Bundesamt
für Sicherheit in der
Informationstechnik

Trust?

Jens Bender
Federal Office for Information Security

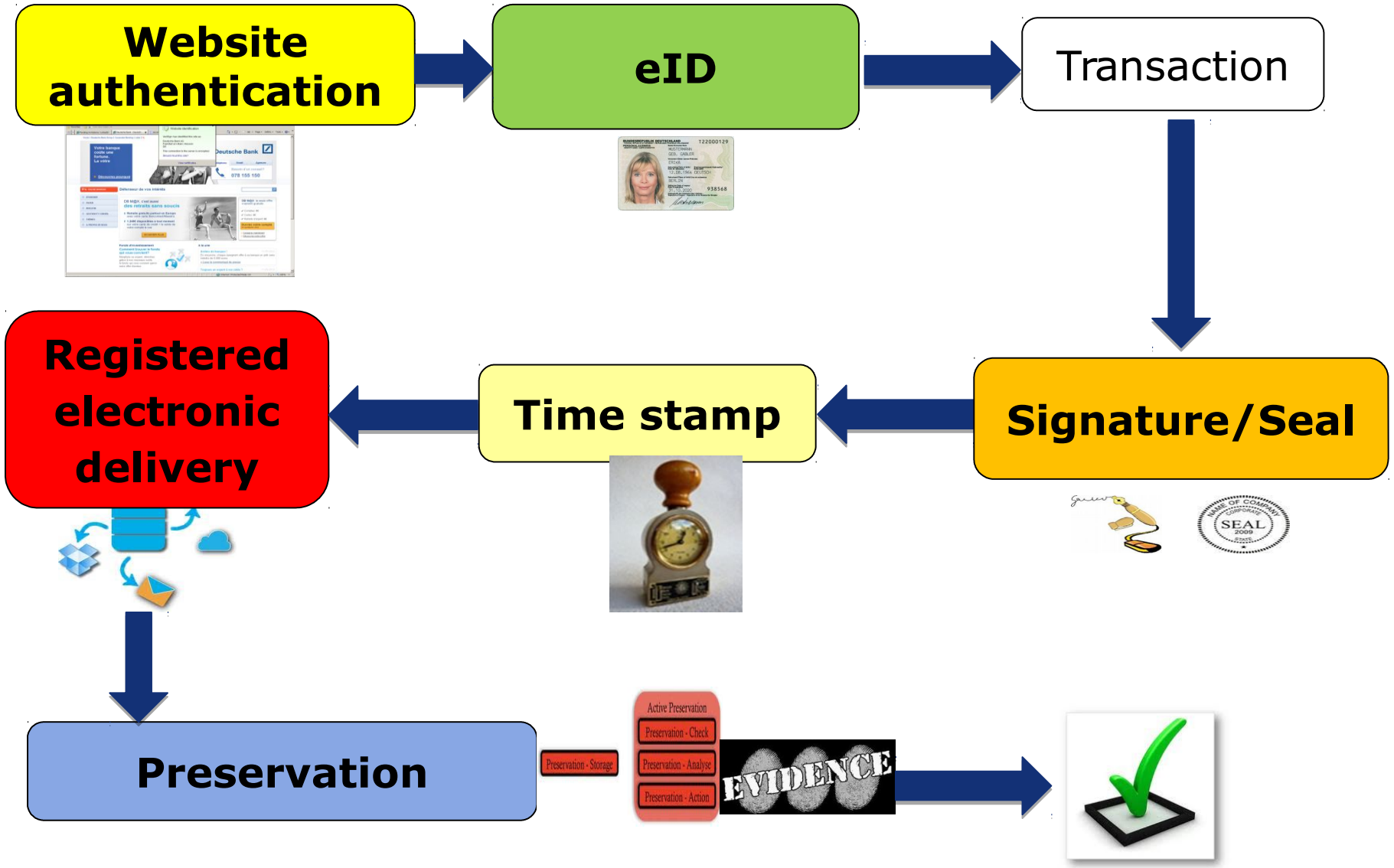
eIDAS Regulation

Recital (1)

Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services.

