EU Trusted Infrastructure: eIDAS - View of Conformity Assessment Bodies

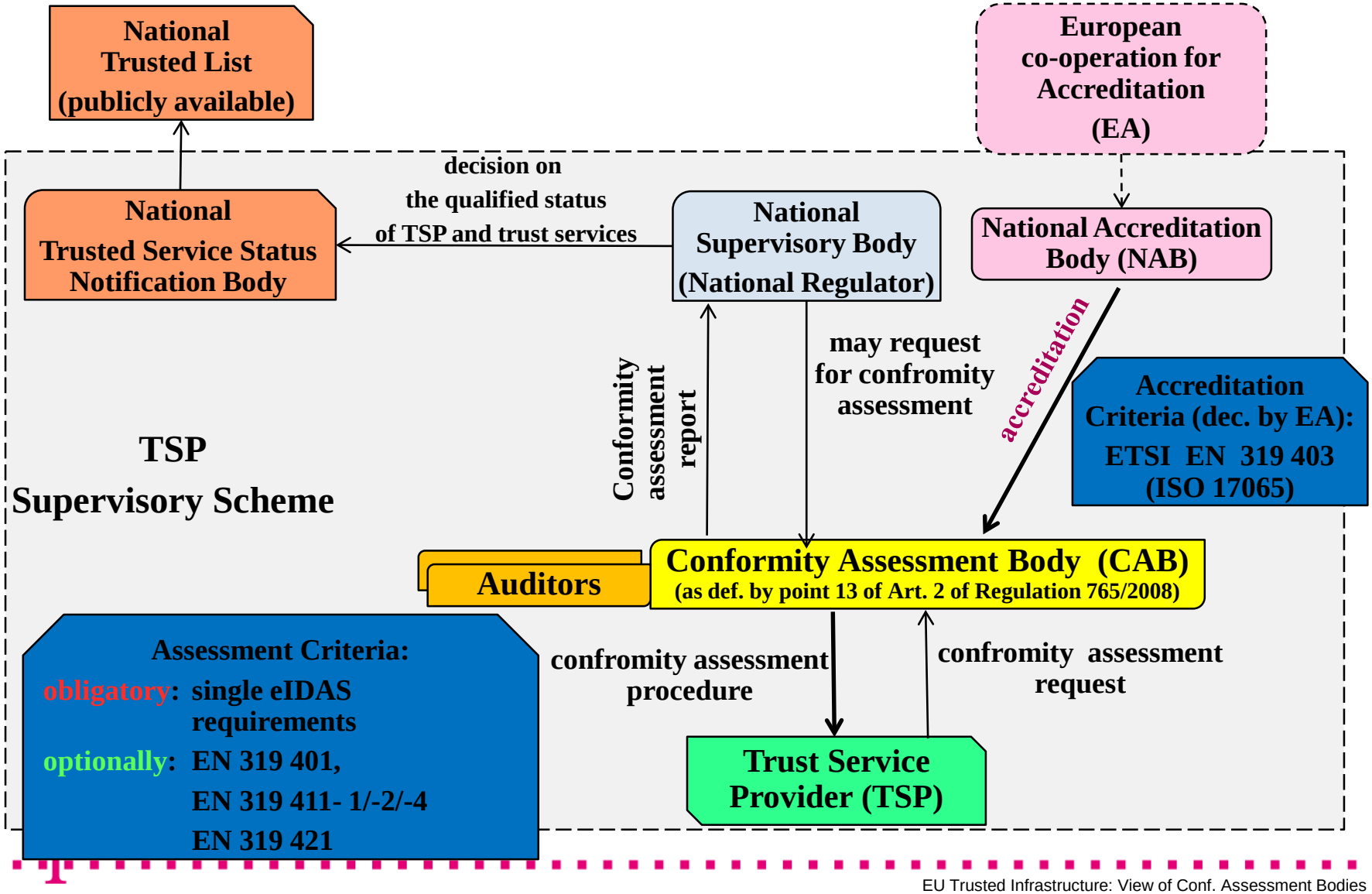
Dr. Igor Furgel
T-Systems International

29th Forum UN/CEFACT,
Mini Conference,
Geneva

What are we speaking about?

- Conformity Assessment Bodies (CABs) within Supervisory Scheme for Trust Service Providers (TSPs)
- CABs Tasks and Conformity Assessment Criteria
- Duties of CABs and Supervisory Bodies (SBs)
- Conformity Assessment Procedure and Report
- Harmonization Challenges for CABs and SBs

CABs: Organisational Embedding into the TSP Supervisory Scheme



CABs and Supervisory Bodies: Separation of Duties

- *Article 17 (4)*:

  " ...the tasks of the supervisory body shall include in particular:

  (b) to *analyse* the conformity assessment reports referred to in Articles 20(1) and 21(1);

  (e) to carry out audits or *request* a **conformity assessment body** to perform a conformity assessment of the qualified trust service providers in accordance with Article 20(2);

  (g) to ***grant*** **qualified status** to trust service providers and to the services they provide and to withdraw this status in accordance with Articles 20 and 21;"

- Clear separation of tasks:
  - **CAB**: confirms (or not) the **compliance** of TSP to eIDAS
  - **SB**: grants (or not) the **qualified status** to TSP acc. to eIDAS

Organisational Embedding of CABs into TSP Supervisory Scheme

- Accreditation of CABs (Article 20 (4))
  - European Accreditation (EA) coordinates National Accreditation Bodies (NAB)
  - NAB determines the fundamental ability of CAB for conducting conformity assessment
  - In accordance with (specific) accreditation criteria (Article 20 (4) – optional Implementing Act): There is no Implementing Act yet, but a **binding decision by EA**
    - EN 319 403 (ref. to ISO/IEC 17065); there, the general requirements of 17065 are supplemented by additional requirements for CABs capabilities for performing conformity assessment (certification) of TSPs and their trust services with resp. to applicable requirements from eIDAS and from the CA Browser Forum
- Attaining this accreditation represents a challenge for CABs that do not possess such accreditation yet.

