

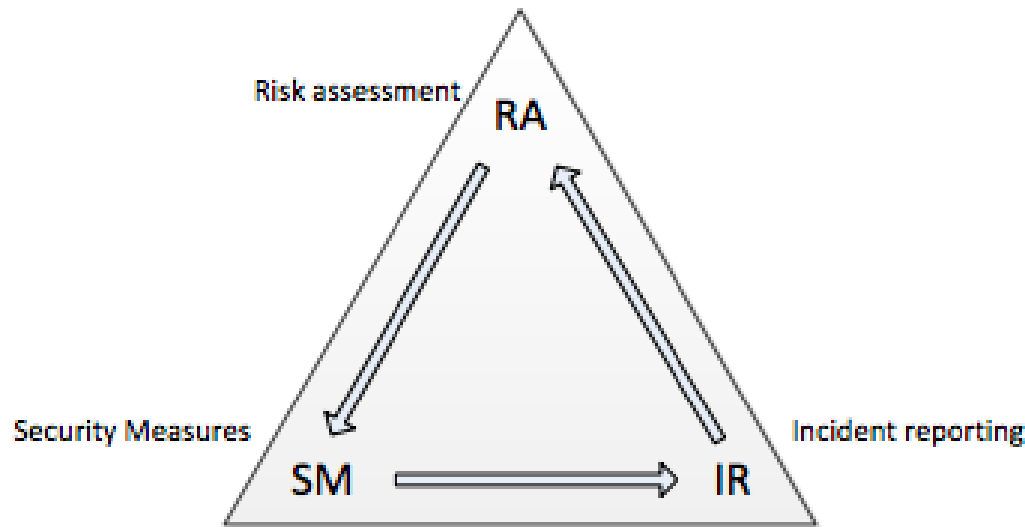
# 2017 ANNUAL TRUST SERVICES SECURITY INCIDENTS ANALYSIS

ENISA Article 19 Team

23 | 10 | 2018

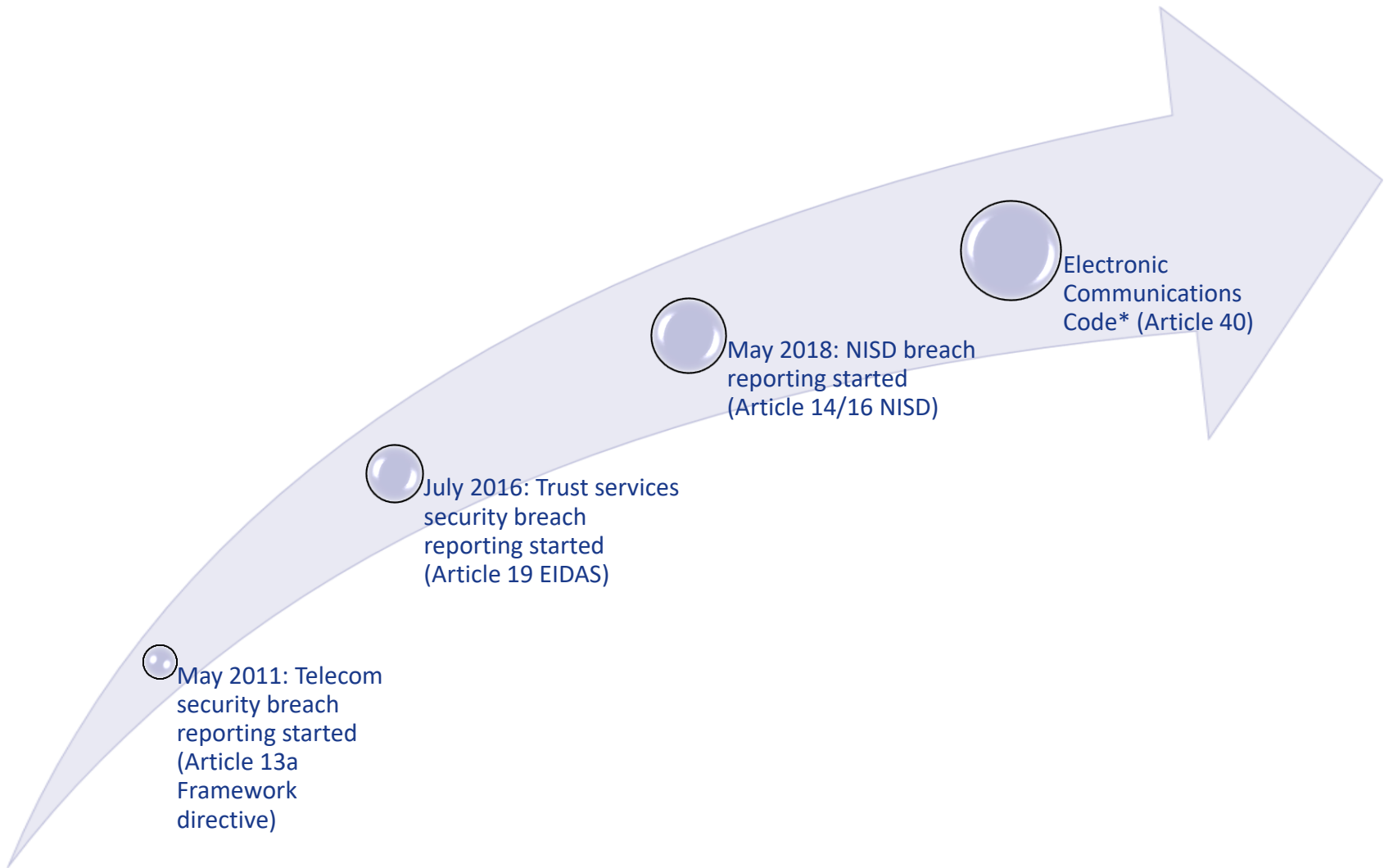


# GENERAL MODEL SECURITY SUPERVISION



**Market operators/providers assess security risks, take appropriate measures, and notify if things go wrong.**



**This triangle is supervised nationally by competent authorities and is present in Article 13a (telecom), Article 19 (EIDAS), Article 14 and 16 (NISD).**



\* under discussion/trialogue – brings telecom breach reporting in line with NIS directive

