TeleTrusT it-sa Auditorium 2019

TeleTrusT
Pioneers in IT security.

Ohne IT-Sicherheit gelingt keine nachhaltige Digitalisierung!

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Vertrauensdienste

(PKI, EBCA, Blockchain)

Prof. Dr. (TU NN)

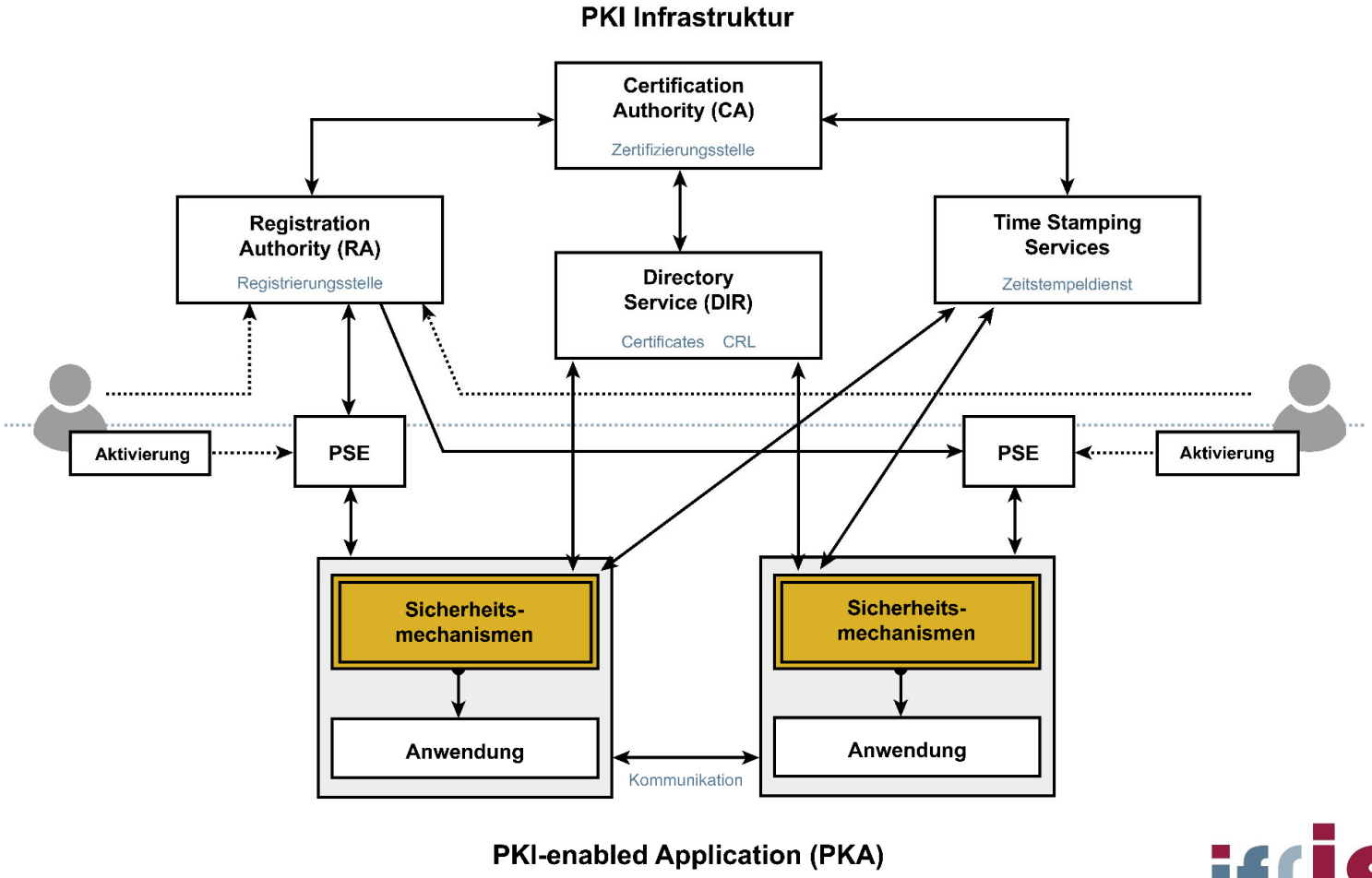
Norbert Pohlmann

Vorstandsvorsitzender - Bundesverband IT-Sicherheit - TeleTrusT

Professor für Informationssicherheit und
Leiter des Instituts für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen

if(is)
internet-sicherheit.

