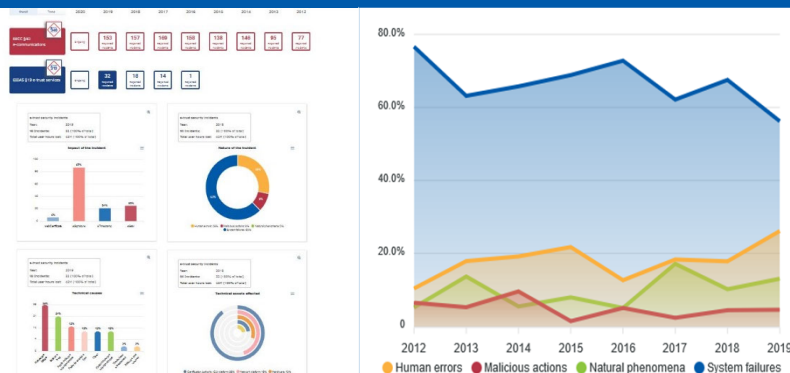




EUROPEAN UNION AGENCY  
FOR CYBERSECURITY



# INCIDENT REPORTING IN TRUST SERVICES AND EID

Dr. Apostolos Malatras, Knowledge & Information Team (KIT)

27 | 10 | 2022



# SCOPE – EIDAS ART. 19

## *Article 19*

### **Security requirements applicable to trust service providers**

1. 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.

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.