# WHY INCIDENT REPORTING

## Incident reporting is a tool for learning for TSPs and SBs

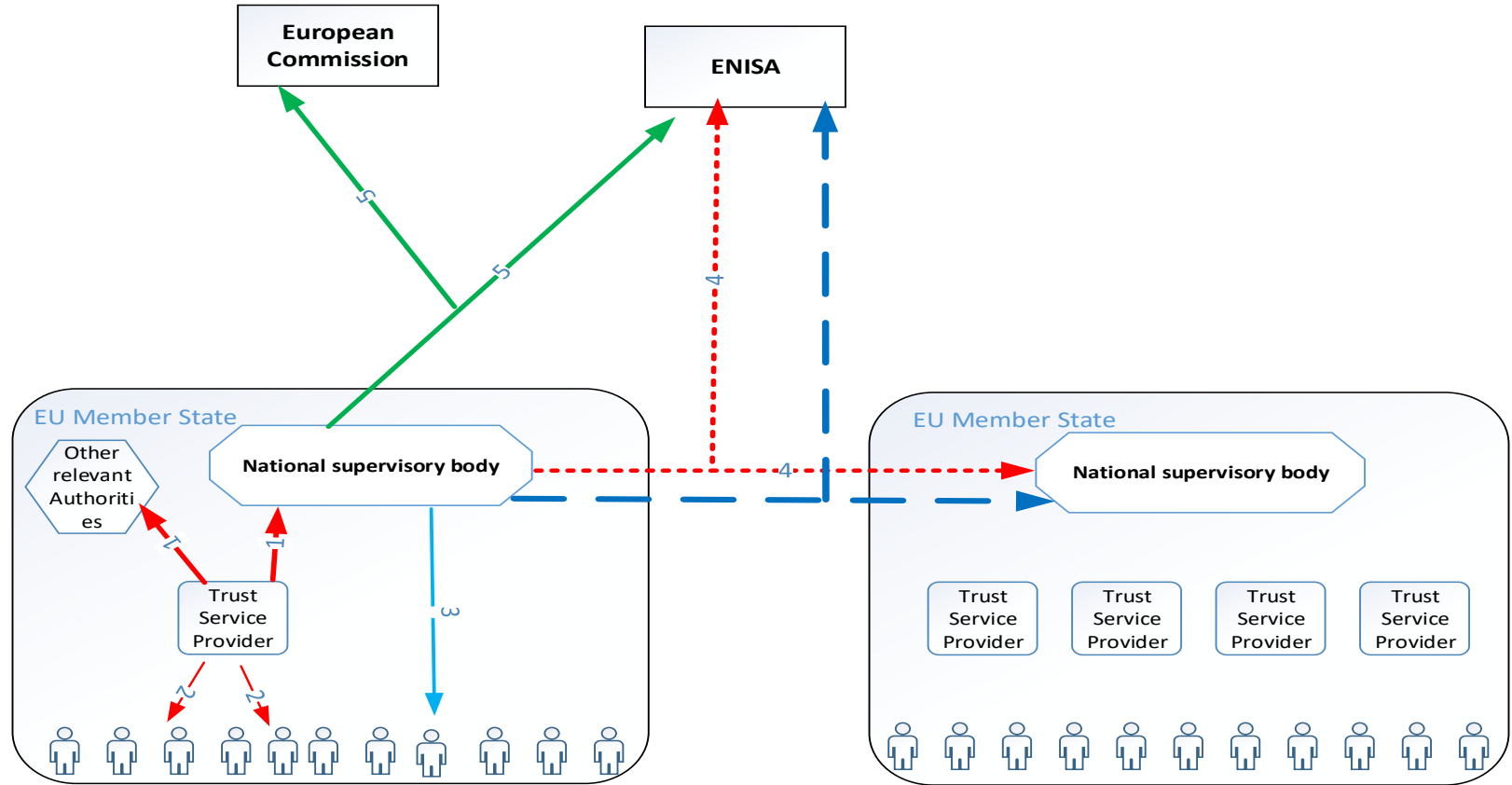
- Supervisory Bodies get correct information about security incidents, root causes, impact
  - actual numbers, statistics production 
- Incident-related data is the key to understand security risks and trends
  - basis to study on root causes and trends
- Input (root causes, trends) for appropriate policy decisions (e.g. guidelines)
- Bilateral collaboration in case of cross-border incidents 
- Input for the SBs to share experience
- Basis for post incident supervision