[Remark: Why is „lack of legal certainty“ singled out? What about a „lack of trustworthiness“ or „lack of trust in correct handling of personal data“?]

eIDAS Regulation



Germany

- Electronic identification for natural persons
  - Card based „Personalausweis“
- Qualified signature since 1999
  - ... and Time Stamps, Long Term Preservation
  - No seals until eIDAS
- Registered electronic delivery
  - De-Mail
- Trusted electronic services key to eGovernment
  - Take up: mixed

De-Mail

Trust is (a) key – random examples

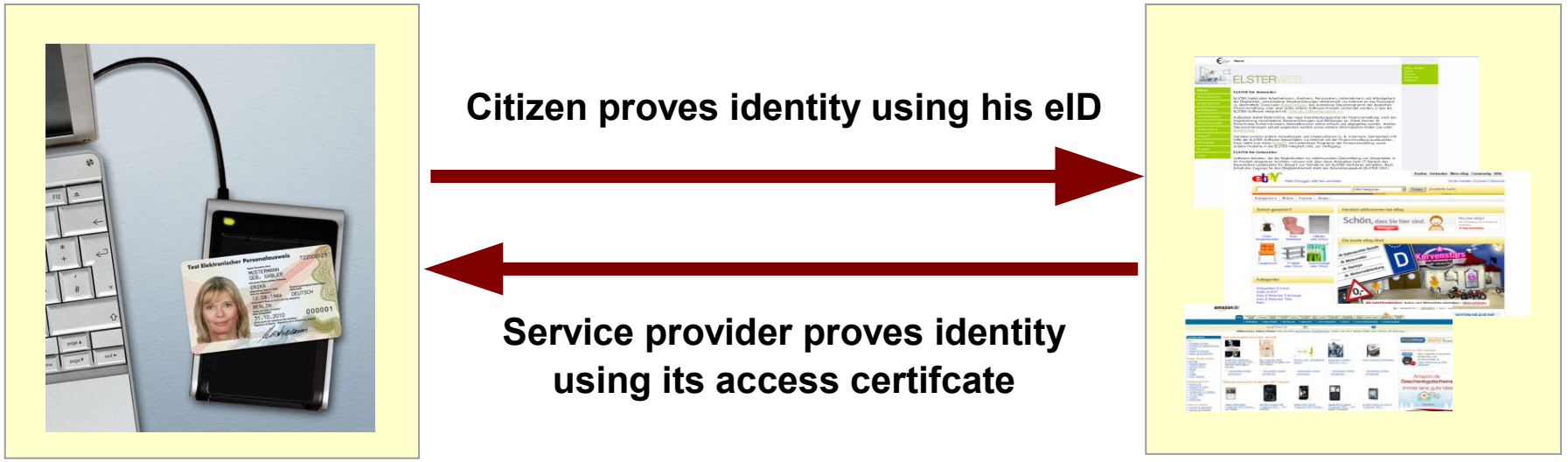
- Online transactions: Trust between citizen and service provider
  - Citizens need to trust issuer of eIDs
  - Service provider need to trust issuer of eIDs
  - If 3rd parties are involved (e.g. IdP), they need to be trusted
- Does a (Q)ERDS-provider respects confidentiality of data?
  - eIDAS only requires integrity/authenticity...
- Is a CA issuing qualified certificates doing its job?
- Remote Signatures
  - How to authenticate users?
  - is access to keys sufficiently controlled?

Trust Model – The simple one

Example: German eID Card

- Gov issues eID Cards and grants access to service provider
  - All other parties (vendor, CAs, …) are supervised by Gov