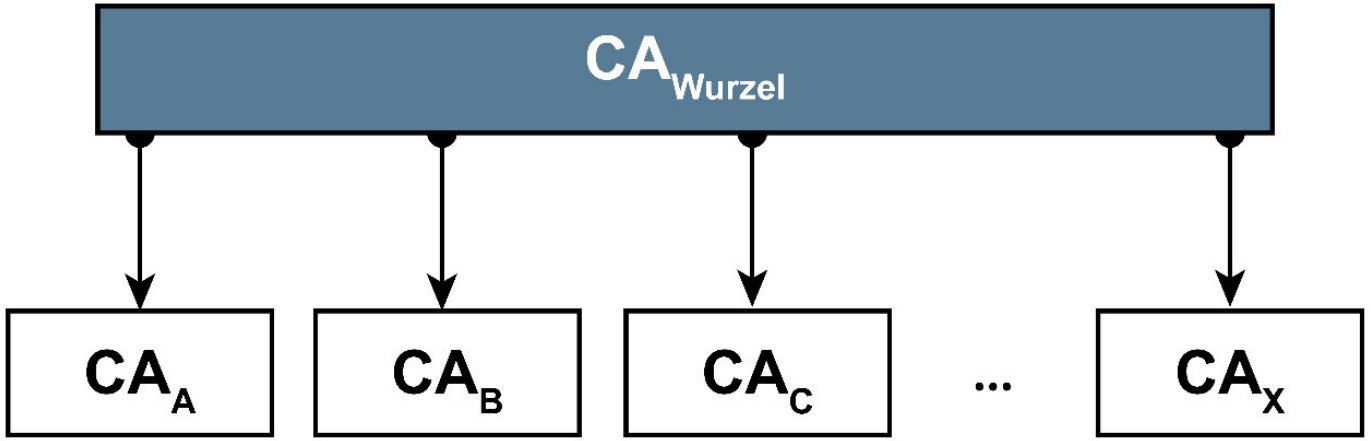
Public-Key-Infrastrukturen
→ Aufbau und Funktionsweise



Public-Key-Infrastrukturen

→ Vertrauensmodell: Übergeordnete CA (Wurzel-CA, Root)

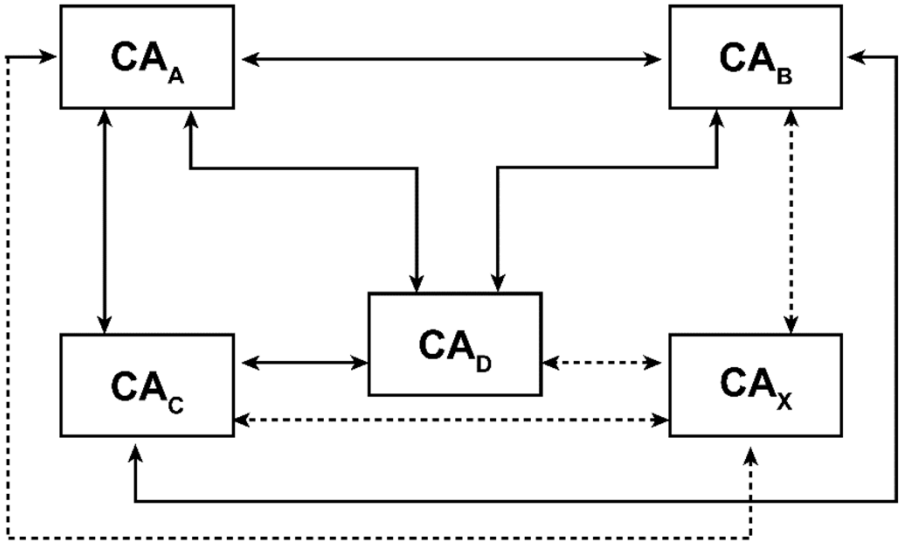
- Wurzel-CA generiert Zertifikate der öffentlichen Schlüssel der untergeordneten CAs.
- Der öffentliche Schlüssel der Wurzel-CA ist im PSE untergebracht oder wird als Zertifikat zum Abrufen angeboten.
- In den meisten Fällen **akzeptieren** Unternehmen, Organisationen oder Länder **keine derartige Unterordnung**.
- Nur in großen, geschlossenen PKI-Systemen etabliert.



