TeleTrusT
Pioneers in IT security.

TeleTrusT EBCA

European Bridge Certificate Authority

Infrastruktur: Vertrauen herstellen, Zertifikate finden

TeleTrusT EBCA
European Bridge Certificate Authority

Allgemeines zur TeleTrusT EBCA

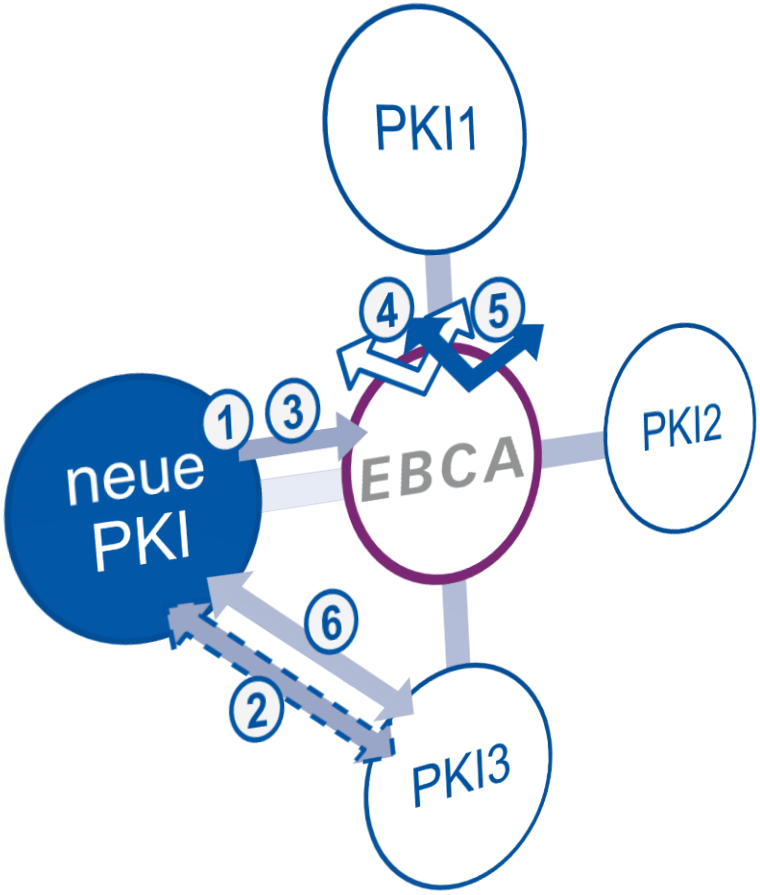
- Seit 2001
- Zusammenschluss einzelner, gleichberechtigter PKIn zu PKI-Verbund
  ➔ einfacher, sicherer E-Mail-Verkehr & Datenaustausch über Internet – mit Signatur, Verschlüsselung und Verifikation
- Zusammenschluss von
  - Unternehmen
  - Institutionen
  - öffentlichen Verwaltungen
- Voraussetzungen
  - eigene Public Key Infrastructure (PKI) mit X.509-Zertifikaten
  - S/MIME-E-Mails
  - eigene Policy
  - Interoperabilitätstest

➔ Es ist dann nur noch ein Vertragspartner nötig (die EBCA), dessen Dienste allen Mitgliedern zur Verfügung stehen

TeleTrusT EBCA
European Bridge Certificate Authority

Wie kann man der EBCA beitreten?

European Bridge CA



Anmeldeprozess

1. Anmeldung, Prüfung
2. Interoperabilitätstest
3. Registrierung, Root-Zertifikat-Übergabe
4. Signierte Certificate Trust List (CTL) — via web
5. Mitarbeiterzertifikate — via LDAP
6. signierte, verschlüsselte E-Mail — via LDAP

TeleTrusT EBCA
European Bridge Certificate Authority

Komponenten der EBCA-Infrastruktur

Die EBCA stellt kostenlos eine Liste der Wurzelzertifikate der Teilnehmer (CTL), sowie einen Verzeichnisdienst bereit.

