

Abkehr vom hierarchischen Vertrauensmodell

Dipl. Wirtsch.-Ing. Arno Fiedler

Nimbus Technologieberatung GmbH



eGovernment und Sicherheit

Zunehmend werden Geschäftsprozesse automatisiert.
Elektronische Medien ersetzen Papier und persönliche Begegnungen.

Dadurch werden Geschäftsprozesse

- schneller
- kostengünstiger
- praktischer
- ortsunabhängig

Sind sie aber noch sicher?



Die EU-Dienstleistungsrichtlinie

- **Ziel:** Förderung des grenzüberschreitenden Handels mit Dienstleistungen
- **Zielerreichung** durch:
 - effektivere Gestaltung des Verwaltungsverfahrens (einheitlicher Ansprechpartner + elektronische Verfahrensabwicklung)
 - Straffung von Genehmigungsverfahren (Art. 5 Abs. 1 EU-DLR)
 - Abbau bürokratischer Hindernisse
 - Verbesserung der Kommunikation der Mitgliedstaaten
- **Fazit:**
 - E-Government wird zur Pflichtaufgabe. Die hohen Anforderungen der RL an die öffentliche Verwaltung sind bis Ende 2009 umzusetzen.

Grundlegende Sicherheitsanforderungen

Authentisierung

Partner können sich gegenseitig eindeutig identifizieren.

Verschlüsselung

Informationen und Daten sind vor dem Zugriff Dritter gesichert.

Integrität

Datenmanipulationen während und nach der Transaktion sind ausgeschlossen bzw. werden transparent.

Unabstreitbarkeit

Einzelne signierte Transaktionen können nicht geleugnet werden und sind somit rechtlich bindend.

Interoperabilität

Weltweit einheitliche Systeme, Schnittstellen, Regeln, Prozesse und Verträge.



Erforderliche Funktionalitäten im eGovernment:

Physical world

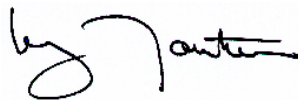


Authentication



Digital world

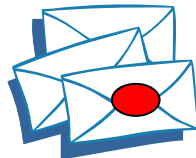
Digital Signatures and Digital Certificates



Non-repudiation



Electronic signatures



Integrity & Confidentiality



“Hash” and Encryption



Zertifikate: Welcher Public Key gehört zu wem?

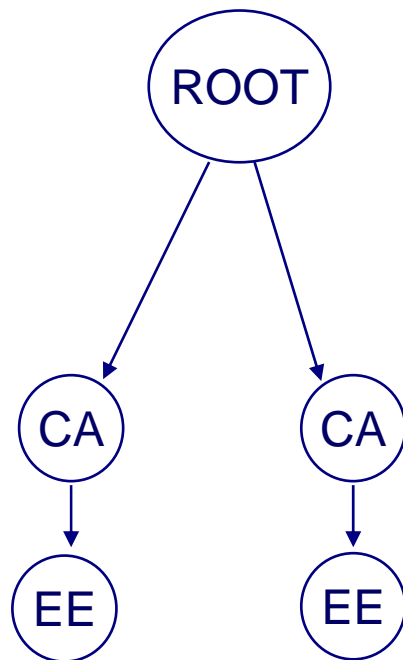
Ein Zertifikat ist eine „untrennbare“ Verbindung zwischen dem Public Key eines Benutzers und seinen Identitätsdaten

Die Daten des Zertifikats werden von einer höheren Instanz (Zertifizierungsstelle, CA) unterschrieben (signiert)

Ein Zertifikat dient zum sicheren Übermitteln der Identitätsdaten und des Public Keys eines Partners

Vertrauens-Modelle:

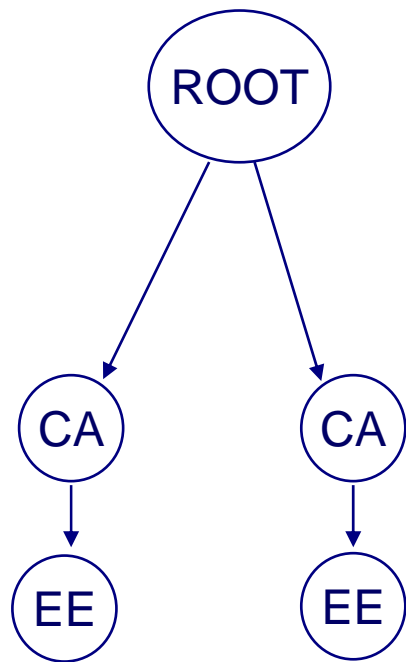
Bundesnetzagentur bei
akkreditierten Anbietern