  → Only one party needs to be trusted by both sides



Bundesamt für Sicherheit in der Informationstechnik

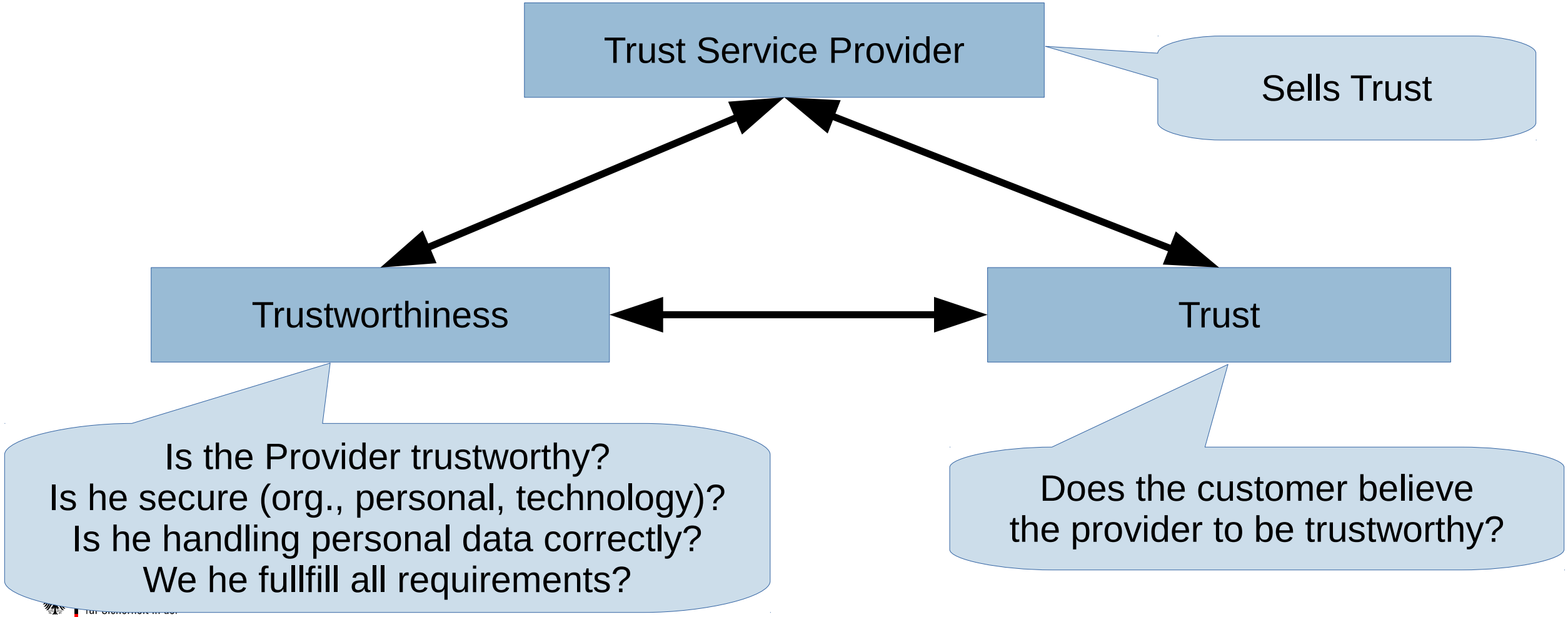
Trust Models – More complex

- Qualified certificates on national level
  - Several CAs, audited by different CABs
  - But: Common supervision