Public-Key-Infrastrukturen

→ Vertrauensmodell:n:n-Cross-Zertifizierung

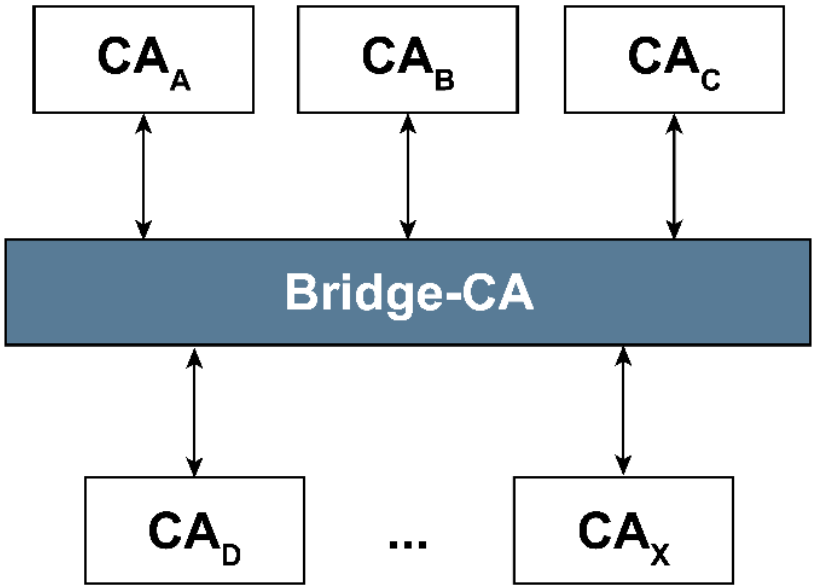
- Jede CA tauscht ihre öffentlichen Schlüssel selbstständig mit jeder anderen CA aus.
- **Authentischer Austausch der öffentlichen Schlüssel aufwendig.**
- Multiple Vertragsverhandlungen nötig.
- Abweichende Verträge und Vereinbarungen zwischen den beteiligten Betreibern möglich.
- Nur bei kleinen Gruppenunabhängiger PKI-Betreiber etabliert, und auch dort nur in abgegrenzten Geschäftsprozessen.



Public-Key-Infrastrukturen

→ Vertrauensmodell: 1:n Cross-Zertifizierung (Bridge CA)

