

eIDAS Amendment - new ecosystem

Challenges and Opportunities

Agenda

eIDAS Amendment

- 1.** what is new for Trust Services and Trust Service Provider?
- 2.** what are the opportunities?
- 3.** what are the challenges?

eIDAS Amendment – what is new for Trust Services and Trust Service Provider

New Trust Services

- **Management of remote electronic signature and seal creation devices (Art. 29.1a, 29a and 39a)**
 - precondition for remote signing or sealing services
 - allows remote management of subjects (users) keys
- **Issuance of electronic attestation of attributes (Art. 45b to h)**
 - will source the EU-Identity Wallet
- **Electronic archiving of electronic documents (Art. 45i, j)**
 - addresses archiving of electronic data, preserving data integrity and origin
(Note: a „Preservation Service“ does typically not archive the data, but signatures, seals,...!)
- **Recording of electronic data into electronic ledgers (Art. 45k, l)**
 - Creation and management of a sequence of electronic data records, ensuring the integrity of those records and the accuracy of the chronological ordering of those records

Main new/updated requirements for TSP/QTSP

- **Article 15 Accessibility for persons with disabilities and special needs**
 - Interface to Directive (EU) 2019/882
- **Article 16 Penalties**
- **Article 19a Requirements for non-qualified trust service providers**
 - Interface to Article 21 of Directive (EU) 2022/2555
- **Article 20 Requirements for non-qualified trust service providers**
 - Interface to Article 21 of Directive (EU) 2022/2555
- **Article 24 Requirements for qualified trust service provider**
 - Paragraph 1 – Identification methods with transition period until 21st of May 2026
- **Article 30 Certification of qualified electronic signature creation devices**
 - Certification validity and vulnerability testing of QSCD

eIDAS Amendment – what are the opportunities?

New Trust Services are the biggest opportunity for QTSP

- **Management of remote electronic signature and seal creation devices (Art. 29.1a, 29a and 39a)**
 - precondition for remote signing or sealing services
 - allows remote management of subjects (users) keys
- **Issuance of electronic attestation of attributes (Art. 45b to h)**
 - will source the EU-Identity Wallet
- **Electronic archiving of electronic documents (Art. 45i, j)**
 - addresses archiving of electronic data, preserving data integrity and origin
(Note: a „Preservation Service“ does typically not archive the data, but signatures, seals,...!)
- **Recording of electronic data into electronic ledgers (Art. 45k, l)**
 - Creation and management of a sequence of electronic data records, ensuring the integrity of those records and the accuracy of the chronological ordering of those records

Identification methods: opportunities for QTSP and ISP

- **Article 24 Requirements for qualified trust service provider**
 - Paragraph 1 – Identification methods (1a (c))
 - No specific recognition on national level required anymore
- **Opens further opportunities for TSP/QTSP to subcontract any eIDAS certified ISP in the EU**
- **Opens further opportunities for ISP to offer its service to any TSP/QTSP in the EU**

eIDAS Amendment – what are the challenges?

Directive (EU) 2022/2555 (NIS 2)

- Article 21 of Directive (EU) 2022/2555
 - Not problematic
- Implementing Regulation 2024/2690 with Annex
 - Article 14 Significant incidents with regard to trust service providers
 - Annex requirements in general
- Implementing Regulation 2024/2690 under Directive (EU) 2022/2555
 - Problematic as the EU Member States do not have implemented the Directive yet (19 member states as of 7th of May 2025)

3.2. Monitoring and logging

3.2.1. The relevant entities shall lay down procedures and use tools to monitor and log activities on their network and information systems to detect events that could be considered as incidents and respond accordingly to mitigate the impact.

3.2.2. To the extent feasible, monitoring shall be automated and carried out either continuously or in periodic intervals, subject to business capabilities. The relevant entities shall implement their monitoring activities in a way which minimises false positives and false negatives.

3.2.3. Based on the procedures referred to in point 3.2.1, the relevant entities shall maintain, document, and review logs. The relevant entities shall establish a list of assets to be subject to logging based on the results of the risk assessment carried out pursuant to point 2.1. Where appropriate, logs shall include:

(a) relevant outbound and inbound network traffic;

(b) creation, modification or deletion of users of the relevant entities' network and information systems and extension of the permissions;

(c) access to systems and applications;

(d) authentication-related events;

(e) all privileged access to systems and applications, and activities performed by administrative accounts;

(f) access or changes to critical configuration and backup files;

(g) event logs and logs from security tools, such as antivirus, intrusion detection systems or firewalls;

(h) use of system resources, as well as their performance;

(i) physical access to facilities;

(j) access to and use of their network equipment and devices;

(k) activation, stopping and pausing of the various logs;

(l) environmental events.

Mixing ETSI and Implementing Regulations

- Implementing regulation overriding the ETSI requirements
 - Lack of synchronization in some cases

Example IR 2025/1567 vs. IR 2025/1566

- IR 2025/1567

- 6.5.5 Network security controls

OVR-6.5.5-02: The vulnerability scan requested by REQ-7.8-13 of ETSI EN 319 401 [1] **shall** be performed at least once per quarter

- IR 2025/1566

- REQ-7.8-13 of ETSI EN 319 401 to be applied unchanged = **should** be performed once per quarter

Transition periods and missing Implementing Regulations

- Not all Implementing regulations ready yet
- Not all details are clear
- Not all timelines are clear
 - e.g. grace periods
 - Identification methods according Article 51 (4) it is 21st of May 2026
 - but for Article 24 1a (c) according IR 2025/1566 it is 19th of July 2027
- QTSP
 - How to implement new services?

Following drafts (as far as available)..?

Upon agreement between CAB and Supervisory Body..?

Transition periods and missing Implementing Regulations

Can a CAB audit the new Trust Services?

PRACTICALLY, YES, WE CAN!

FORMALLY, NO WE CAN NOT!

Without formal accreditation, we are not allowed to issue **the appropriate** conformity assessment report!

Accreditation processes needs time!

As of today, not a single CAB is accredited to audit the new trust services!

**CABs need formal and legal GO to
perform Conformity Assessments!**

Speaker



Boryana Uri

Deputy Head Trust Infrastructure Div.

TÜV TRUST IT GmbH

TÜV AUSTRIA Group

Phone: +4942605459

Boryana.Uri@tuv-austria.com