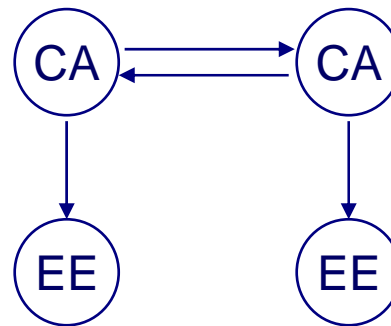
Hierarchisches System

Vertrauens-Modelle:

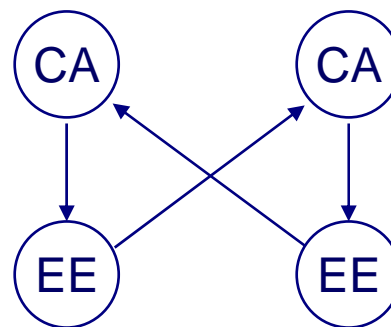
Bundesnetzagentur bei akkreditierten Anbietern



Hierarchisches System



Cross Certificate

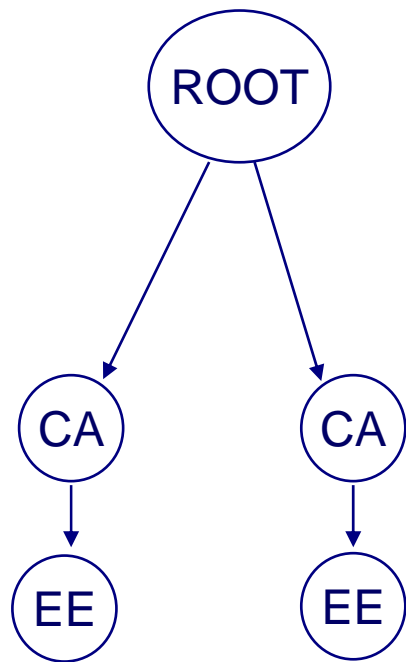


Cross Recognition

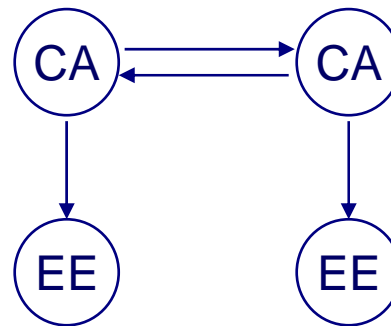


Vertrauens-Modelle:

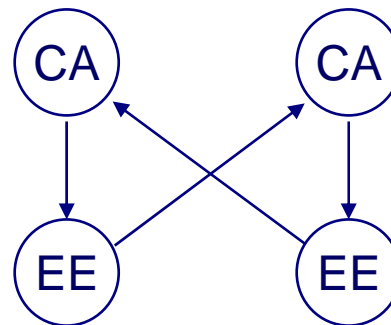
Bundesnetzagentur bei akkreditierten Anbietern