- **ENISA supports Art. 19 incident reporting since 2016**



# SCOPE – EIDAS ART. 10

## *Article 10*

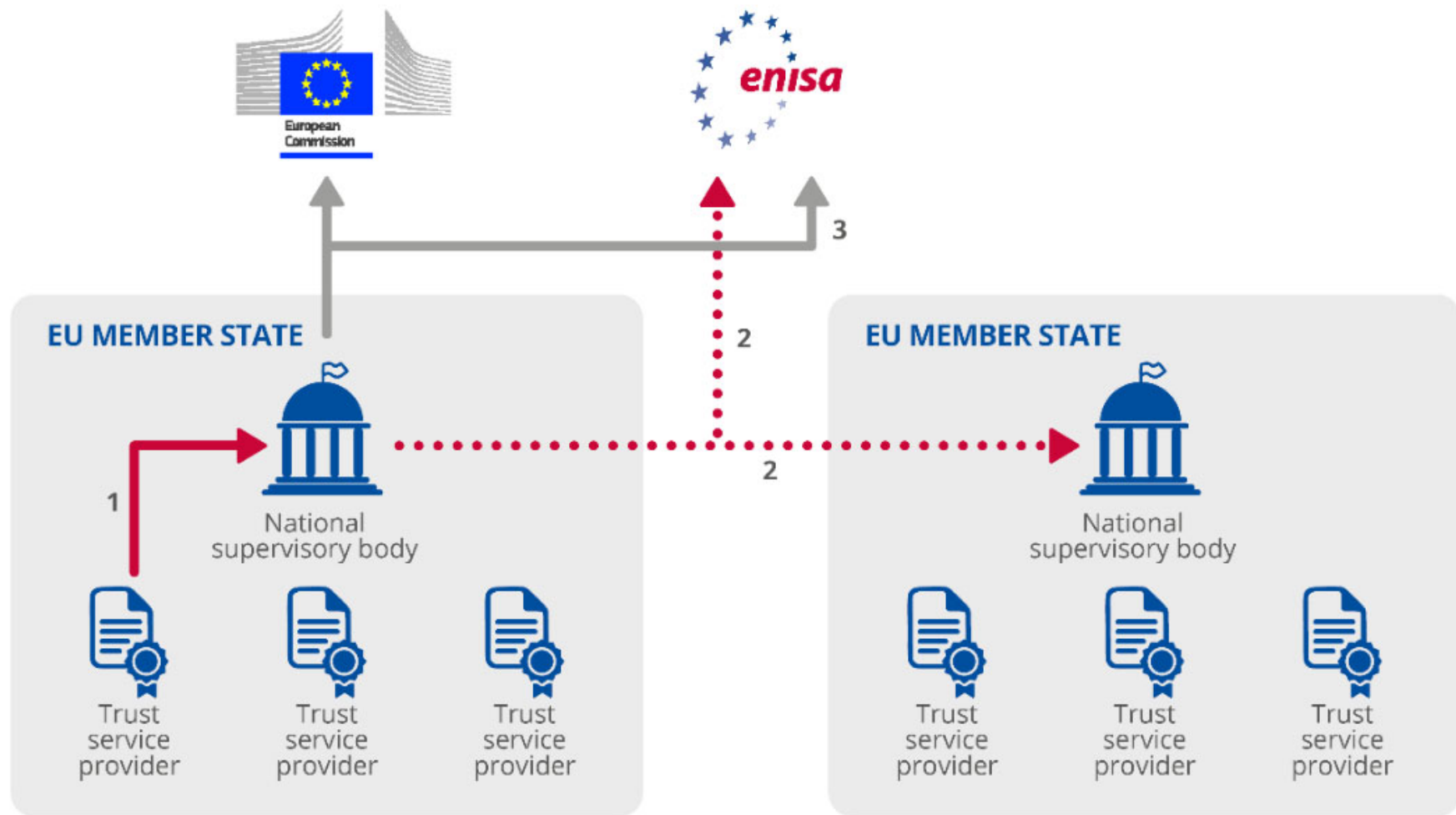
### **Security breach**



1. Where either the electronic identification scheme notified pursuant to Article 9(1) or the authentication referred to in point (f) of Article 7 is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission.
2. When the breach or compromise referred to in paragraph 1 is remedied, the notifying Member State shall re-establish the cross-border authentication and shall inform other Member States and the Commission without undue delay.
3. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension or revocation, the notifying Member State shall notify other Member States and the Commission of the withdrawal of the electronic identification scheme.


- **eID Cooperation Network has tasked ENISA to support incident reporting under Art. 10**
- **Process to begin as of 2023**



# INCIDENT REPORTING PROCESS



Security breach notification  Cross-border information  Annual summary reporting 





# TYPES OF INCIDENTS



## **A SERVICE OUTAGE**

(e.g. continuity, availability)



## **B OTHER IMPACT ON SERVICE**

(e.g. confidentiality, authenticity, integrity)



## **C IMPACT ON OTHER SYSTEMS**

(e.g. ransomware in an office network, no impact on the service)



## **D THREAT OR VULNERABILITY**

(e.g. discovery of crypto flaw)



## **E IMPACT ON REDUNDANCY**

(e.g. failover or backup system)