CTL: Vertrauen herstellen

- Zertifikate der EBCA-Teilnehmer werden vom Nutzer als sicher anerkannt.
- Technische Umsetzung des Vertrauens erfolgt über Installation einer Certificate Trust List (CTL).
- Nicht alle Wurzelzertifikate müssen einzeln anerkannt werden, sondern nur die CTL installiert werden.
- CTL ist signiert, um Integrität zu garantieren.

ebca.de/tools/vertrauen-herstellen/

Web/LDAP: Zertifikate finden

- Zur Versendung verschlüsselter Mails an Mitarbeiter eines EBCA Teilnehmers wird ihr öffentliches Zertifikat benötigt.
- Bereitstellung dieser kann über zentralen EBCA-Verzeichnisdienst erfolgen.
- Abruf der Zertifikate über Website und über LDAP möglich.
- Zum Schutz der Teilnehmer muss E-Mail-Adresse des Empfängers bekannt sein.

Übersicht, Anleitung und Link:
ebca.de/tools/zertifikate-finden/

Aufnahme in die Certificate Trust List

- Eine Aufnahme in die Certificate Trust List erfolgt für alle Wurzelzertifikate der EBCA-Teilnehmer.
- Dazu ist nur das Wurzelzertifikat zu übertragen (z.B. über Mail/ Verlinkung auf Website, etc.).
- Zur Gewährleistung der Integrität ist zusätzlich der Hashwert/ Fingerprint über ein zweites Medium zu übertragen.
- Die Teilnehmer teilen der EBCA Änderungen zu den hinterlegten Zertifikaten mit.

- Die CTL kann frei im Internet heruntergeladen werden.
- Mittels eines Online-Tools können Nutzer die Integrität selbst prüfen.

TeleTrusT EBCA
European Bridge Certificate Authority

Aufnahme in den Verzeichnisdienst

- Als EBCA-Teilnehmer kann man seine öffentlichen Zertifikate über den Verzeichnisdienst verfügbar machen.
- Nutzer müssen nur diesen einen Verzeichnisdienst einbinden, um alle EBCA-Teilnehmer zu erreichen.

- Voraussetzung:
  1. Der EBCA-Teilnehmer hat einen extern verfügbaren Verzeichnisdienst, der an den EBCA-Verzeichnisdienst angebunden werden kann.