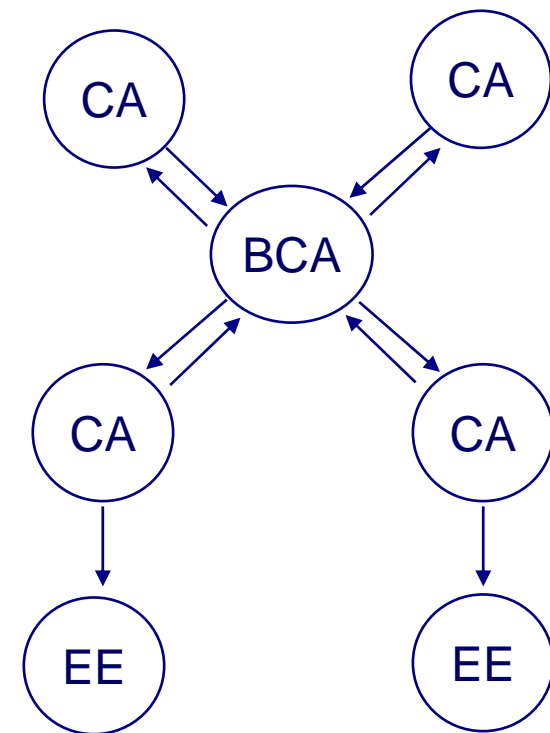
Hierarchisches System



Cross Certificate



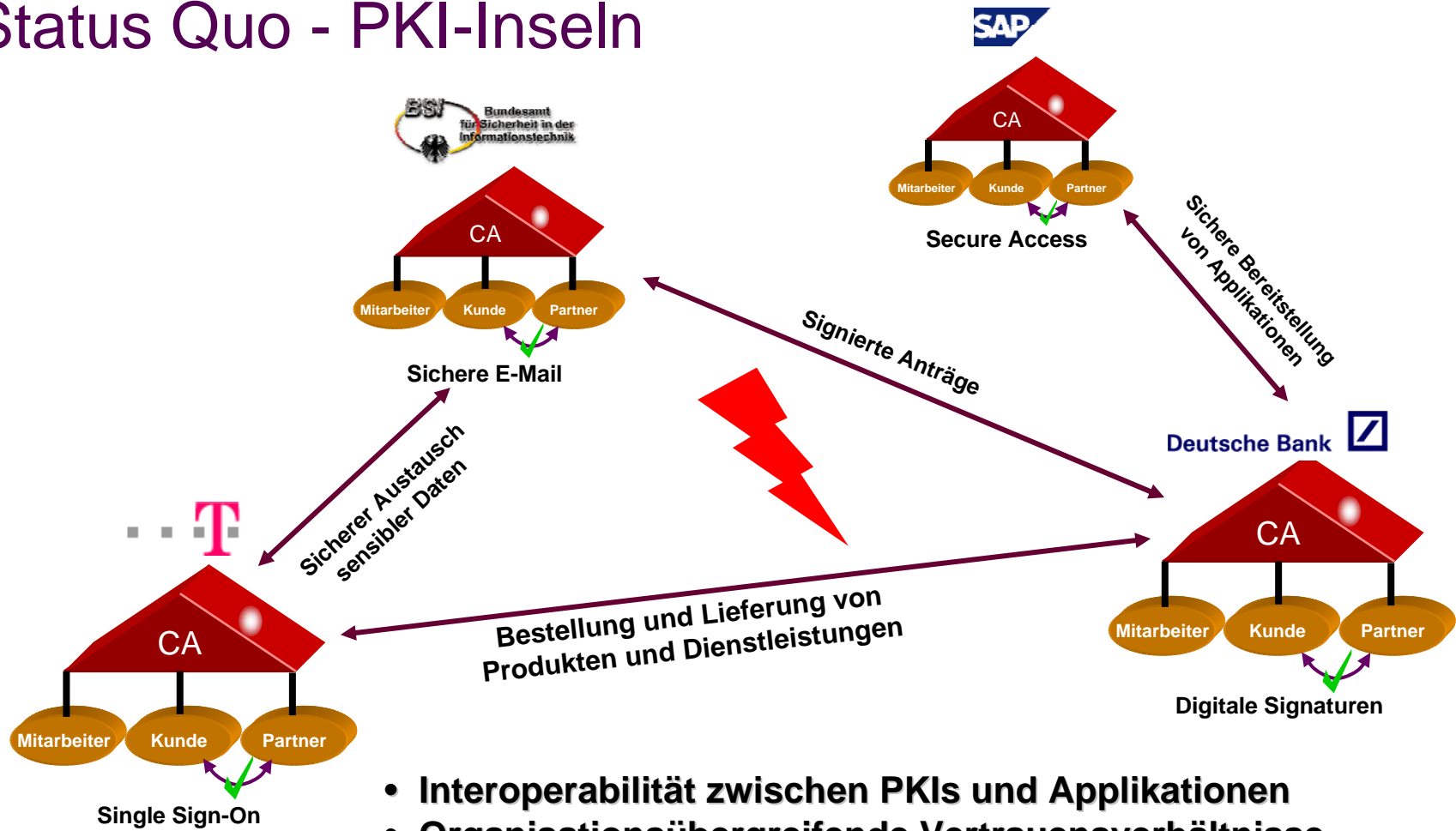
Cross Recognition



Bridge CA



Status Quo - PKI-Inseln

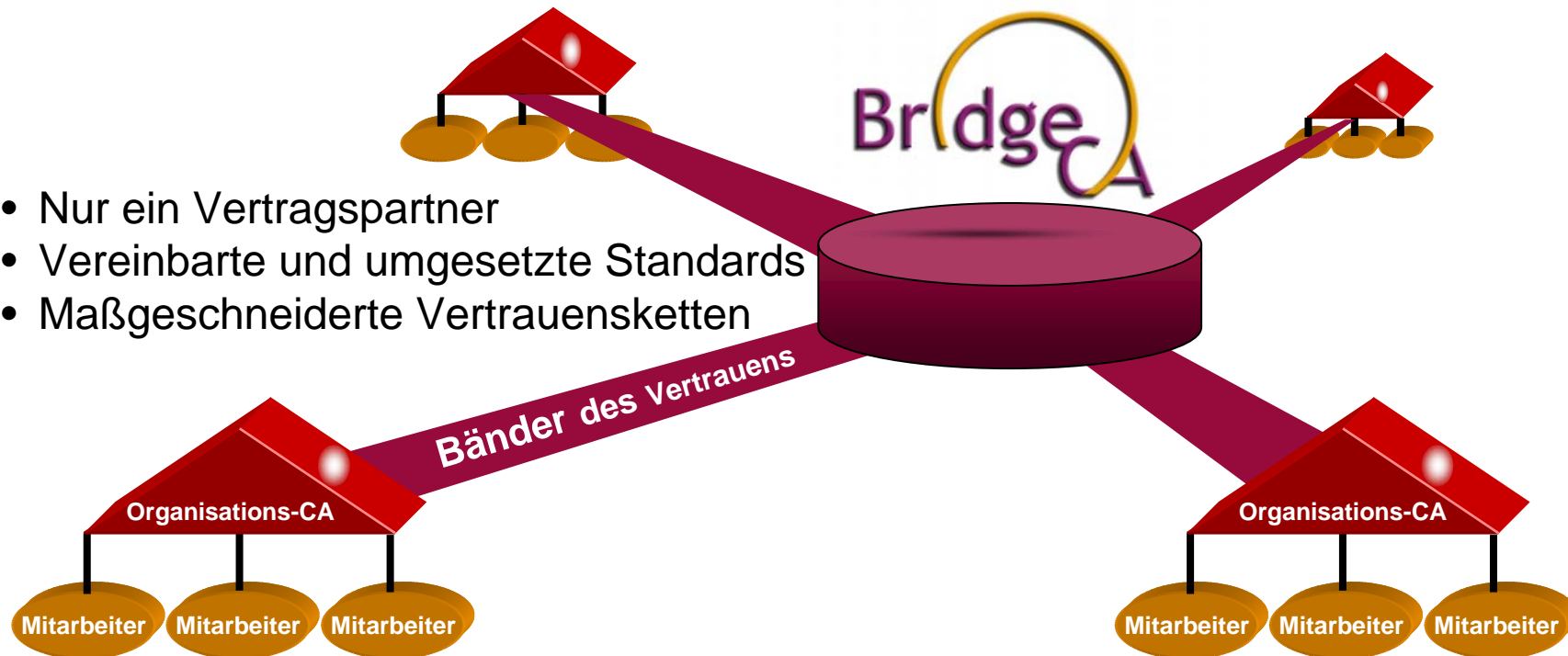


- Interoperabilität zwischen PKIs und Applikationen
- Organisationsübergreifende Vertrauensverhältnisse
- Integration in verschiedene Anwendungen



Die European Bridge-CA ist ein nicht-hierarchischer, 1:n-Netznoten für gleichrangige PKIs

- Nur ein Vertragspartner
- Vereinbarte und umgesetzte Standards
- Maßgeschneiderte Vertrauensketten



Die Ziele der European Bridge-CA sind...

- ... eine Brücke des Vertrauens zwischen verschiedenen PKIs weltweit zu etablieren.
- ... Standards für die organisationsübergreifende sichere Kommunikation zwischen Firmen & Behörden zu fixieren.
- ... ein gemeinsames Verständnis für den Einsatz von Zertifikaten in Geschäftsprozessen zu schaffen.
- ... Grundsätzen zu folgen: Anwendbarkeit, Flexibilität, Interoperabilität, Investitionsschutz.