# eIDAS AND INCIDENT HANDLING

## eIDAS sets mandatory security breach notification requirements

- TSPs to notify the SBs (or any other relevant bodies) of any security breach that has a significant impact on the trust service provided.
- SBs to inform each other and ENISA if there is a security incident with cross-border impact.
- SBs, to send annual summary reports about the notified breaches to ENISA and the EC (Article 19).



-  Annual summary reporting - CIRAS-T tool
-  Cross-border information – CIRAS-T tool
-  Incident notification (authorities/ customers affected)
-  Informing the public
-  Voluntary information sharing – Art. 19 EG ENISA portal

### eIDAS incident reporting process





# eIDAS INCIDENT REPORTING FRAMEWORK

## **ENISA Guidelines “Incident reporting framework for eIDAS art. 19”**

cooperation with art. 19 Expert Group

## **Defining the thresholds was a really challenging task. Two approaches were used**

- Scenarios/examples of security incidents in the context of eIDAS article 19
- Assets assigned impact values according to the eIDAS services

Article 19 EG preference was the first one, however both are included in CIRAS-T



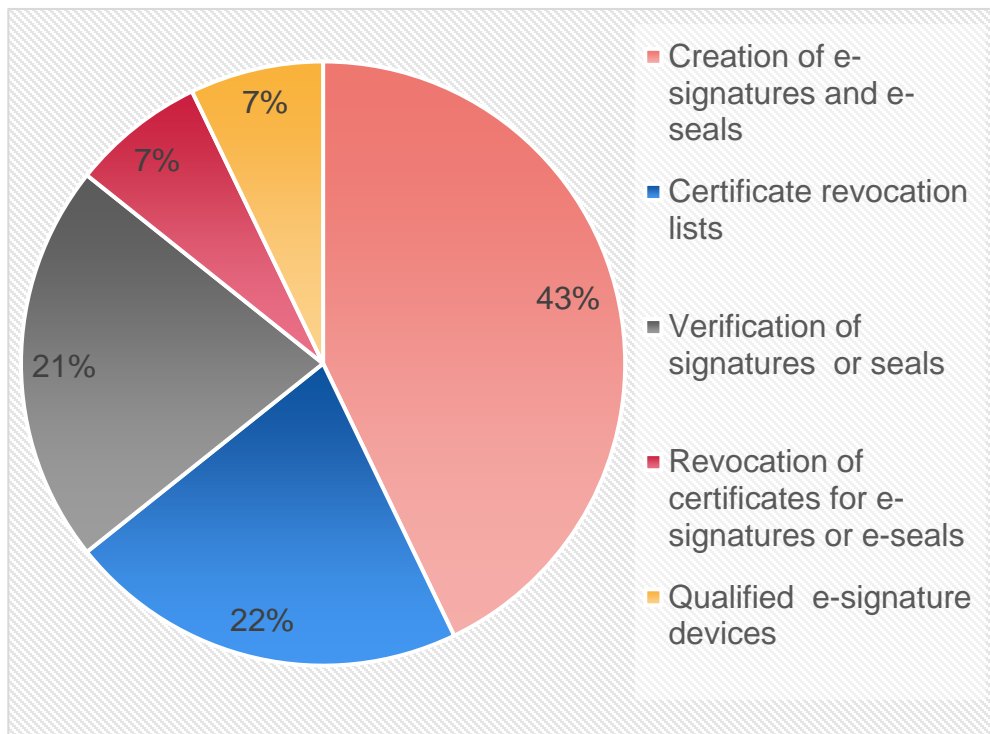
# ANNUAL INCIDENT REPORTING 2017

## 13 security breaches were reported with a significant impact on trust services

- Second round: first full year of security incident reporting for the EU's trust services sector
- ENISA annual report on trust service security incidents 2017
  - aggregated EU-wide overview of security incidents



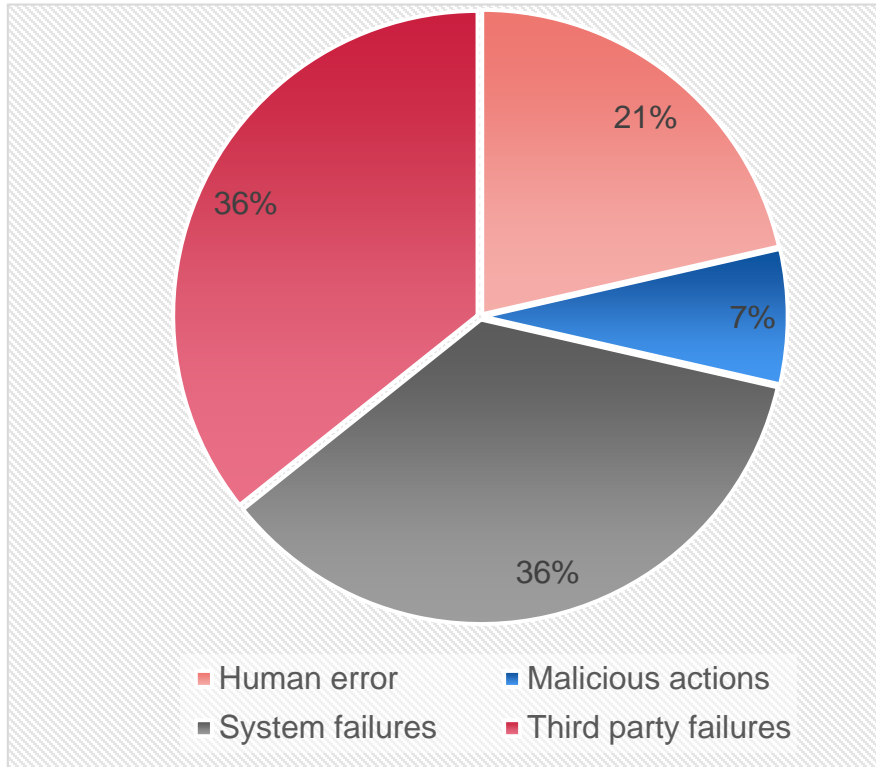
# 2017 ANNUAL INCIDENT REPORTING - 1



## Trust services affected by security incidents

Most incidents (43%) affected the creation of certificates for electronic signatures and electronic seals

