Knowledge-building on Cryptography for eIDAS Supervisory Bodies

Today and yesterday, ENISA, the European Union Agency for Cybersecurity organised a two-day knowledge-building event on cryptography, specifically for the national supervisory bodies for electronic trust services and electronic signatures.

Published on November 27, 2019



Tagged with

* [Article19](https://www.enisa.europa.eu/search?Subject%3Alist=Article19)
* [Training](https://www.enisa.europa.eu/search?Subject%3Alist=Training)
* [Cryptography](https://www.enisa.europa.eu/search?Subject%3Alist=Cryptography)
* [eIDAS](https://www.enisa.europa.eu/search?Subject%3Alist=eIDAS)

In total 34 experts from 13 Member States attended the training, which is a part of the Agency’s support for the ENISA Article 19 Expert Group. The ENISA Article 19 group was set up by ENISA in 2015 to bring together experts from supervisory bodies who supervise Article 19 of the eIDAS, i.e. the security requirements for providers of electronic trust services in Europe.

**Day one – Cryptography foundations**

Day one of the knowledge building was dedicated to the foundations of cryptography and the cryptographic primitives. For this first day, ENISA had contracted the services of Professor Christian Rechberger, crypto researcher at TU Graz IAIK, and his colleague Daniel Kales. They went over cryptographic primitives and the foundations, and discussed new developments in the area of quantum-safe algorithms, as well as new cryptographic protocols such as homomorphic encryption and zero-knowledge proof-systems.

In the afternoon participants did some hands-on work and practical exercises to delve into multiparty computation, discussing threats and use-cases for the new cryptography.

**Day two – Applied cryptography**

Day two of the knowledge building was dedicated to the application of cryptography in practice. For this second day ADACOM put together a programme with different teachers and subject matter experts from the University of the Aegean, QMSCERT, Ascertia, Gemalto amongst others.

This second day covered themes including the IT infrastructure and architecture of a qualified Trust Service Provider (TSP), a roadmap for a TSP for complying with eIDAS, audits under eIDAS, from the perspective of the Conformity Assessment Body (CAB), and also more technical topics like remote Qualified Signature Creation Device solutions, remote ID Identification, secure remote on-boarding. In the afternoon participants did a hands-on exercise on two-factor biometric authentication architectures using smartphones and hardware security module One Time Passwords (OTPs).

**Further Information:**

* This work has been carried out under Output O.1.2.3 ‘Support incident reporting activities in the EU’ of the 2019 Annual work programme of ENISA.
* In 2015, ENISA founded the Article 19 Expert Group, to bring together experts from supervisory bodies, to discuss on the technical details of incident reporting and the supervision of the security requirements in Article 19. Article 19 of the eIDAS Regulation requires that trust service providers assess risks, take appropriate security measures, and notify significant security incidents and breaches of integrity to the national supervisory bodies. A representative from RTR Austria chairs the group, ENISA acts as its secretariat, and ENISA supports the group with logistics, collaboration tools, as well as breach reporting tooling and analysis.
* The ENISA[Article 19 Expert Group](https://resilience.enisa.europa.eu/article-19)