Bundesnetzagentur

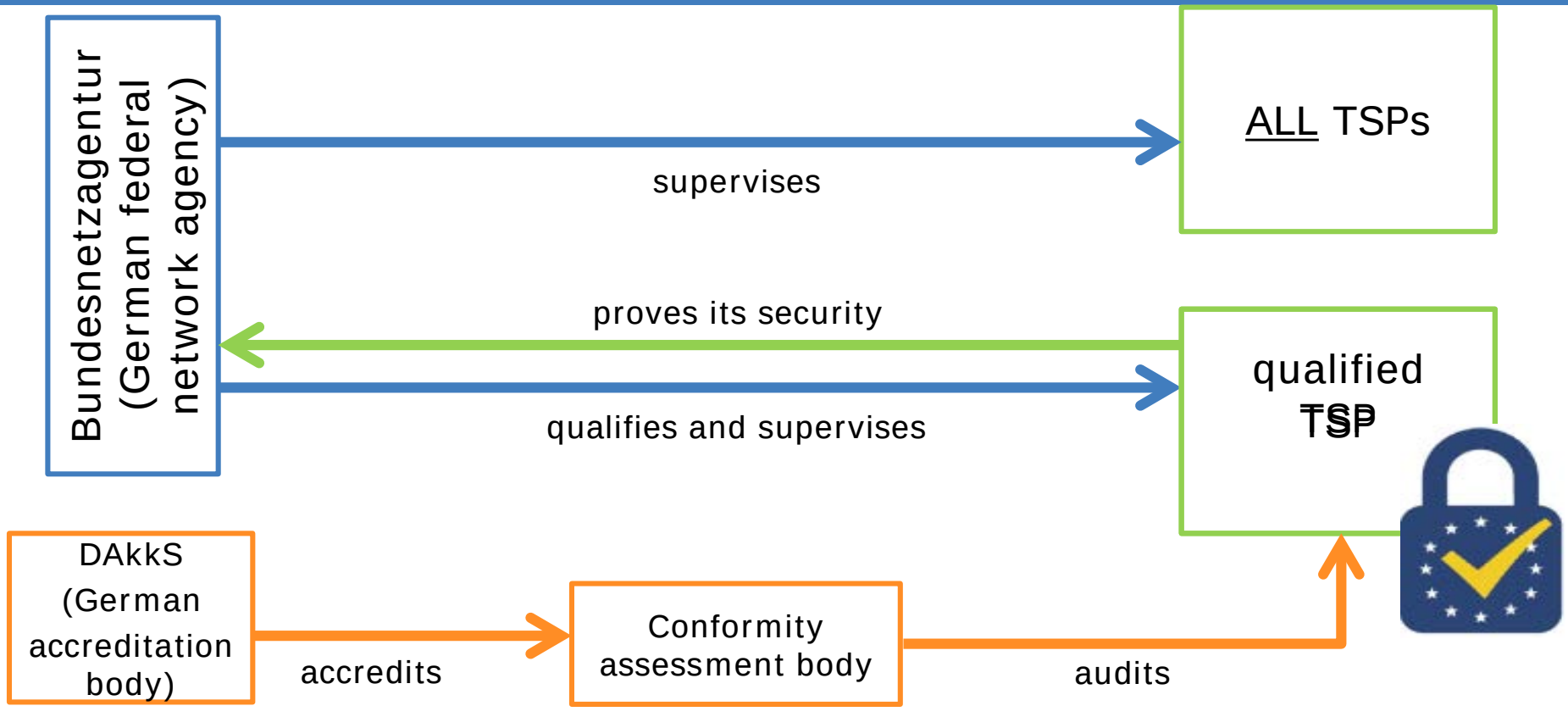
EU Trusted Infrastructure: eIDAS View of Supervisory Bodies

Jürgen Schwemmer

29th Forum UN/CEFACT, Mini-Conference

Geneva, 29.03.2017

Players under eIDAS



What does NOT exist

Most of the non-mandatory „Implementing Acts“ and many of the technical standards needed for the „complete picture“ according to Standardization-Mandate M 460

The Committee according to Article 48 of eIDAS („assisting“ the Commission in the ongoing work)

Official position/mandate for FESA (Forum of European Supervisory Authorities for electronic Trust Services) plus binding rules for collaboration and interpretation of facts, procedures and incidents

What does NOT exist (2)

Harmonized administrative rules and procedures for Supervisory Bodies with respect to (a.o.)

- Liability Insurance (sums insured/liability details…)
- Check of criminal records and other relevant documents
- Fees and fines (occasions, amounts…)

Harmonized regulations in case of TSP´s termination of business or even „disappearance“

„Mandatory“ catalogue for the use of crypto-algorithms

Longterm-Availability under eIDAS?

