Submission date

Jun 20, 2017

Recipients

Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom, Liechtenstein, Iceland, Norway, Croatia

Message for recipients

Incident report

ID 163484

2017
Severity 3 **Root cause**

- Third party failures

Created on Jun 20, 2017 **Modified on** Jun 20, 2017

General description of the incident
: The Austrian supervisory body has received a report on a weakness of the “asymmetric crypto library” which is used by several qualified electronic signature devices produced by Atos IT Solutions and Services GmbH, Munich, in particular • “CardOS V5.0 with Application for QES, V1.0” and • “CardOS V5.3 QES, V1.0”. The problem affects generating electronic signature creation data for use with the RSA algorithm. There is no evidence of weaknesses in generating electronic signature creation data for ECDSA or in creating electronic signatures by means of either RSA or ECDSA. Due to the mentioned weakness, a qualified trust service provider established in Austria revoked all qualified certificates issued prior to 9 June 2017 and informed both the public and the signatories affected.

Duration (in hours)
: —

Percentage of subscribers affected
: —

Severity of the incident
: 3

Year
: 2017

Personal data impacted
: Electronic signature creation data

Number of subscriptions
: 29

Cross border impact
: Yes

Services affected

- Creation of (qualified) certificates for electronic signatures
- Creation of (qualified) certificates for electronic seals service
- Creation of electronic timestamps service

Asset types affected

- Qualified electronic signature creation devices

Category of impact
: Confidentiality

Impact on assets
: High

Trust service concerned
: Qualified

Root cause category

- Third party failures

Detailed causes

- Algorithms for generating electronic signature creation data

Actions taken
: Revocation of qualified certificates

Lessons learned
: —

Mitigating security measures
: —

Other authorities notified, nationally
: —

Other authorities notified, abroad
: yes, SBs

Customers affected notified
: yes, by TSP

Public informed
: yes, by TSP

Information disclosure by supervisory body under freedom of information legislation
: —