Tasks of CABs

- Tasks of CABs under eIDAS
  - *perform* the audit of qualified TSPs (Article 20 (1))
  - *report* the audit results in written (a requirement by CAB accreditation)
  - *make* a compliance statement confirming (or disproving) the compliance of a qualified TSP and its qualified trusted services with all the applicable eIDAS requirements (Article 20 (1))
  - *provide* the 'conformity assessment report' with the 'compliance statement' to
    - the TSP (Article 20 (1)) and
    - usually also directly to Supervisory Body (SB) (Article 17 (4) b), Article 20 (2));

    the 'compliance statement ' by CAB is formally *not* binding for SB for granting or not granting the qualified status to TSP, but represents an important decision basis

Conformity Assessment Criteria / Standards

- TSP assessment criteria that shall be used by CABs (Article 20 (4) – optional Implementing Act). There is no Implementing Act yet =>
  - Obligation: Single applicable eIDAS requirements on qualified TSPs and qualified trust services shall be directly applied by CABs as assessment criteria
    - These applicable eIDAS requirements shall be compiled from eIDAS by each single CAB: there is no binding compilation => it may lead to deviations in the assessment scope.
  - Additional option: usage of ETSI EN 319 401, 319 411-x, 319 421 and connected standards additionally to the direct eIDAS requirements

- The current experience shows that there are some different interpretations on the topic of the assessment criteria by Supervisory Bodies => a binding reconcilement between SBs is necessary in order to avoid deviations in the assessment scope

CABs: Conformity Assessment Procedure: How?

- Analysing the TSP Policy Statement (the ‘shall’ state)
  - Certification Praxis Statement (CPS) of TSP
    - based on risk assessment with regard to
    - CPS’s appropriateness for the fulfilment of the applicable eIDAS requirements
- Performing on-site audit (comparison ‘shall’ <=> ‘is’ states)
  - Verification of a
    - correct – i.e. according to the CPS –, and
    - effective (by performing penetration testing)
    implementation of the measures stated in the CPS

s. EN 319 403

- Reporting the assessment results
  - assessment scope: the TSP, the CPS, trust service(s)
  - single conformity assessment activities by auditors as required by the applicable assessment criteria
  - overall assessment verdict by the ‘compliance statement’
- *Deviations between single National Schemes due to different interpretations by SBs are possible (and there)*

CABs: Conformity Assessment Report: How?

- Submitting by TSP to SB regularly (24 months, Article 20(1)) or on request by SB (Article 20(2))
- No specific requirements on the form and content, only general requirements sourcing in the CAB accreditation acc. EN 319 403
- The content of the report will represent the results of the application of the *assessment procedure* (deviations between single National Schemes are already in place)
- The **rigour** of presentation (the level of details) is *not* specified, but may be **crucial for SB** to enable making a decision on 'qualified status' of TSP
- The **form** of presentation is also *not* specified: it is to **assume** that reports might follow / reflect the structure of the single requirements from the applied assessment criteria: eIDAS directly and perhaps EN 319 401, 319 411-x, 319 421.
- *Harmonisation between SBs on the one side, and between CABs and SBs on the other side is necessary*

Harmonised Application of Conformity Assessment Criteria

- Known **general challenge**:

  equally accredited CABs may differently interpret and apply the *conformity assessment criteria*
  => it may result in badly comparable qualification of TSPs and their qualified services

- Known eIDAS **specific challenge**:

  there are some different interpretations by national Supervisory Bodies on the topic of the *assessment criteria* => it may result in non-negligible deviations in the assessment scope
  => it may result in badly comparable qualification of TSPs and their qualified services

Harmonisation Challenges for CABs and SBs

- In order to avoid badly comparable qualification of TSPs and their qualified services, it is necessary
  - to harmonise interpretations by national Supervisory Bodies on the topic of the *conformity assessment criteria* to be applied by all CABs
  - to harmonise comparable / standardized application of the reconciled *conformity assessment criteria* by different CABs acting for the European SBs
- Currently, there is no established procedure for this harmonisation

- Informal "Forum of European Supervisory Authorities for trust service providers" (www.fesa.eu) is a joint platform *of* and *for* SBs as National Regulators, but this Forum **cannot** currently make binding decisions

Re-establishing FESA as the EU Coordinating Body making binding decisions for its members (national SBs) would significantly contribute to the solution of the harmonisation issue

Thank you for your attention!

Dr. Igor Furgel

T-Systems International GmbH
Telekom Security

Certification Body

Bonner Talweg 100
53113 Bonn

igor.furgel@t-systems.com