5) TSP Supervision, Certification and Audit under eIDAS Part III

Presented by: Arno Fiedler

For: Training on ETSI Standards for trust services
eIDAS Part III Audit and Supervision Framework

eIDAS Audit Framework (Art 17, 18, 19)

TSP+CAB+SB=>TSL
eIDAS Qualified Trust Services Supervision process flow


© ETSI 2021 – All rights reserved

5) TSP Supervision, Certification and Audit under eIDAS Part III
ETSI Best practise audit framework

**EN 319 403-1 on requirements for bodies auditing TSPs**

- Primary reference: ISO/IEC 17065 specifying general requirements for conformity assessment bodies (CABs) performing certification of products, processes, or services
- Supplements ISO/IEC 17065 to provide additional dedicated requirements for CABs performing certification of TSPs
- Incorporates additional requirements on CABs relating to the audit of a TSP's management system, as defined in ISO/IEC 17021 and in ISO/IEC 27006

**New supplements on additional requirements for CABs auditing**

- Part 2: TSPs issuing PTC (e.g. as in CA/Browser Forum)
- Part 3: QTSPs against eIDAS Regulation
Audits based on EN 319 403

- Audit report provided to supervisory body every 2 years
- Full audit required in case of major changes
- Meets the eIDAS requirement areas (esp. Art. 19, 24, 28)
- Follows best practices (e.g. ETSI standards 319 401 and 411)
- Communication with supervisory body
Audits based on EN 319 403

Document assessment (security concept / operations) – Stage 1
- all necessary technical, functional and organisational security measures and
- their appropriateness for fulfilment of eIDAS requirements

On-Site assessment – Stage 2
- verify the implementation of security measures,
- including technical and penetration testing

Results report
- scope: identification of the TSP, service and policy
- content and summary of conformity assessment activities
- additional content as required by supervisory authority
Conformity assessment process flow

Preparation
- Preparation (e.g., design, testing, staging) of Provision of QTS
- Documentation
- Scope and purpose of the assessment
- Dialogues with SB
- Selection of CAB
- Trialogue with SB & CAB
- Assessment preparation with CAB

Review of documentation incl.:
- Security concept
- Risk assessment
- Practices & policies
- Processes, procedures & instructions of work
- Plans (e.g. BCP, DRP, TP)
- Agreements
- Etc.

Passed

Technical set-up
- Technical processes
- IT network & ISMS
- Trustworthy systems
- Execution of plans
- Evidence & logs review
- Organisational aspects
- Procedures & work instructions
- Sampling & testing
- Etc.

Passed

Certificate
- Certification report

(Surveillance)
Re-assessment

Timeline to become a TSP

Source: Christoph Sutter, TUVIT GmbH, CA-Day 2016

1. preparation
   - S1
   - S2
   - SB

2. preparation
   - S1
   - S2
   - SB

3. prep
   - S1 & S2
   - SB

4. S1/S2

1. new TSP normal case (~1 year)
2. new TSP very fast case (~9 month)
3. existing TSP normal case (~6 month)
4. re-assessment of Q-TSP (~1 month)
Complete Toolset for auditing trust services *(and Identification?)*

**EN 319 403(-1) TSP Conformity Assessment (based on ISO 17065) in context of European Accreditation for Audit Bodies**

**Conformity Assessment**
- TS 319403-2: Additional requirements for CAB auditing TSP that issue Publicly- Trusted Certificates
- TS 319403-3: Additional requirements for CAB assessing qualified TSP against the eIDAS Regulation requirements

**Certification Policies**
- General Policy
- EN 319 401 General TSP Policy Requirements including generic eIDAS based on ISO 27002 Req.

**Certificate Profile**
- EN 319 412-1 Certificate Profiles and common data structures

**Checklist**
- TR 119 411-4: Check-list for self-assessment or independent conformity assessment of TSPs issuing certificates according to EN 319 411-1 and/or EN 319 411-2 with 540+ controls

**eIDAS and CA/Browser Forum**
- EN 319 411-1 TSP issuing X.509 Certs for Policy Level LCP/NCP/BR/EV
- EN 319 412-2 Natural Persons
- EN 319 412-3 Legal Persons
- EN 319 412-4 QWACs

**eIDAS Qualified Trust Services**
- EN 319 411-2 TSP issuing Qualified Certs for Signatures, Seals and Websites
- EN 319 412-5 QC-Statements
Many thanks!
Arno Fiedler