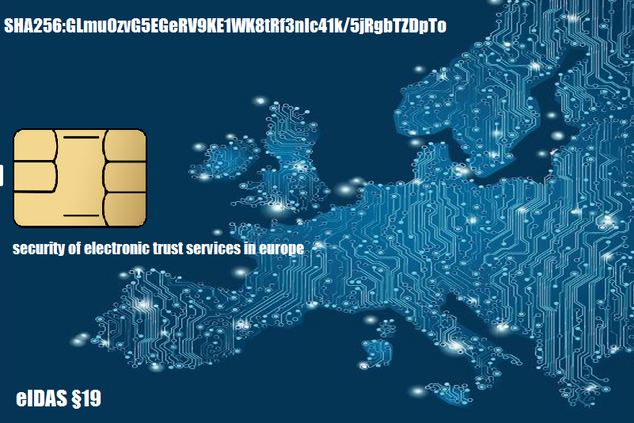
Annual report Trust Services Security Incidents 2018

ENISA releases its annual report on trust services security incidents.

Published on July 15, 2019



Tagged with

* [Incident Reporting](https://www.enisa.europa.eu/search?Subject%3Alist=Incident%20Reporting)
* [Trust service providers](https://www.enisa.europa.eu/search?Subject%3Alist=Trust%20service%20providers)

[The document](https://www.enisa.europa.eu/publications/trust-services-security-incidents-2018) gives an aggregated overview of security breaches with significant impact reported in 2018 by EU national supervisory bodies. It shows root causes, statistics and trends, and marks the third round of security incident reporting for the EU’s trust services sector.

According to the eIDAS regulation, trust service providers must notify these security breaches to their national supervisory body. The annual summary reporting for 2018 totalled 18 incident reports. A total of 28 EU countries and one 1 EFTA country take part in annual summary reporting.

**Key statistics relating to the 2018 incidents**

*Malicious actions and system failures are the dominant root causes of reported incidents*: System failures amount for 39% of the total incidents (consistent with 36% in 2017). Malicious actions have gone up to 39% (compared to 7% in 2017).

*A few, but critical security breaches with cross border impact:* Some 25% of the reported incidents had a cross-border impact. Although the ratio is small, the seriousness of the incidents was high: 75% of them were classified as level 4 – severe and 5 – disastrous.

*Qualified e-signatures certificates creation – the most affected service:* Roughly 50% of the incidents reported affected the qualified creation of qualified certificates for e-signatures.

**The EU Agency for Cybersecurity ENISA**

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.

**Outlook**

The cooperation network of authorities for national electronic identity systems and the group of national supervisory bodies for the electronic trust services market will benefit from the close collaboration on security supervision and information sharing about incidents, threats, good practices, etc.

Basic situational awareness about vulnerabilities and large-scale 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.

A close connection with regular exchange and updates about past incidents, threats, good practices, etc. between eIDAS, the European Electronic Communication Code (EECC) and the Digital infrastructures part of the NIS Directive is important, because these are closely related areas. ENISA will facilitate this and act as a bridge.

**For the full report:**[**Trust Services Security Incidents 2018 - Annual report**](https://www.enisa.europa.eu/publications/trust-services-security-incidents-2018)