The struggle of auditing – Towards harmonization of conformity assessments

Matthias Wiedenhorst
Head of Certification Division TSP

CA-Day, 2019-09-26

TÜV NORD GROUP

ACCREDITATION SCHEMES

- In practical, there is only one accreditation scheme for conformity assessment bodies under the European trust service auditing framework

  Accreditation according to ISO/IEC 17065 and ETSI EN 319 403 as conformity assessment body with eIDAS Art. 3 (18) scope of accreditation by the responsible national accreditation body

Name:		TÜV Informationstechnik GmbH
URL to body:		https://www.tuvit.de/en/services/eid-trust-services/
Date of accreditation:		24.06.2016 (until 17.07.2023)
URL to accreditation certificate:	'de'	http://www.dakks.de/as/ast/d/D-ZE-12022-01-01.pdf
QTSP/QTS type(s) for which accreditation is granted:		All
Accreditation scheme:		ISO/IEC 17065 + ETSI EN 319 403 + eIDAS Art.3.18 scope of accreditation
URL to eIDAS conformity assessment scheme:		-
URL to CAB's Directory of assessed QTSP/QTS:		https://www.tuvit.de/en/certification-overview-1265-4512.htm

Example from EU list of accredited CABs
https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation

AUDITING FRAMEWORK

- Only one set of European Standards applied for auditing of Trust Service Providers

ETSI EN 319 xxx series of European Norms and related / referenced standards

TSPs supporting digital signatures and related services								Replaces	Expected publication
			Sub-areas						
			Guidance						
TR	1	19	4	0	0		Guidance on the use of standards for TSPs supporting digital signatures and related services	(new)	published
			Policy & Security Requirements						
EN	3	19	4	0	1		General policy requirements for trust service providers	Replacing generic parts of TS 101 456, TS 102 042, (TR 102 040), TS	published
EN	3	19	4	1	1		Policy and security requirements for trust service providers issuing certificates - Part 1: General requirements - Part 2: Requirements for trust service providers issuing EU qualified certificates - Part 3: *To be withdrawn* - Part 4: Requirements for trust service providers issuing code signing certificates	- TS 102 042 (EV & BR), EN 319 411-3 - TS 101 456 (& TR 102 458), EN 319 411-3 - historical - (new)	- published - published - withdrawn - undefined
EN	3	19	4	2	1		Policy & security requirements for trust service providers issuing time-stamps	TS 102 023	published
EN	3	19	4	3	1		Policy and security requirements for trust service providers providing AdES digital signature generation services	(new)	Undefined
EN	3	19	4	4	1		Policy and security requirements for trust service providers providing AdES digital signature validation services	(new)	Undefined
			Technical Specifications						
EN	3	19	4	1	2		Certificate profiles - Part 1: Overview and common data structures - Part 2: Certificate profile for certificates issued to natural persons - Part 3: Certificate profile for certificates issued to legal persons - Part 4: Certifcate profile for web site certificates - Part 5: QCStatements	- (new part) - TS 102 280 & TS 101 862 - (new part) - (new part) - TS 101 862	all parts published
EN	3	19	4	2	2		Time-stamping protocol and time-stamp token profiles	TS 101 861	published
EN	3	19	4	3	2		Protocol profiles for trust service providers providing AdES digital signature generation services	(new)	Undefined
EN	3	19	4	4	2		Protocol profiles for trust service providers providing AdES digital signature validation services	(new)	Undefined

Excerpt from ETSI TR 119 000, V1.2.1 (2016-04)

CONFORMITY ASSESSMENT

- ETSI EN 319 403 - Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers
  - Different requirements for conformity assessment
  - For this presentation I'm going to focus on audit times

7.4.2 Audit time

The Conformity Assessment Body shall allow auditors sufficient time to undertake all activities relating to an initial audit, surveillance audit and re-assessment audit. The time allocated shall consider the following factors:

a) the size of the trust service scope (e.g. number of information systems used, number of employees, number of certificates issued);

b) complexity of the trust service;

c) the type(s) of business performed within scope of the trust service;

d) extent and diversity of technology utilized in the implementation of the various components of the trust service;

e) number of sites;

f) previously demonstrated performance of the trust service;

g) extent of outsourcing and third party arrangements used within the scope of the trust service;

h) the standards, publicly available specifications and regulatory requirements which apply to the certification; and

i) existing certifications.