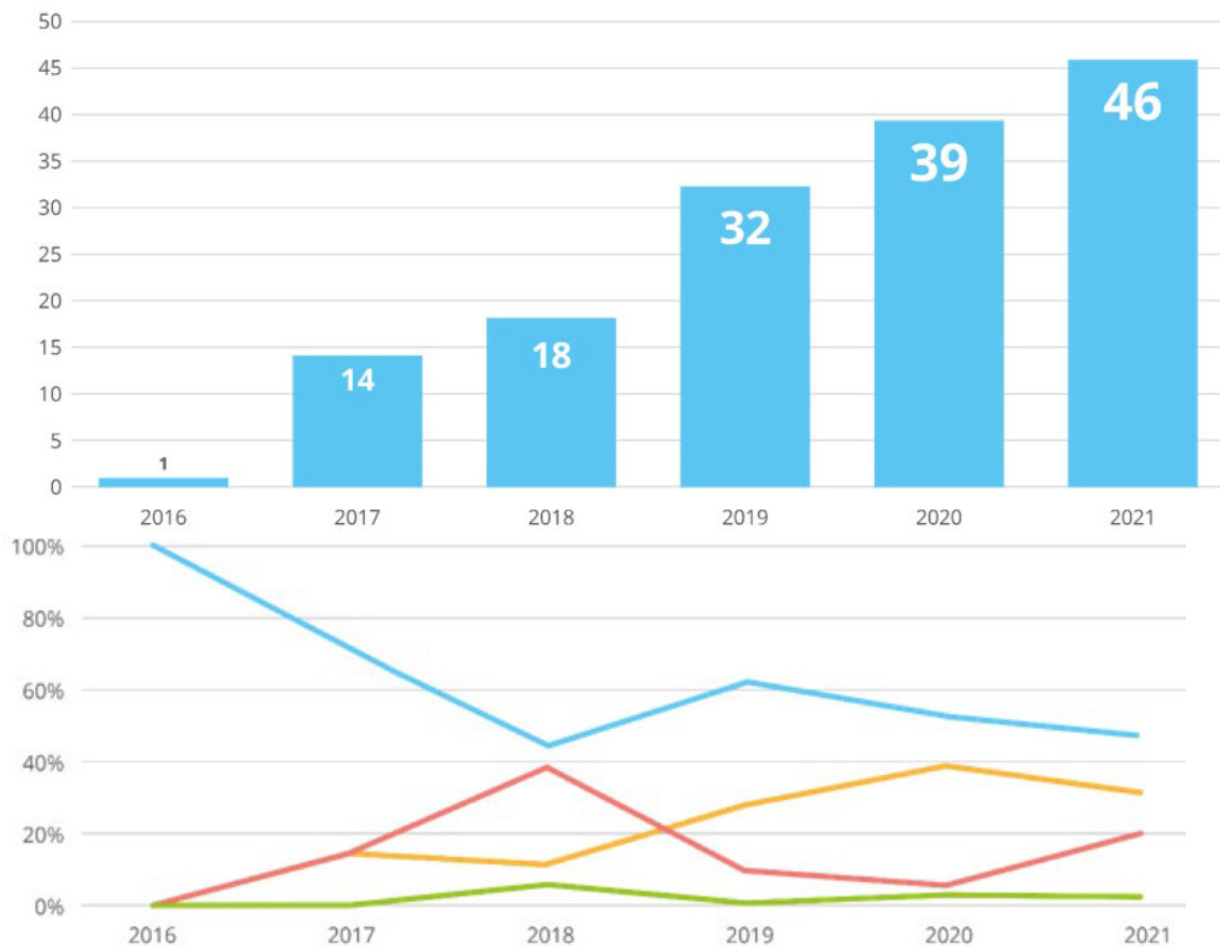


## **F NEAR-MISS INCIDENT**

(e.g. activation of security measures)