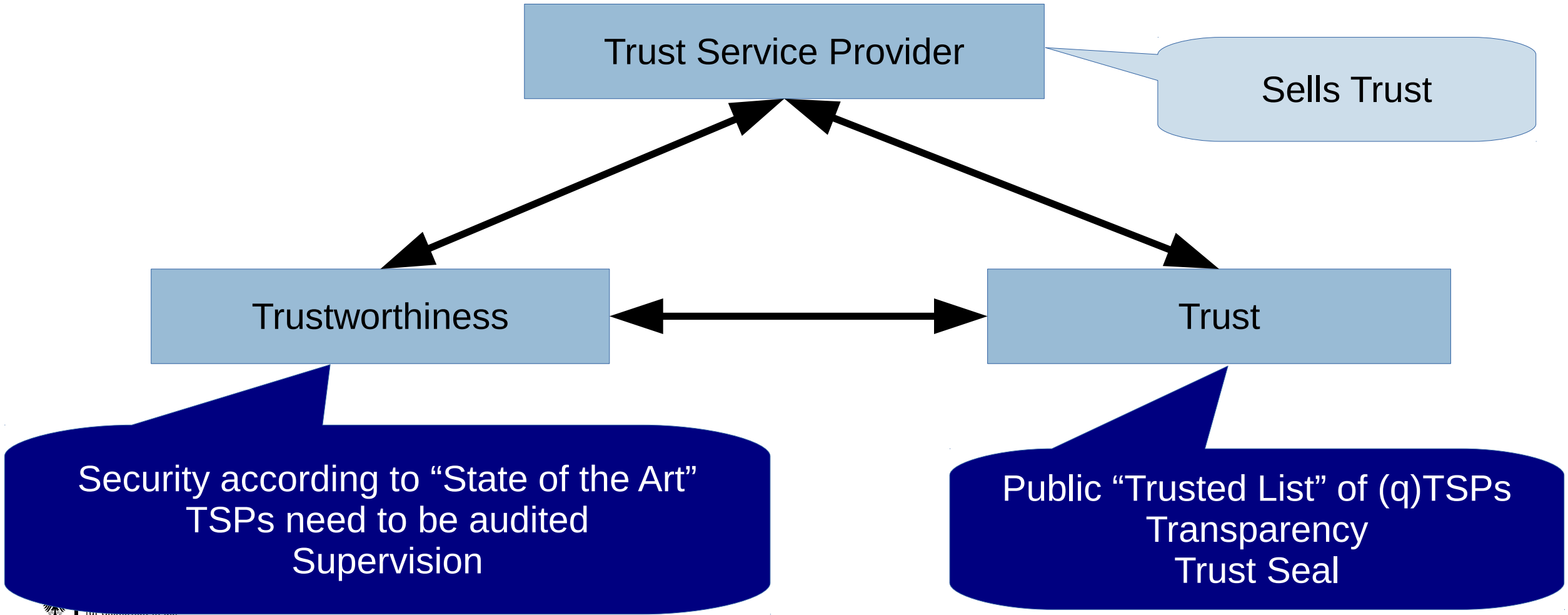
- Registered Electronic Delivery
  - Sender ↔ (Q)ERD Service Provider S ↔ (Q)ERD Service Provider R ↔ Recipient
  - In DE: Common rules „Technical Guideline De-Mail“
  - Nationally: Common supervision

- Everything gets more complicated if we cross borders
  - No common supervision
  - Not necessarily common standards