EXAMPLE: Existing certifications can include information security management certification according to ISO/IEC 27001 [i.8] or product certification against ISO/IEC 15408 [i.7].

The Conformity Assessment Body shall document the justification of the amount of time used in any initial audit, surveillance audits and re-assessment audit.

HARMONIZATION OF CONFORMITY ASSESSMENTS

- So there is **one** accreditation scheme and **one** auditing framework
- Can we expect conformity assessment bodies to calculate harmonized audit times?

The answer is **not** yes…

…at least not today…

CALCULATION EXAMPLE

- Trust Service Provider offering a collection of different qualified and non-qualified trust services
- All services shall be audited and certified in a joint assessment project

CALCULATION EXAMPLE

LCP, NCP, NCP+, DVCP, IVCP, OVCP, EVCP, CSCP, qcp-n-qscd, qcp-l-qscd, qcp-n, qcp-l, qcp-w

- The most minimalistic TÜViT calculation approach
- Presuming several assumptions that I‘ve never seen to hold in real live
- Would results in an assessment project of
  - Approx. 14 person days of On-site audit

- Competitor calculation result as published on certificate

The full audit took 16 days. The risk analysis assessment requirements described in ETSI 319411-1 consideration of section 7.1.

Start date of the audit: [redacted]	End of the audit: [redacted]	
Documentation inspection:	[redacted]	11 days
Risk analysis evaluation:		1 day
On-site audit:		2 days
Audit report preparation:		2 day
Examined period		[redacted]

- How harmonized are 14 days of audit with 2 days of audit?

HARMONIZATION OF CONFORMITY ASSESSMENTS

- *"The purpose of the audit shall be to confirm that the [QTSP / QTS] fulfil the requirements laid down in this Regulation."* (Regulation No. 910/2014, Article 20)
- Regulation does not define a required level of detail during conformity assessments
- Attemps to include calculation guidelines into ETSI EN 319 403 all failed due to lack of consensus
- At the end of the audit, after all questions deemed necessary and important have been asked, the auditor has to be sufficiently satisfied and convinced about the conformity of the TSP operations according to the best of his knowledge

HARMONIZATION OF CONFORMITY ASSESSMENTS

- Who could solve the problem?
  - Trust Service Providers
    - Often forced to choose the cheapest, but even if not…
    - Why invest in a longer audit, if the shorter fulfils the same goal
  - Conformity Assessment Bodies
    - Longer audits result in higher prices
    - Shorter audits increase the risk of missing material problems with the trust service
  - Supervisory Bodies / Report Consumers
    - Can’t / Won’t decline conformity assessments from duly accredited conformity assessment bodies
- Can ACAB’C provide assistance?

Accredited Conformity Assessment Bodies Council (ACAB-c)

www.acab-c.com

ACAB'C in short

- Association of CAB, all members "A" are private companies
- "A" Members provide conformity assessment of TSP
- It's main goal is to harmonize amongst CABs a comparable/standardized application of the conformity assessment requirements by different CABs in respect with the REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS).
- Trusted by accreditation based on ISO standards (ISO 17065, ETSI EN 319403)
- New: Free of charge membership available

HARMONIZATION OF CONFORMITY ASSESSMENTS

- Possible resolution
  - ACAB-c
    - *Could develop a reference audit time calculation*
  - Conformity Assessment Bodies
    - *Would have to justify their audit time calculation*
  - Supervisory Bodies / Report Consumers
    - *Could request justification for material deviations from reference calculation window*

Thank you for your attention!

Your contact person

Matthias Wiedenhorst

Head of Certification Division TSP
IT Infrastructure
+49 201 8999-536
m.wiedenhorst@tuvit.de

The Accredited Conformity Assessment Bodies' council

72 Bd Edgar quinet
75014 Paris – France

secretary@acab-c.com

TÜV NORD GROUP