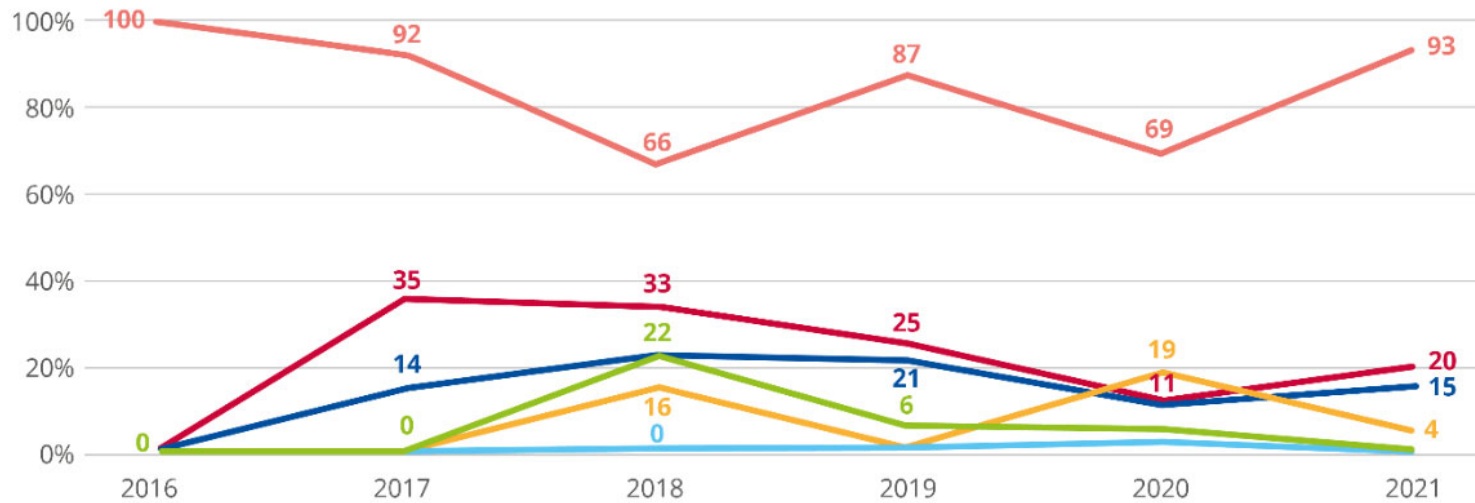
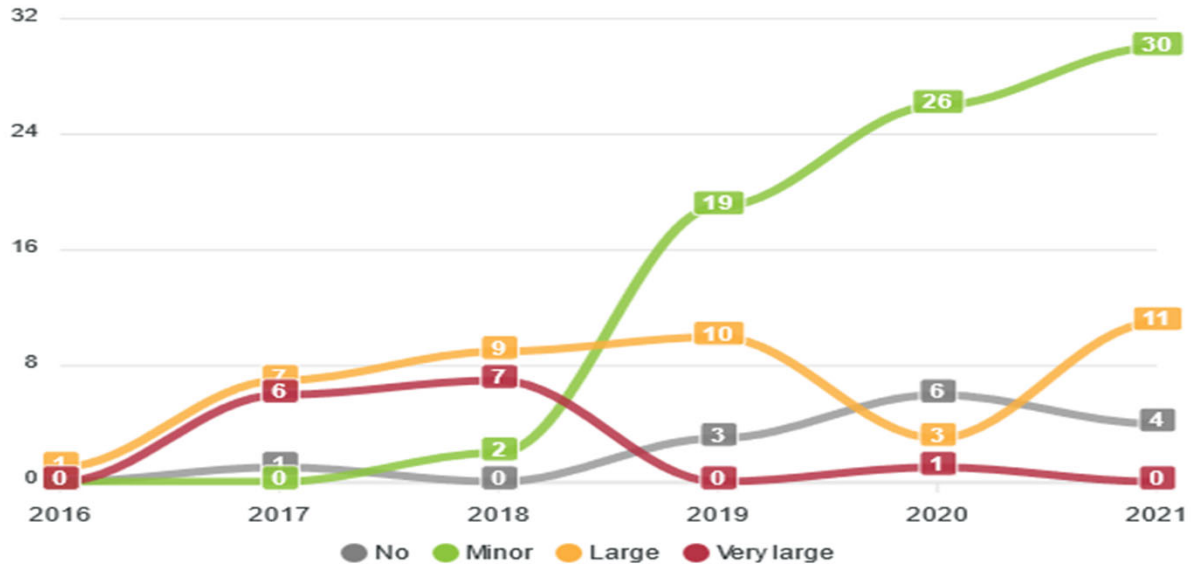


# ART. 19 OVER THE YEARS



# ART. 19 OVER THE YEARS

Severity of impact per year





# ANNUAL INCIDENT REPORT – ART. 19

- **More detailed root cause analysis**
- **Multi-annual impact on services and severity of impact**
- **Report already validated by Art. 19 Group**
- **Art. 10 will join in from 2023**

- **General findings**

- Increase in notified incidents by around 18%
- Incidents with a large impact has increased: quadruple increase.
- Ratio of qualified trust services over non-qualified remains high.
- First reporting of a threat/vulnerability.
- Root causes for malicious actions consistent with ETL 2021.







