The struggle of audit reporting

Matthias Wiedenhorst
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.

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

<table>
<thead>
<tr>
<th>TSPs supporting digital signatures and related services</th>
<th>Replaces</th>
<th>Expected publication</th>
</tr>
</thead>
<tbody>
<tr>
<td>TR 1 20 4.1 1 Guidance on the use of standards for TSPs supporting digital signatures and related services</td>
<td>(new)</td>
<td>published</td>
</tr>
<tr>
<td>EN 2 20 4 3 General policy for requirements for trust service providers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EN 3 20 4.3 1 Policy and security requirements for trust service providers issuing certificates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EN 3 20 4.3 2 Policy and security requirements for trust service providers providing AEnS digital signature generation services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EN 3 20 4.3 3 Policy and security requirements for trust service providers providing AEnS digital signature validation services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EN 3 20 4.3 3 Technical specifications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EN 3 20 4.3 1 2 Certificate profiles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EN 3 20 4.3 2 2 Time-stamping protocol and time-stamp token profiles</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

- So there is one accreditation scheme and one auditing framework
- How many reporting frameworks do we need?

The answer is not one...

...at least not today...
REPORTING FRAMEWORK

- ENISA – Guideline "Conformity assessment of Trust Service Providers"
- Requirements from Supervisory Bodies
  - Reporting required in national language
  - Special reports regarding national eIDAS implementation laws required
  - Special content requirements
- ETSI TS 119 403-2 V1.1.1 (2018-07)
- ETSI TS 119 403-3
- CAB-Forum requirements
- tbc...
REPORTING FRAMEWORK

- Struggle of audit reporting...
  - for TSPs, because they have to
    - request and maintain different kind of reports for the same service
    - provide to correct report to the different parties
  - for conformity assessment bodies, because they have to
    - maintain a huge variety of reporting templates and template variants
    - identify the correct set of reports for the given use case
  - for supervisory bodies / report consumers, because they have to
    - verify whether or not they received the correct report variant
REPORTING FRAMEWORK

- Who could solve the problem?
  - ACAB-c ?
  - FESA ?
  - European Commision ?

eIDAS Art. 20, 4 (a):
The Commission may, by means of *implementing acts*, establish reference number of the following standards:
(a) accreditation of the conformity assessment bodies and **for the conformity assessment report** referred to in paragraph 1;
CONCLUSION

- There are too many different report types

- The goal of having only one report per trust service might be unrealistic

- Nevertheless all parties should work together and try to minimize variants in order to fulfil the eIDAS goal of European Harmonization
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