Nutzen für die Teilnehmer

Investitionsschutz: Unternehmen, die schon eine PKI und ein S/MIME-fähiges Mailsystem haben, können jetzt nicht nur unternehmensintern sondern auch unternehmensübergreifend ohne zusätzliche Investitionen sicher kommunizieren. Zukünftig wird sich die European Bridge-CA nicht nur auf sichere E-Mail fokussieren.

Flexibilität: Sowohl software- als auch hardwarebasierte Zertifikate können innerhalb der European Bridge-CA genutzt werden.

Erfahrungsaustausch: Alle teilnehmenden Organisationen profitieren von den gemeinsam gewonnenen Erkenntnissen und Erfahrungen.

Netzwerkeffekt: Je mehr Organisationen sich an der European Bridge-CA beteiligen, desto größer wird der Nutzen und desto größer werden die Synergien beim Einsatzes einer PKI.

Innovationen: Standards für die organisationsübergreifende sichere Kommunikation.



TeleTrust Deutschland e.V. - Betreiber der European Bridge-CA

- Gründung 1989 mit dem Ziel, die Vertrauenswürdigkeit von Informations- und Kommunikationstechnik in einer offenen Systemumgebung zu fördern.
- Hauptaufgaben:
 - Einflussnahme auf die deutsche und europäische IT-Sicherheitspolitik und die nationale Gesetzgebung
 - Einflussnahme auf die Standardisierung im Sinne herstellerübergreifender Interoperabilität [z.B. Standards für Trustcenter ISIS/MTT, European Bridge-CA].
 - Förderung innovativer Technologien (z.B. biometrische Verfahren)
- Internationale Aktivitäten (gemeinsam mit EEMA und PKI-Forum; Ausrichten der ISSE-Konferenzen, etc.)



Aktuelle Teilnehmer & Interessenten



Deutsche Telekom



Deutsche Bank



Siemens



TC TrustCenter



Bundesamt für Sicherheit in der Informationstechnik



Sparkassen Informations Zentrum



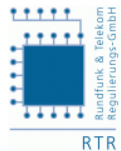
Allianz Gruppe



SAP



D-Trust



Regulierungsbehörde Österreich (RTR)



Allianz Group



BMW



Daimler Chrysler



Giesecke & Devrient



Utimaco



Secude



Cable & Wireless

Mit wem sprechen wir international:

IBM, Microsoft, Verisign, PKI-Forum Asia, Japanische Bridge-CA, etc.



EU-Richtlinie für Elektronische Signaturen

Kontinentaleuropäischer Ansatz



Prävention im Sinne umfassender Vorabprüfung von:

- Produkten
- technisch-administrativen, organisatorischen Abläufe der Zertifizierungstätigkeit
- Zuverlässigkeit und Fachkunde des eingesetzten Personals

- Entwicklungskosten (Evaluierung von Produkten und Sicherheitskonzepten)
- zu Beginn erhöhter Zeitaufwand