# CYBERSECURITY INCIDENT REPORTING AND ANALYSIS SYSTEM

EIDAS Article 19  
Trust services

0  
Reported  
Incidents

45  
Reported  
Incidents

36  
Reported  
Incidents

32  
Reported  
Incidents

18  
Reported  
Incidents

14  
Reported  
Incidents

1  
Reported  
Incidents

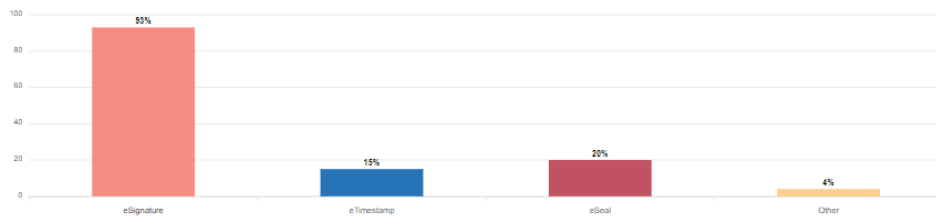
0  
Reported  
Incidents

0  
Reported  
Incidents

0  
Reported  
Incidents

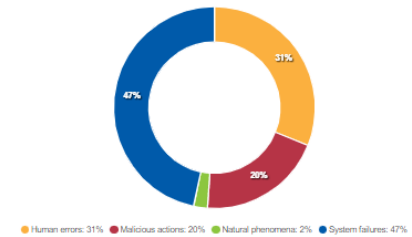
e-trust security incidents  
Year: 2021  
Nb Incidents: 45 (100% of total)  
Total user hours lost: 76M (100% of total)

Impact of the incident



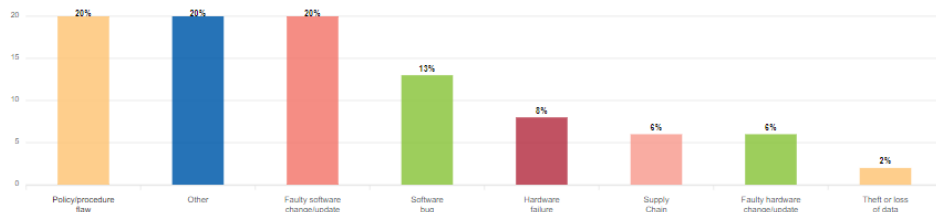
e-trust security incidents  
Year: 2021  
Nb Incidents: 45 (100% of total)  
Total user hours lost: 76M (100% of total)

Nature of the incident



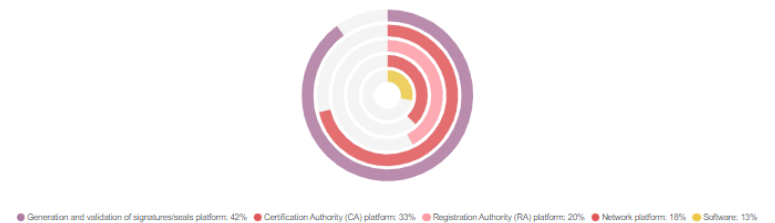
e-trust security incidents  
Year: 2021  
Nb Incidents: 45 (100% of total)  
Total user hours lost: 76M (100% of total)

Technical causes



e-trust security incidents  
Year: 2021  
Nb Incidents: 45 (100% of total)  
Total user hours lost: 76M (100% of total)