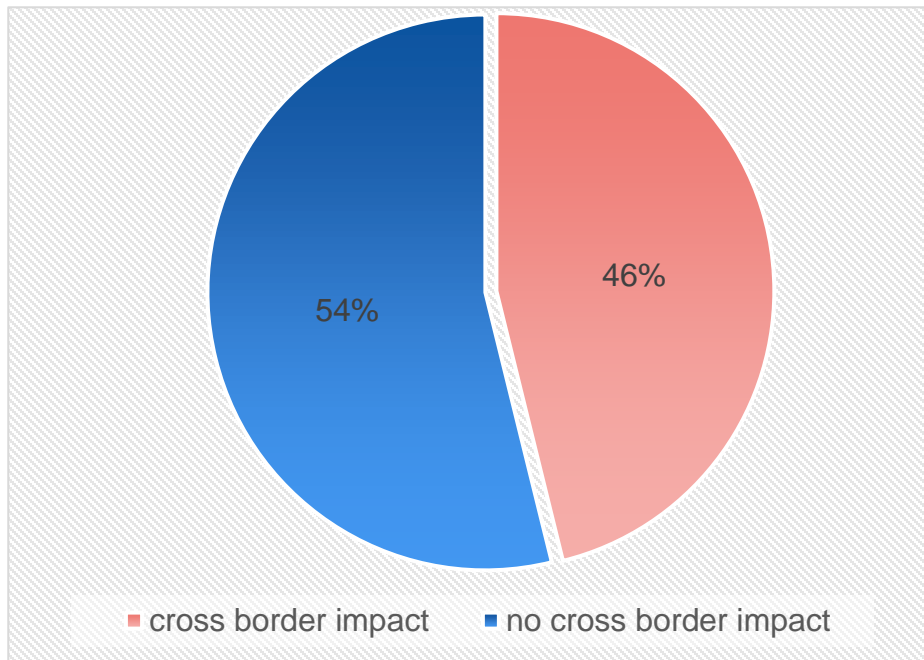
# 2017 ANNUAL INCIDENT REPORTING - 2



## Root causes of TSPs security incidents

Most common root causes of security incidents were system failures (36%) and third party failures (36%)

# 2017 ANNUAL INCIDENT REPORTING - 3



## Cross border impact of TSPs security incidents

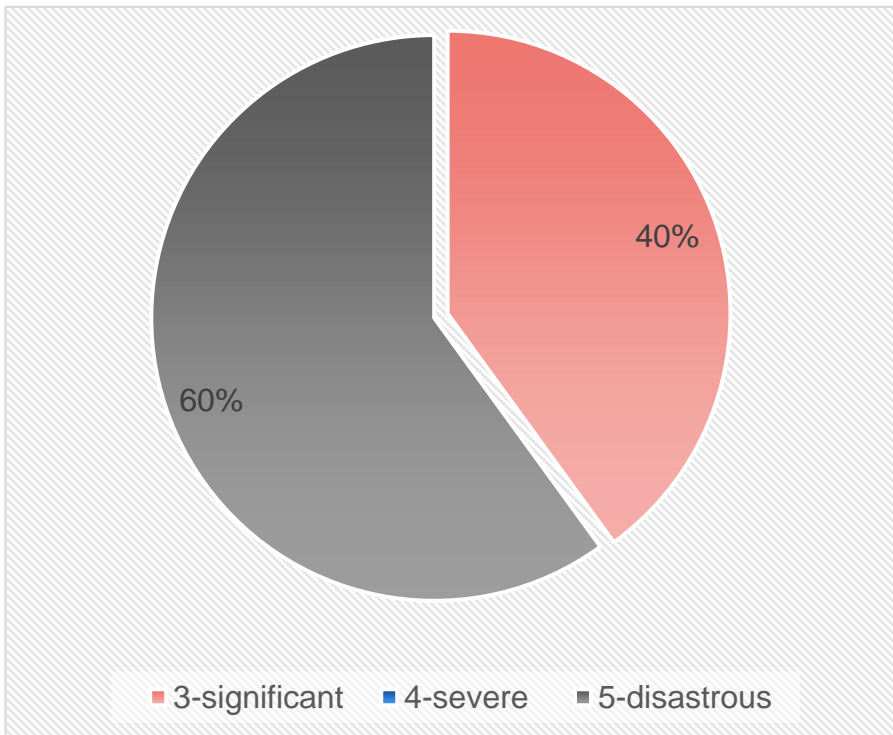
Almost half of the security incidents (46%) had impact across other EU Member States

# 2017 ANNUAL INCIDENT REPORTING - 4

## Severity rating ROCA related incidents

A number of notified breaches had the same underlying cause: ROCA case

- 60% was rated at severity level 5-disastrous, 40% at severity level 3-significant
- ROCA was mitigated by trust service providers in different ways





# CONCLUSIONS

**Incident reporting mechanism is operational**

**Implementation of the breach reporting requirements is maturing**

TSPs getting familiar with the procedure

**Early exchange of sufficient info about threats and incidents**

It makes mitigation easier

**Cross-border collaboration and information exchange**

Very important for supervision and security of trust services in the EU

# ENISA INCIDENT REPORTING PAPERS

## Annual Report Trust Services Security Incidents 2017

<https://www.enisa.europa.eu/publications/annual-report-trust-services-security-incidents-2017>



## Article 19 Incident reporting framework

<https://www.enisa.europa.eu/publications/article19-incident-reporting-framework>



# THANK YOU FOR YOUR ATTENTION

Vasilissis Sofias Str 1, Maroussi 151 24,  
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)