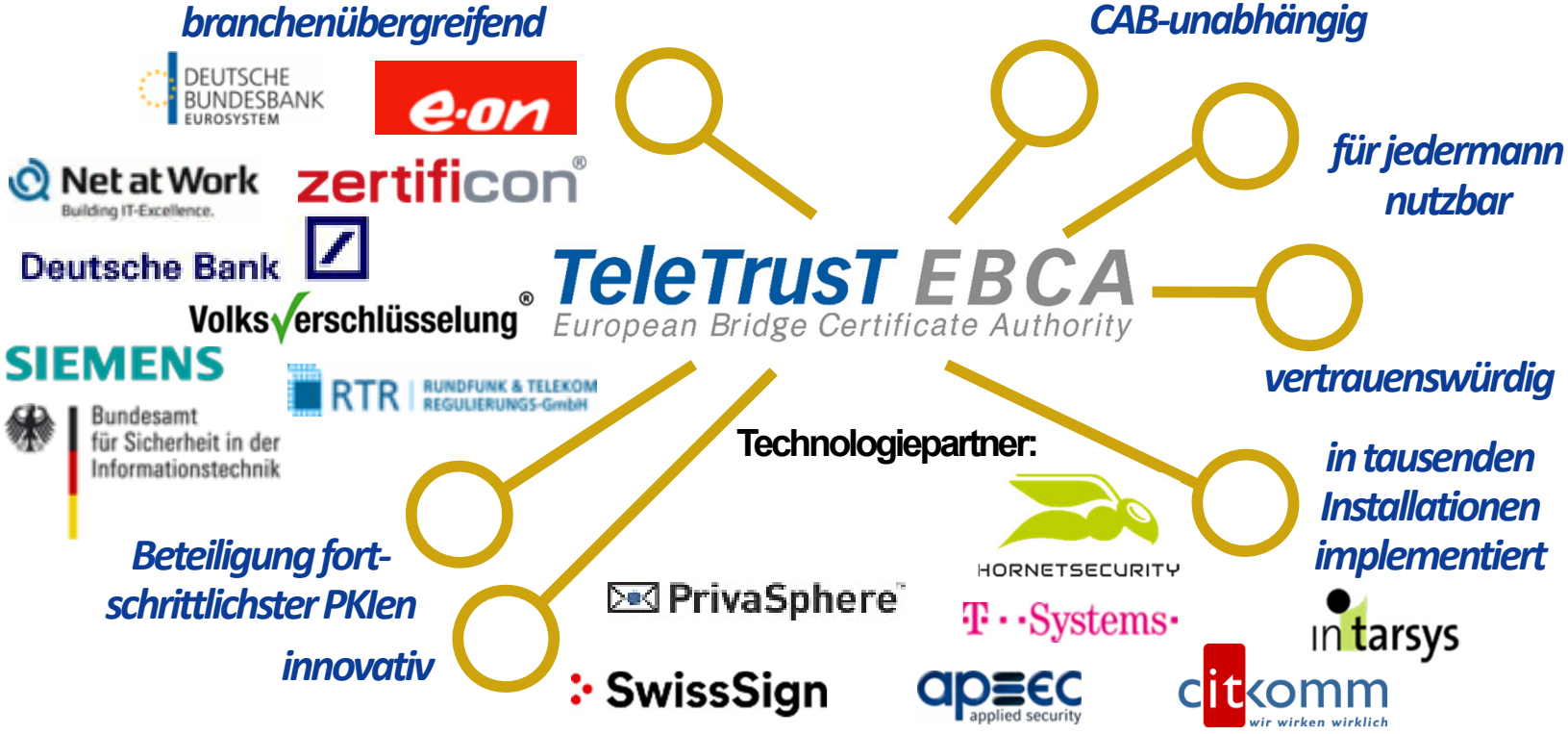
- **Geringer Verwaltungsaufwand, da es für jede CA nur einen Vertragspartner gibt.**
- Entscheidungsfreiheit über die passende Vertrauenskette.
- Bridge CA fungiert als zentrale Vermittlungsinstanz zwischen den beteiligten Organisationen
  → Geeignete Policy benötigt.
- CAs übergeben authentisch ihre öffentlichen Schlüssel an die Bridge CA.
- Bridge CA signiert eine Tabelle der öffentlichen Schlüssel aller beteiligten CAs.
- Die eigene CA stellt dann all ihren Nutzern den öffentlichen Schlüssel der Bridge CA als Zertifikat zur Verfügung.



Bundesverband IT-Sicherheit

→ European Bridge CA (EBCA)

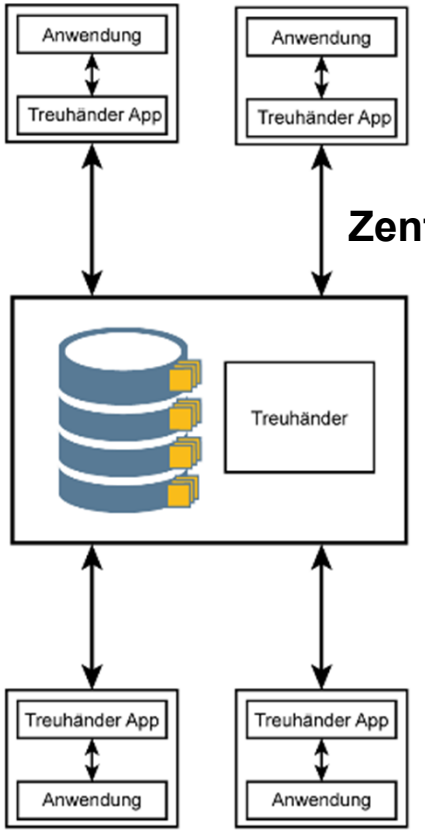
- **Seit 2001: Vertrauenswürdiger PKI-Verbund**
  - → sichere u. vertrauenswürdige Kommunikation über Organisationsgrenzen
  - → mit Signatur, Verschlüsselung und Verifikation