Technical assets affected





# CIRAS TOOL



EIDAS Article 19  
Trust services

**45**  
Reported incidents

**36**  
Reported incidents

**32**  
Reported incidents

**18**  
Reported incidents

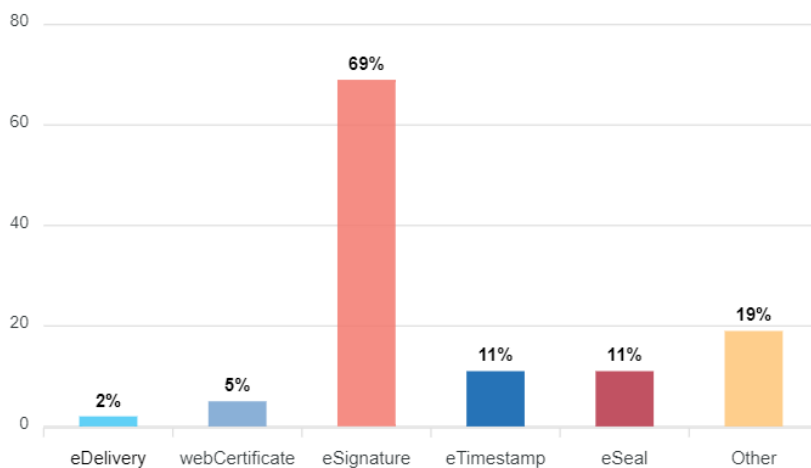
**14**  
Reported incidents

**1**  
Reported incidents

## e-trust security incidents

Year: 2020  
Nº Incidents: 36 (100% of total)  
Total user hours lost: 162M (100% of total)

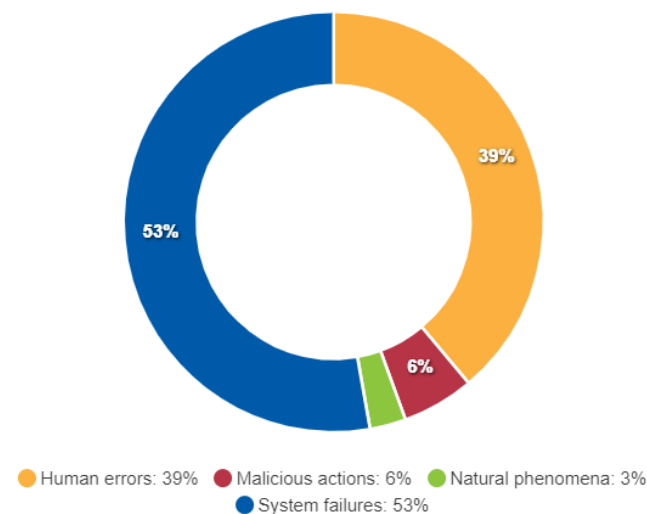
### Impact of the incident



## e-trust security incidents

Year: 2020  
Nº Incidents: 36 (100% of total)  
Total user hours lost: 162M (100% of total)

