



your connection to the network of trust.



**Mobile Commerce**  
Bernhard Esslinger, Deutsche Bank AG



## mCommerce und die verflixte Sicherheit

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

- ortsunabhängig
- schneller
- kostengünstiger
- praktischer

**Sind sie aber noch sicher?**



Der Automatisierung von Geschäftsprozessen schreitet unaufhaltsam voran. mBusiness ist in jedermanns Munde.

Zwar können mittels durchgängiger Nutzung elektronischer Medien enorme Einsparungspotentiale hinsichtlich Zeit, Kosten und Qualität realisiert werden, ungelöst bleibt vielfach das Problem der Sicherheit. Vertrauen ist aber die Grundlage jedes Geschäfts und so implementieren immer mehr Hersteller und Dienstleister leistungsfähige Sicherheitsinfrastrukturen.

Banken sind mit dieser Problematik bestens vertraut und haben eine Reihe von Lösungen entwickelt. Schon vor dem Internet haben sie Transaktionen über elektronische Netzwerke abgewickelt, ein Großteil des Bankgeschäfts ist digitalisiert und Bankgeschäfte sind von jeher vertraulich.



## Grundlegende Sicherheitsanforderungen

<div style="background-color: #f4a460; border-radius: 15px; padding: 10px; display: inline-block;">Authentifizierung</div>	▶	Partner können sich gegenseitig eindeutig identifizieren
<div style="background-color: #f4a460; border-radius: 15px; padding: 10px; display: inline-block;">Verschlüsselung</div>	▶	Die Informationen und Daten bleiben vor dem Zugriff Dritter verschlossen
<div style="background-color: #f4a460; border-radius: 15px; padding: 10px; display: inline-block;">Integrität</div>	▶	Datenmanipulation während und nach der Transaktion sind ausgeschlossen bzw. werden transparent
<div style="background-color: #f4a460; border-radius: 15px; padding: 10px; display: inline-block;">Unabstreitbarkeit</div>	▶	Einzelne signierte Transaktion sind unabstreitbar und somit rechtlich bindend
<div style="background-color: #f4a460; border-radius: 15px; padding: 10px; display: inline-block;">Interoperabilität</div>	▶	Weltweit einheitliche Systeme, Schnittstellen, Regeln, Prozesse und Verträge



Bridge-CA Initiative, Mai 2001, Seite 3

Jedes Unternehmen, das via Web Geschäfte macht oder Prozesse steuert, schickt sensitive Informationen über das globale Netz. Sensitive Daten, die im Unternehmen oder zwischen Partnern versandt werden, müssen für Dritte unveränderbar und nur für Absender und Empfänger lesbar sein. Wer an einem Online-Geschäft teilnehmen will, muss sich zunächst eindeutig identifizieren. Online-Geschäfte sollten schließlich juristisch bestehen können.

An die Stelle von anwendungsbezogenen Identifikationsverfahren (Benutzerkennung/Passwort) ist es heute gängige Praxis dem Nutzer einen elektronischen Ausweis auszuhändigen. Mit diesem Ausweis kann er sich bei verschiedenen Anbietern und Marktplätzen ausweisen und erteilte Aufträge digital signieren. Mit der digitalen Signatur entfällt der mit der handschriftlichen Unterschrift verbundene Medienbruch. E-Business wird damit einfacher und sicherer.

Aufgrund der applikations- und systemübergreifenden Nutzung der skizzierten Ausweise entsteht die Notwendigkeit umfangreicher Interoperabilität.

Elektronische Ausweise (Zertifikate und digitale Signaturen) basieren auf der Public-Key-Technologie.

Bridge-CA your connection to the network of trust

## Status Quo - PKI-Inseln

The diagram illustrates three isolated PKI islands. Each island consists of a CA (Certificate Authority) at the top, which is connected to three nodes: Mitarbeiter (Employee), Kunde (Customer), and Partner. The islands are not connected to each other, representing a fragmented trust landscape. Arrows indicate internal communication and transactions within each island, but no external connections exist between them.

- Sichere Kommunikation** (Secure Communication) - Internal to each island.
- Sicherer Austausch sensibler Daten** (Secure Exchange of Sensitive Data) - Internal to each island.
- Digitale Signaturen** (Digital Signatures) - Internal to each island.
- Bestellung von Produkten** (Ordering of Products) - Internal to each island.
- Bestellung und Lieferung von Produkten und Dienstleistungen** (Ordering and Delivery of Products and Services) - Internal to each island.
- Signierte Anträge** (Signed Requests) - Internal to each island.