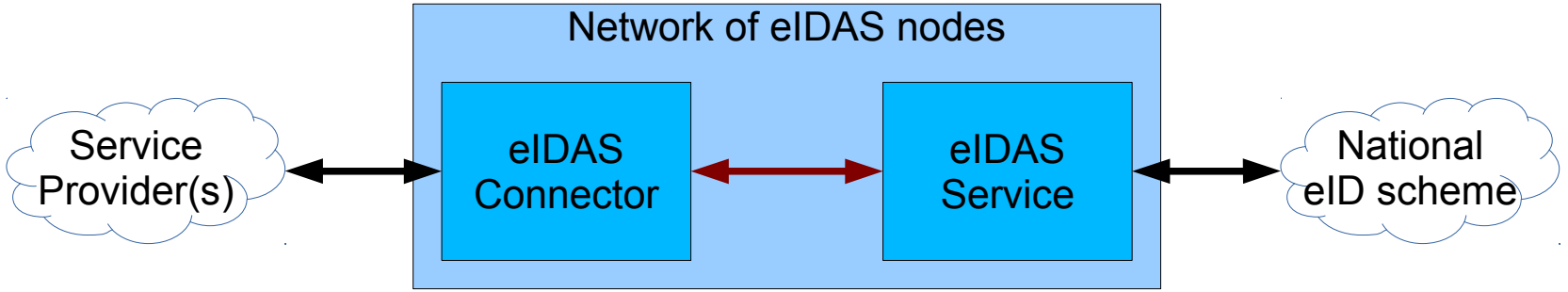
Trust and Trustworthiness



eIDAS – Crossborder trust for Trust Services



eIDAS – Crossborder trust for eIDs



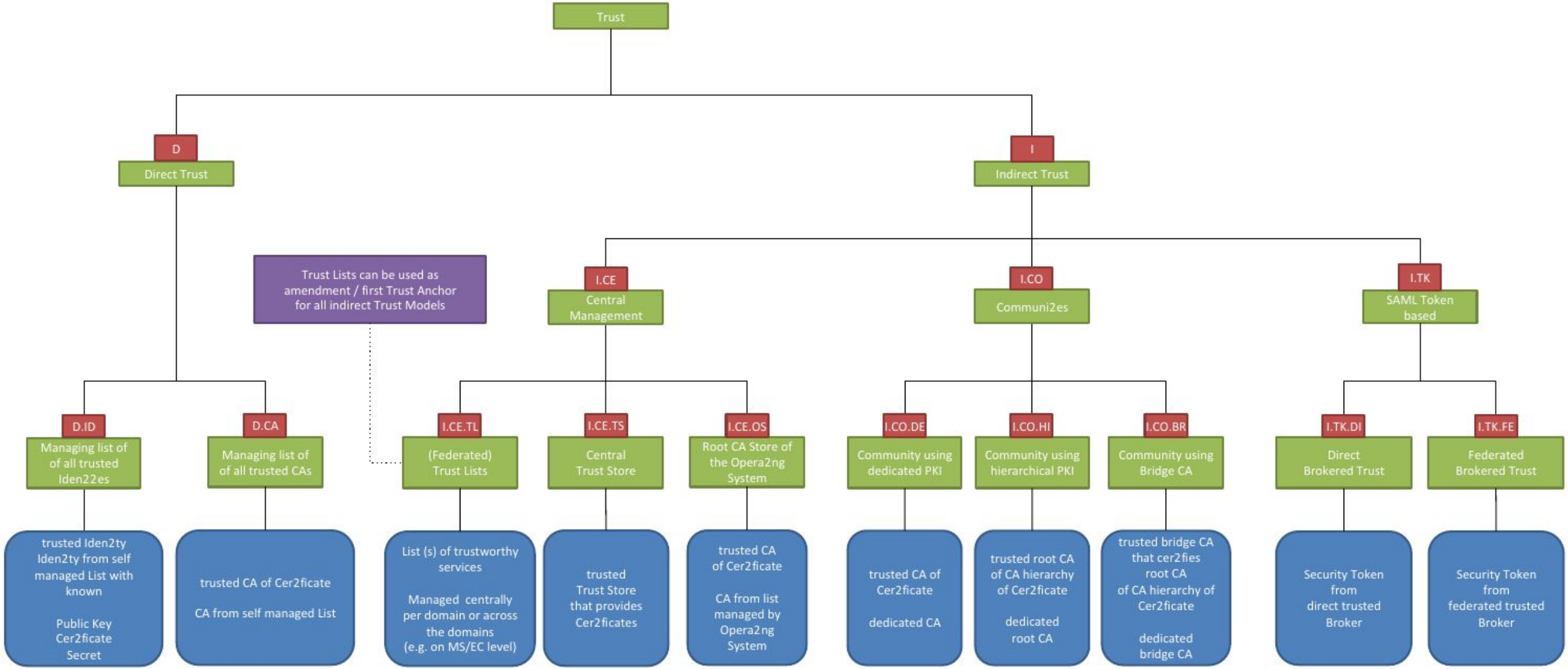
- Security of Nodes via requirements in Implementing Act
- National eID schemes
  - Trustworthiness assessed via „Level of Assurance“
  - Trust via notification and peer review
- Service Provider?

Trust Models – The Mess

Qualified website certificates

- Several hundred CAs worldwide issuing website certificate
  - Any CA can issue a certificate for any domain
- Managed by Trust Store in Browser / Operating System
  - Who is managing these Trust Stores?
  - Is Security/Trustworthiness part of their business model?
  - Have security failures impact on their business?
- User delegates trust decision to third party
  - But choice of browser rarely depends on „quality“ of TS

Trust Models – eSENS



We need...

- … electronic services for ...
  - Identification of persons and things
  - Document authenticity and integrity
  - Document transmission
- … in order to facilitate ...
  - eGovernment
  - eBusiness
  - Digitization of „everything“
- … and they need to be …
  - Trustworthy
  - Trusted
  - Usable for their purpose

Thanks for your attention!

Contact

Jens Bender
Section „eID-Technologies and smart cards“
jens.bender@bsi.bund.de
Tel. +49 (0) 228 99 9582 5051
Fax +49 (0) 228 99 109582 5051

Federal Office for Information Security
https://www.bsi.bund.de