  oder

  2. Der EBCA-Teilnehmer publiziert seine Zertifikate direkt im EBCA-Verzeichnisdienst

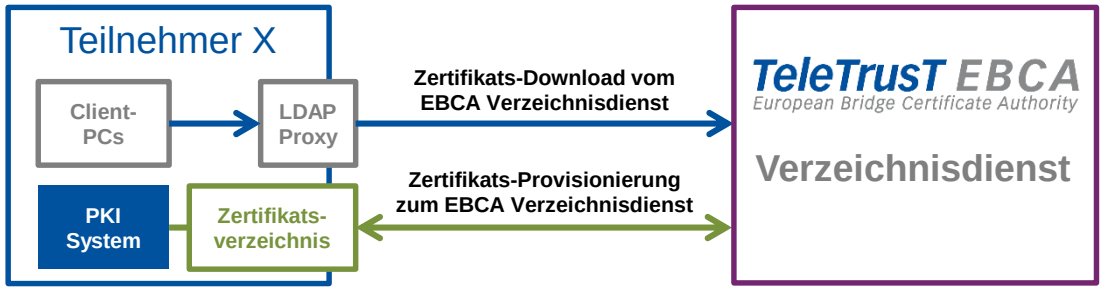
  oder

  3. Der EBCA-Teilnehmer publiziert seine Zertifikate in einem externen Zertifikatsspeicher.

TeleTrusT EBCA
European Bridge Certificate Authority

Szenarien: Bereitstellung der öffentlichen Zertifikate

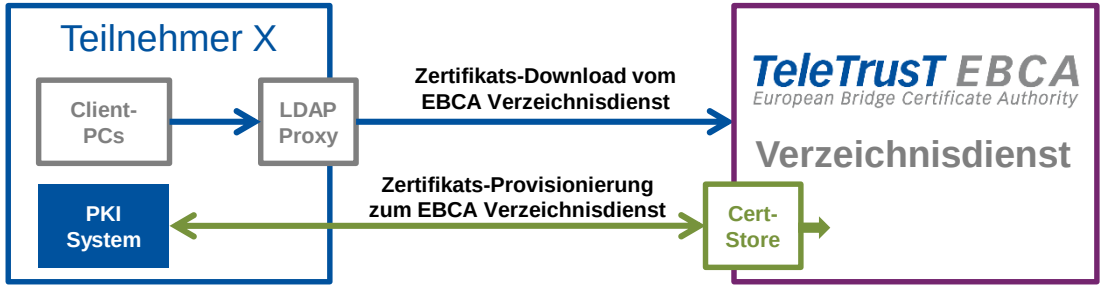
1. Eigener externer Verzeichnisdienst



- EBCA-Teilnehmer besitzt bereits einen Verzeichnisdienst, der extern zugänglich ist.
- Der externe Verzeichnisdienst wird über ein LDAP-Proxy an den EBCA-Verzeichnisdienst angebunden.

Keine zusätzlichen Kosten

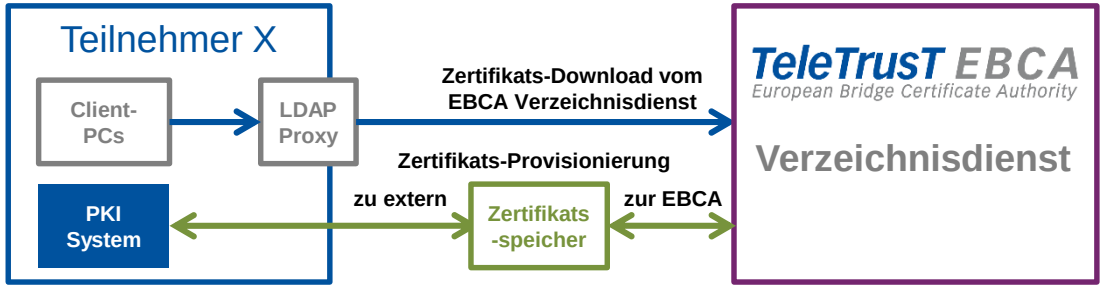
2. Publizierung direkt im EBCA-Verzeichnisdienst



- EBCA-Teilnehmer erwirbt Lizenzen für die Speicherung von Zertifikaten im EBCA-Verzeichnisdienst.
- Ein Zusatzvertrag mit Dienstleistungspartner ist notwendig.
- Es gelten Sonderkonditionen.