Duties of qualified Trust Service Providers (TSPs) according to eIDAS Article 24 (2.) lit. (h):

record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information…

Goal: providing proof and ensuring the continuity of services.

Detailed requirements see e.g. ETSI EN 319 411-1

Longterm-Availability under eIDAS? (2)

The TSP shall retain [log(s) of all events relating to the life cycle of keys managed by the CA...] for at least seven years after any certificate based on these records ceases to be valid.

By this (only) nothing is said about how and/or how long information is available

after termination of business/end of service

of the Certificate Provider (TSP)!

Longterm-Availability under eIDAS? (3)

Art. 24 (4): Information on the validity or revocation status shall be made available at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.

Again, nothing is said about how and/or how long information is available

<u>after termination of business/end of service</u>

of the Certificate Provider (TSP)!

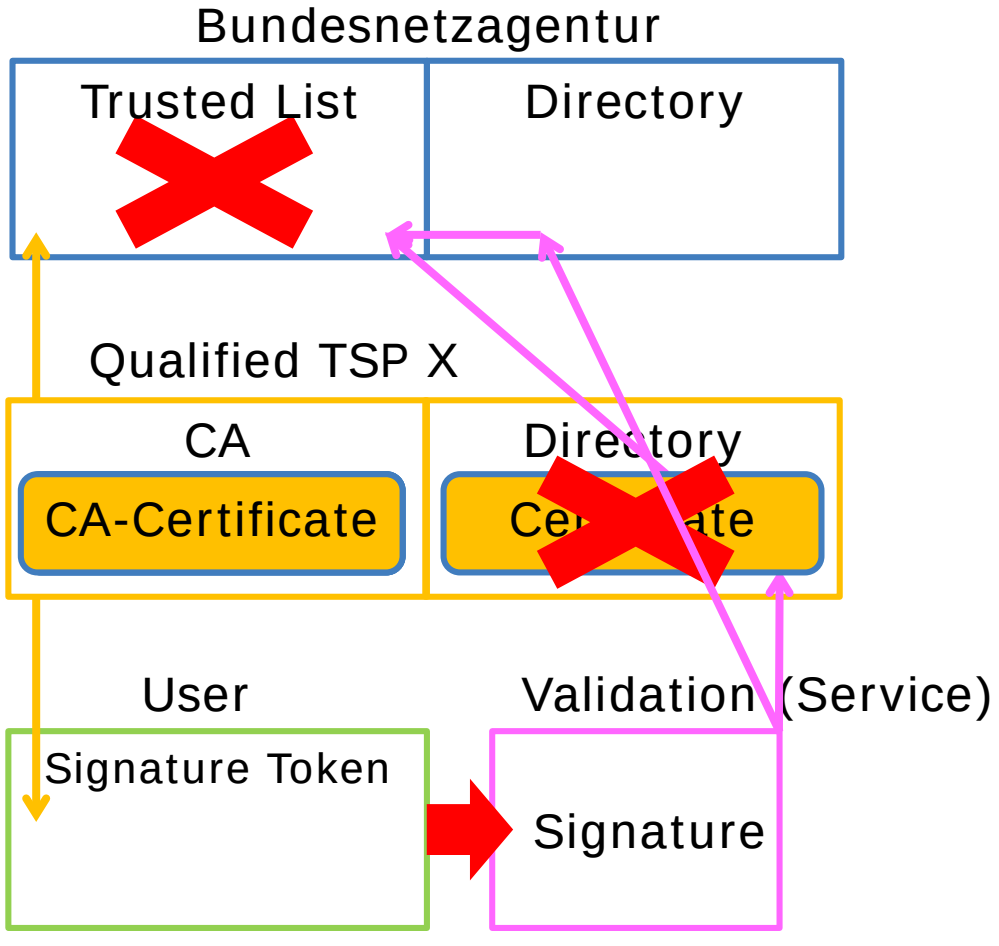
What absolutely MUST be assured w.r.t. qualified electronic signatures and seals

In case of operational setting of the Trust Service Provider, issued certificates still must be verifiable, possibly for a very long time, so

„Take-over-concepts“ by a governmental body or by another qualified TSP (if available/suitable) are necessary

In case of (Root-) CA certificate revocation or end of validity period of any certificate, signatures still must be verifiable, possibly for a very long time, so THE method for certificate-verification should be the „Chain“-model

Possible solution for takeover



Bundesnetzagentur

Thank You! Questions/Comments?

Jürgen Schwemmer

juergen.schwemmer@bnetza.de
eidas@bnetza.de
www.bnetza.de/evd