BlockChain-Technologie

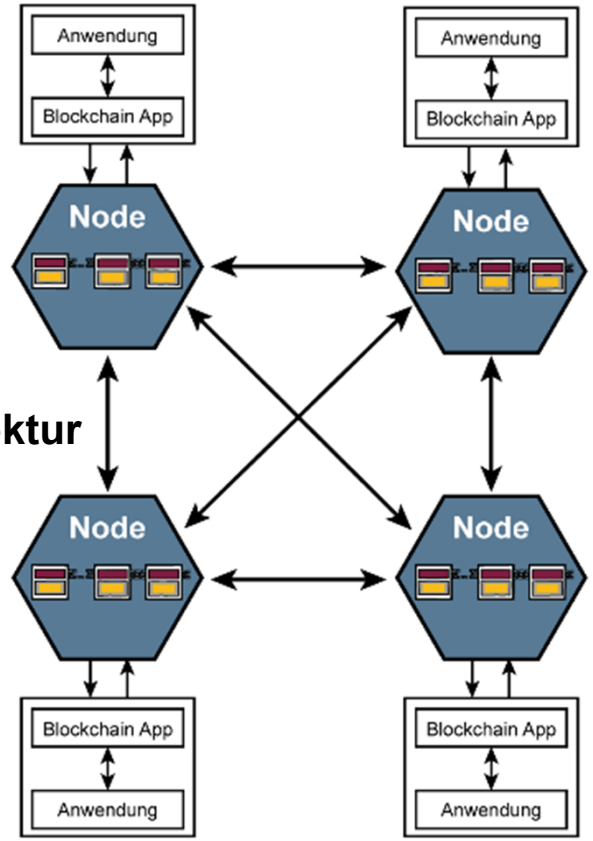
→ auf den Punkt gebracht

Transaktionsspeicher



Zentrale Architektur

Dezentrale Architektur



BlockChain Konzept
→ Unterschiedliche Sichtweisen

- Für einen **Informatiker** ist die **BlockChain** eine **einfache Datenstruktur**, die Daten sind in einzelnen „Blöcken“ verkettet und in einem ***verteilten Netz*** **redundant** (mehrfach) verwaltet.

  Die Alternative wäre z.B. eine konventionelle Datenbank, die von allen Teilnehmern fortlaufend repliziert wird.

- Für die **IT-Sicherheitsexperten** hat die **BlockChain** den Vorteil, dass die **Daten** in den einzelnen „Blöcken“ **manipulationssicher gespeichert** werden können, das heißt, die Teilnehmer an der **BlockChain** sind in der Lage,
  → die **Echtheit**,
  → den **Ursprung** und
  → die **Unversehrtheit der gespeicherten Daten** zu überprüfen.

  Die Alternative wäre z.B. ein PKI-System.

- Für den **Anwendungsdesigner** bedeutet die Nutzung der **BlockChain** -Technologie eine **vertrauenswürdige und automatisierte Zusammenarbeit zwischen verschiedenen Organisationen**.

  Die Alternative wäre z.B. ein kostenintensiver Treuhänder.

Anhang / Credits

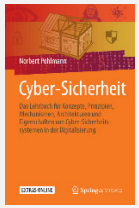
Wir empfehlen

- **Kostenlose App securityNews**

- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/cyberschutzraum

- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/

- **Cyber-Sicherheit**
  Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2019
- https://norbert-pohlmann.com/cyber-sicherheit/



Besuchen und abonnieren Sie uns :-)

WWW
https://www.internet-sicherheit.de

Facebook
https://www.facebook.com/Internet.Sicherheit.ifis

Twitter
https://twitter.com/_ifis

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Quellen Bildmaterial

Eingebettete Piktogramme:
- Institut für Internet-Sicherheit – if(is)

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
https://www.it-sicherheit.de/