„garantiertes“
Sicherheitsniveau
„time-to-market“ kritisch

Angelsächsischer Ansatz



Sicherstellung eines ausreichenden Mindestniveaus über

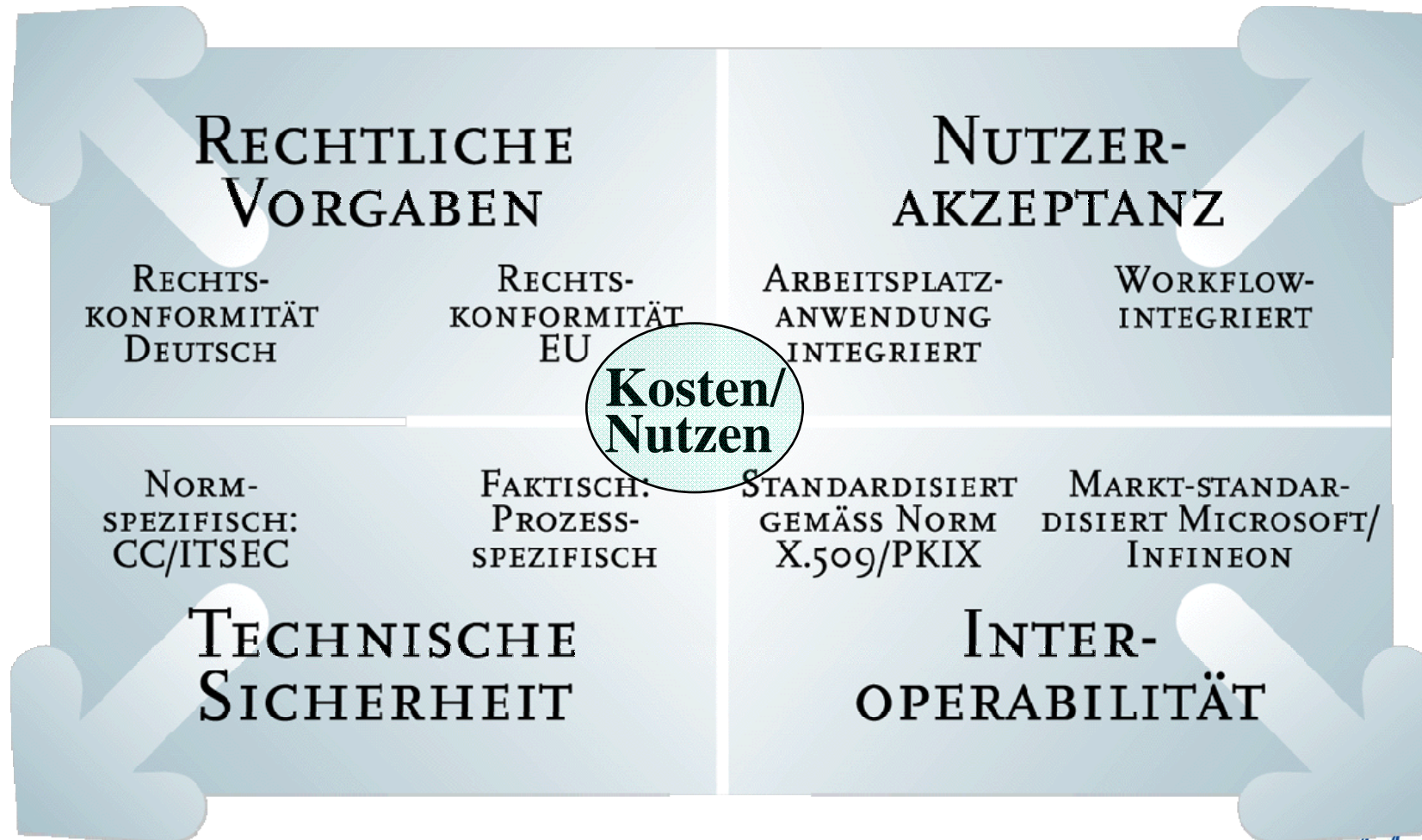
- **Wettbewerb** des Marktes
- **Haftung**

Haftung setzt Haftungsfähigkeit und Haftungswilligkeit voraus
Haftung setzt erkannte Schadensfälle voraus



Flexibel bezüglich Kundenbedarf

Das Spannungsfeld der Anforderungen



Zusammenfassung

- eGovernment benötigt PKI (elektronische Signaturen) als Fundament.
- Die Regulierungspraxis in Deutschland verhindert den bedarfsgerechten Einsatz.
- Vertrauens- und Kompetenznetzwerke bilden eine flexible Alternative, dieses setzt aber gegenseitige Anerkennung voraus.

Kontakte: www.bridge-ca.org [.de / .com]

Ansprechpartner und Mitglieder des Bridge-CA-Boards:

Helmut Reimer
TeleTrusT e.V.
email: helmut.reimer@teletrust.de

Bernhard Esslinger
Deutsche Bank AG
bernhard.esslinger@db.com

Detlef Dienst
Deutsche Telekom AG
detlef.dienst@telekom.de

Dieter Bartl
SIZ Informatikzentrum der
Sparkassenorganisation GmbH
dieter.bartl@siz.de

Joachim Rieß
DaimlerChrysler AG
joachim.riess@daimlerchrysler.com

Michael Hange
BSI - Bundesamt für Sicherheit
in der Informationstechnik
hange@bsi.bund.de

Bernd Kowalski
BSI - Bundesamt für Sicherheit
in der Informationstechnik
bernd.kowalski@bsi.bund.de

Hans-Joachim Bierschenk
Bitkom - Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.
h.j.bierschenk@bitkom.org