Zusätzliche Kosten – bitte erfragen

3. Publizierung über einen externen Zertifikatsspeicher

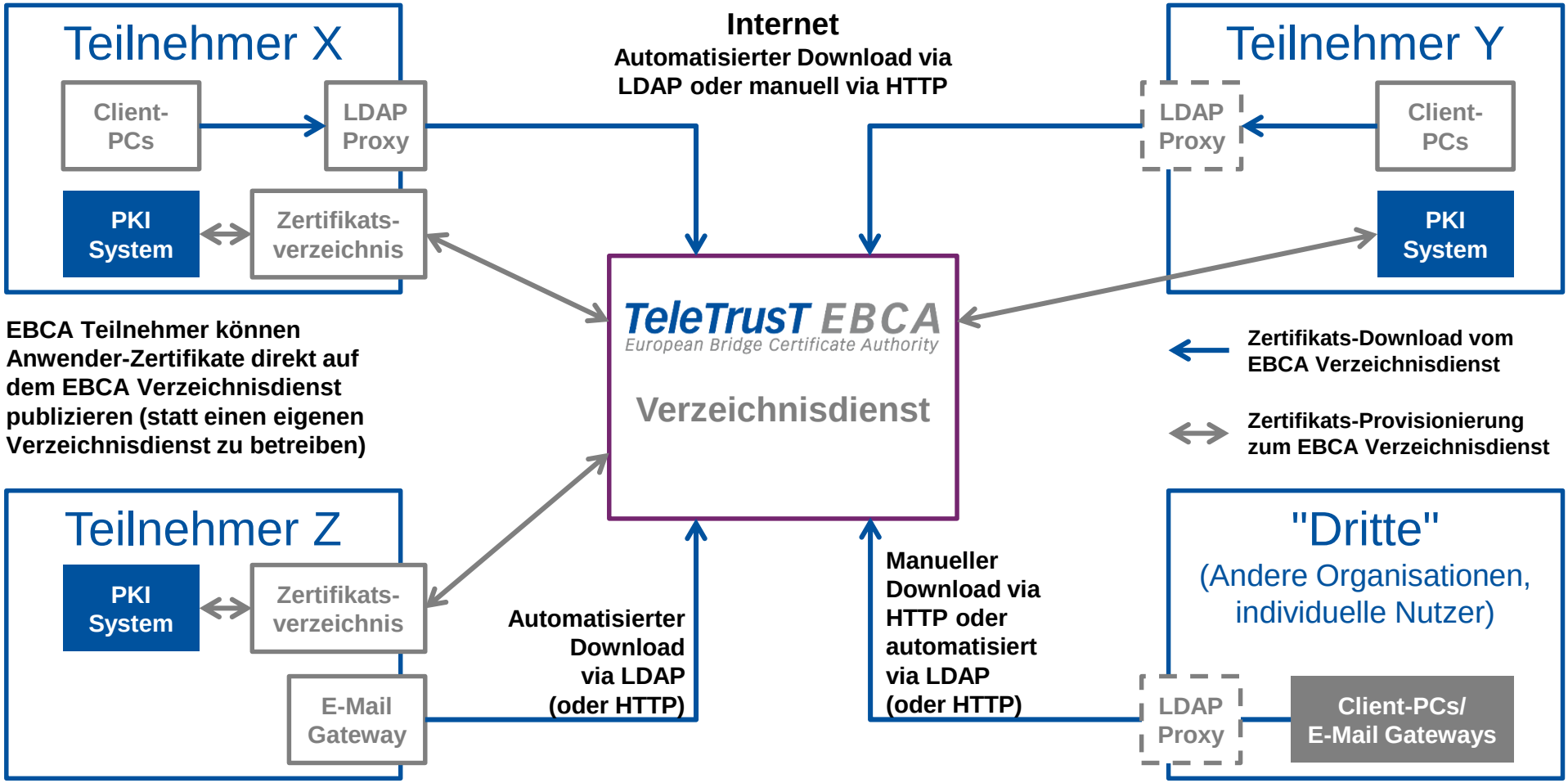


- EBCA-Teilnehmer kann auch jeden anderen Dienst für die Speicherung und Bereitstellung von Zertifikaten nutzen.
- Nur sinnvoll, wenn die Zertifikate über LDAP-Proxy abgerufen werden können.

Zusätzliche Kosten je nach Anbieter

Zusammenfassende EBCA Referenzarchitektur (E-Mail)

TeleTrusT EBCA
European Bridge Certificate Authority



TeleTrusT EBCA
European Bridge Certificate Authority

Warum Zertifikate über den EBCA-Verzeichnisdienst bereitstellen?

- EBCA repräsentiert einen PKI-Verbund, der eine festgelegte Mindestrichtlinie erfüllt
  - Nutzen einer sicheren PKI wird nach außen weitergegeben, wenn Zertifikate von extern gefunden werden können
  - Eine Anerkennung der PKI von außen kann erfolgen, da der Effekt, z.B. durch sicheren E-Mail-Austausch direkt von Dritten "erlebt" werden kann
  - Dritte erhalten immer aktuelle Zertifikate
  - EBCA-Teilnehmer muss nur auf den Verzeichnisdienst verweisen und nicht manuell Zertifikate nach außen weitergeben (z.B. durch wiederholtes Senden signierter Mails)
- Der Nutzen der EBCA steigt mit der Anzahl der Teilnehmer
  - EBCA-Verzeichnisdienst betrifft das im Besonderen:
    - bei allen EBCA-Teilnehmern eingebunden
    - vereinfacht Kommunikation unter EBCA-Teilnehmern
    - ermöglicht Dritten durch Einbindung des EBCA-Verzeichnisdienstes verschlüsselte Mails an alle EBCA-Teilnehmer zu senden

Fragen?
Kontaktieren Sie uns!

Ihr Ansprechpartner bei TeleTrusT – Bundesverband IT-Sicherheit e.V.

Marieke Petersohn
Projektkoordinatorin
Chausseestraße 17
10115 Berlin

marieke.petersohn@teletrust.de

Tel.: +49 30 4005 4308
Fax: +49 30 4005 4311
http://www.teletrust.de