### Nature of the incident





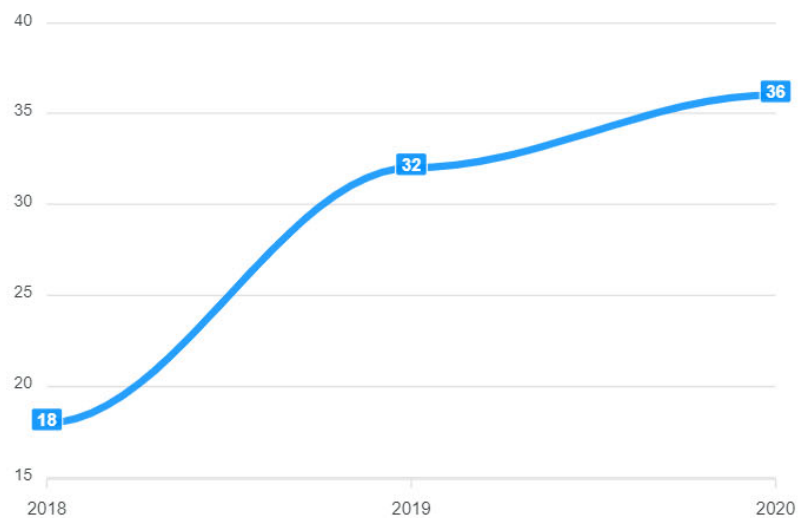
# CIRAS TOOL



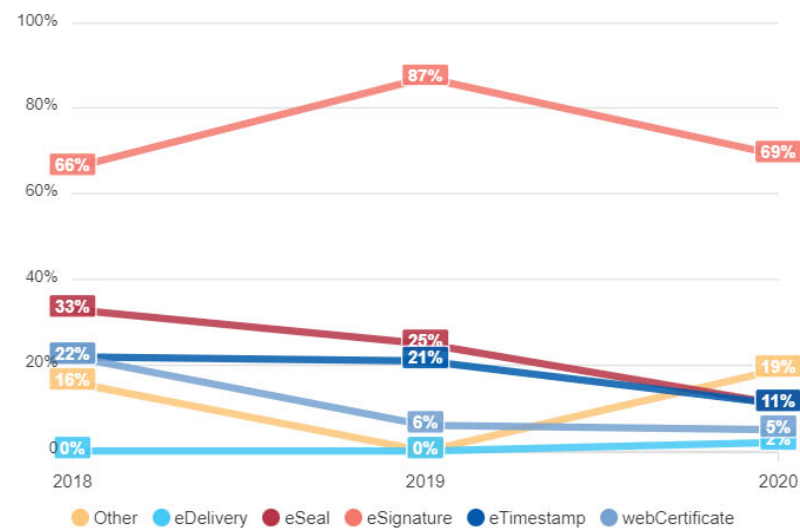
EIDAS Article 19  
Trust services



Number of incidents per year



Impact per service per year





# THE WAY FORWARD – NISD 2.0

CIRAS CONSOLIDATED REPORTING



In the EU, critical service providers have to notify cybersecurity incidents with a significant impact to the national authorities in their country. At the end of each year, the summary reports about these incidents are collected, analyzed, aggregated and analyzed by ENISA. The visualization tool shows the overall EU statistics. You can select subsets of incidents and drill down into root causes, services affected, etc. by clicking on the years, sectors, or parts of each chart. Clicking again clears the selection. Graphs and charts can be enlarged by clicking the top right corner. Feel free to use them in slide decks or documents.

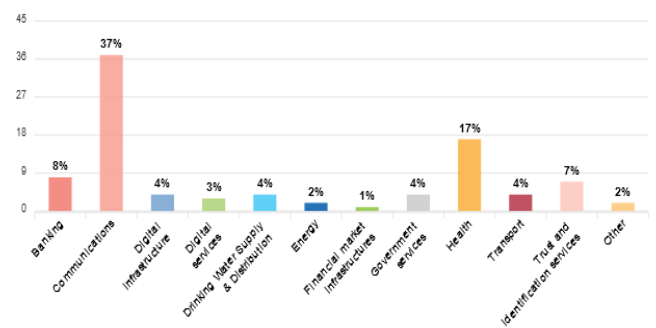
Overall Trend

- All
- Energy
- Transport
- Banking
- Health
- Drinking Water Supply & Distribution
- Digital infrastructure
- Communications
- Trust and identification services
- Digital services
- Government services
- Other
- Financial market infrastructures



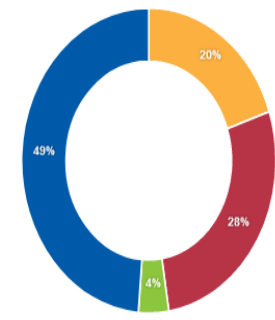
Year: 2020  
No Incidents: 495 (100% of total)

Impact per sector



Year: 2020  
No Incidents: 495 (100% of total)

Nature of the incident



Human errors: 20% Malicious actions: 28% Natural phenomena: 4% System failures: 49%



# THANK YOU FOR YOUR ATTENTION

**European Union Agency for Cybersecurity**  
Ethnikis Antistaseos 72 & Agamemnonos 14,  
Chalandri 15231, Attiki, Greece

 +30 28 14 40 9711

 [info@enisa.europa.eu](mailto:info@enisa.europa.eu)

 [www.enisa.europa.eu](http://www.enisa.europa.eu)

