees and launched an awareness and education campaign for its employees.*

- ***Unavailability of Revocation Services (severity level 3- significant):*** *A trust service provider's revocation services were unreachable for 3 hours. This was caused due to a human error in the configuration of domain name records. The trust service provider informed the public. Afterwards the provider acknowledged the need to improve the process for detecting and resolving IT issues. The provider also analyzed the redundancy of the links for the operation of the revocation services.*

- ***Certificate serial number errors (severity level 3- significant):*** *A trust provider inserted incorrect certificate serial numbers in the certificates, due to a software bug. The bug was not detected due to insufficient testing. Hundreds of certificates had to be revoked as a result. The provider informed all affected customers. Afterwards the provider fixed the software bug and improved the testing processes.*

- ***Services offline (severity level 3- significant):*** *A trust service provider experienced multiple problems with installing a new internet connection. As a result, its customer service and all internet-facing services offered by the trust service provider were unavailable for hours. The provider notified the customers of the problem via email. As an immediate action the trust service provider rolled back to its previous internet connection.*

- ***Unavailability of time stamping service (severity level 4- severe):*** *A trust provider experienced a hardware failure in one of the components underpinning it's time stamping server. This blocked the creation of timestamps. The provider disconnected the faulty system and informed its customers about the service unavailability. After the hardware fault was resolved and the service was restored, the provider investigated the case by analyzing event logs. The trust service provider also analyzed a number of failure scenarios for unforeseen circumstances like these and improved their failover procedures.*

The ROCA case

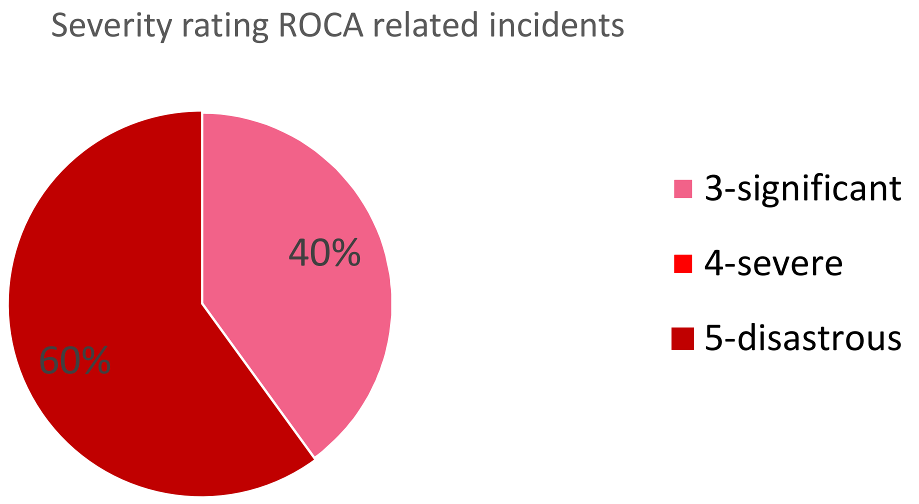
We discuss the ROCA vulnerability[6] in more detail, because it was a case with implications across Europe, widely discussed in press and media, and because the ROCA vulnerability was the underlying cause for a number of security breach notifications from trust service providers. From the total of 13 incidents included in the annual reports, 5 security incidents were related to ROCA.

[6] ROCA (Return of Coppersmith Attack) is a vulnerability discovered by academic researchers in a cryptographic library, used in a wide range of cryptographic chips and was publicly disclosed in October 2017. The issue was that the library generated RSA key pairs in such a way that an attacker could *compute* the corresponding private key from the corresponding public key. In many settings and implementations of RSA the public key is published or widely known, but the private key is supposed to remain a secret. More info see https://crocs.fi.muni.cz/public/papers/rsa_ccs17

It is good to highlight here that ROCA was a vulnerability that triggered the revocation of cryptographic keys and certificates by trust service providers, but there are (to our knowledge) no successful attacks or exploitations of this vulnerability (yet), besides proof of concept attacks.

The impact of ROCA was different across the EU, depending on the usage scenario and the number of customers involved. This means that ROCA was mitigated by trust service providers in different ways. In some cases trust providers had to revoke a small number of certificates, while in other cases, large numbers of customers were affected, requiring even coordination by national authorities to manage the situation. Overall, across the EU, trust service providers, revoked, approximately, 18 million vulnerable certificates.

Some ROCA related incidents were not even notified to the supervisory body because the impact was insignificant. The severity of the ROCA-related incidents in the annual summary reporting varied: 60% was rated at severity level 5-disastrous, 40% at severity level 3-significant (see the chart below).



We give some examples of incidents caused by ROCA and their impact severity:

- ***Small number of revocations (severity 3- significant):*** *In one country a trust service provider had to revoke a small number of impacted certificates.*

- ***Update of eID cards (severity 5- disastrous):*** *In one country the ROCA vulnerability was found to be present in hundreds of thousands of national e-ID smartcards, issued over the last 3 years. As a mitigation the national authorities decided to close the public key database in order to protect against a potential future attack. All affected electronic identity cards were suspended. The affected citizens had to update their electronic identity documents remotely or at specific service points.*

- ***Electronic signatures affected (severity 5- disastrous):*** *In one country only the qualified electronic signature part of the national eID cards was affected by ROCA. The national authority decided to revoke hundreds of thousands of certificates and issued new certificates with a longer (RSA 3072 bit) key pair. Additionally ROCA triggered a transition from RSA to ECDSA, and the usage of Extended Access Control (EAC) to secure remote issuance of qualified certificates.*

5. Conclusions

This document, the Annual Report Trust Services Security Incidents 2017, aggregates and analyses the annual summary reports from EU Member States about security breaches notified by trust service providers. We can draw the following conclusions:

- The number of notified security breaches increased significantly, in comparison to the previous year. This should not be interpreted as a sign of decreasing security. Also in the first years of security incident reporting in the telecom sector there was a gradual increase of the number of reported incidents, because it takes some time for service providers to become familiar with the breach reporting obligations and the procedure.
- Almost half of the notified breaches, 43%, involve certificates for electronic signatures and electronic seals.
- System failures, third party failures and human errors are the main root causes. Only 7% of the breaches are caused by malicious actions.
- Almost half of the notified breaches, 46%, had an impact across borders. This shows that indeed the EU trust services sector is to a large extent cross-border with suppliers and providers offering services across the EU.
- Half of the incidents were rated as having a severe (level 4) or disastrous impact (level 5). Half of the cross-border incidents were rated has having a disastrous impact (level 5).
- A number of notified breaches had the same underlying cause, i.e. the ROCA case.

The general conclusions we can draw from this is that cross-border collaboration and information exchange are very important when it comes to supervision and ensuring the security of trust services in the EU. eIDAS provides the legal basis for collaboration and information exchange mechanisms between supervisory bodies. The sooner organizations learn about threats and incidents, the sooner they can decide the best course for mitigation. Good information exchange about threats and incidents makes mitigation easier.

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

TP-06-18-131-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-258-5
DOI: 10.2824/835041