**• Interoperabilität zwischen PKIs und Applikationen**  
**• Organisationsübergreifende Vertrauensverhältnisse**

BRUNNEN

Bridge-CA Initiative, Mai 2001, Seite 4

Viele Firmen und Behörden haben eine eigene Public-Key-Infrastruktur aufgebaut und nutzen Public-Key-Zertifikate, so wie z.B. die Deutsche Bank ihre Software Zertifikate für den internen Austausch von verschlüsselten und signierten E-Mails nutzt.

Nun möchten diese Organisationen ihre Zertifikate auch für die externe Kommunikation verwenden. Bisher wurden dazu Zertifikate für die externen Partner ausgestellt. Mit der zunehmenden Zahl von Firmen, die eine Public-Key-Infrastruktur aufbauen, tritt immer häufiger der bald zur Regel werdende Fall ein, dass die Partnerfirma bereits selbst über eine Public-Key-Infrastruktur verfügt und der Kommunikationspartner ein Zertifikat hat, das aus einer anderen Public-Key-Infrastruktur stammt. Diese begrüßenswerte Situation wirft für die Entwickler und Betreiber von Public-Key-Infrastrukturen die Frage auf, wie unterschiedliche Public-Key-Infrastrukturen miteinander verknüpft werden können, damit die Anwender nicht an Grenzen stoßen. Die Bridge-CA ist die Antwort darauf.

Die Bridge-CA-Initiative wurde gegründet, weil mangelndes Vertrauen und mangelnde Interoperabilität Haupthindernisse des eBusiness sind und weil die meisten bisherigen Versuche, PKIs zu etablieren, nur zu Insellösungen führten.

Die Bridge-CA bildet die Brücke zwischen diesen „Vertrauens-Inseln“.

## Herausforderungen des mCommerce

- Geringer Speicherplatz der Chips verhindern momentan den Einsatz von gewünschten Standardformaten (PKCS#7, X.509v3 Zertifikate)
- Begrenzte Prozessorleistung erschwert den Einsatz von Standardalgorithmen (RSA, SHA-1)
- Mangelnde übergreifende Standardisierung erschwert die Interoperabilität zwischen verschiedenen Systemen

Technische Herausforderung

Organisatorische Herausforderung



## Die Mission der europäischen Bridge-CA ist es...

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



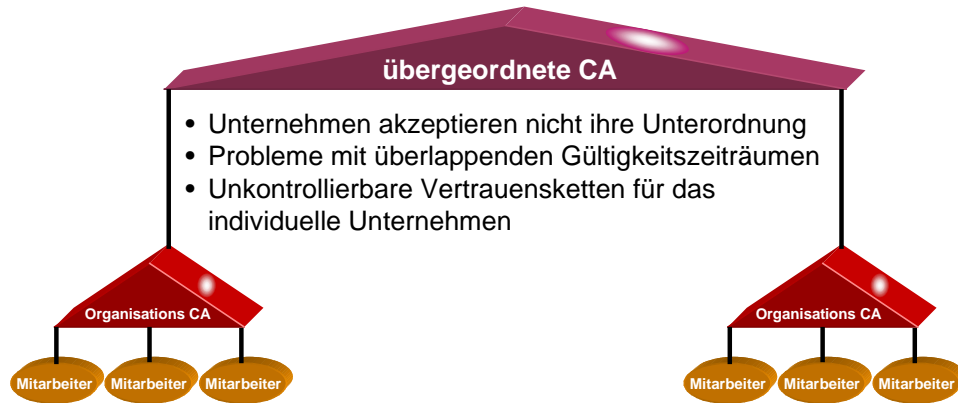
Die Bridge-CA ist das Ergebnis einer Initiative der Deutschen Bank und der Deutschen Telekom, bestehende Public-Key-Infrastrukturen zu verknüpfen und so für die sichere Kommunikation zwischen Firmen und Behörden zu nutzen.

Der Bridge-CA-Initiative hatten sich Ende März schon 20 Firmen und Institutionen angeschlossen, u.a. auch die Bundes-PCA des BSI.

Offen werden in dieser Interessengemeinschaft Erfahrungen im Aufbau und im Betrieb einer PKI ausgetauscht. Gemeinsam einigt man sich auf Standards und löst offene Fragen, die eine Interoperabilität sicherstellen.

Ihren Erfolg verdankt sie der Kombination aus starker Sicherheit, Investitionsschutz, Flexibilität und hohem Pragmatismus.

## Die Bridge-CA ist keine ...



Die folgenden 3 Folien zeigen 3 Arten, wie man technisch diese Vertrauensbrücke schaffen kann (Neue Top-Root, n:n-Cross-Zertifizierung, 1:n-Stern). Die ersten 2 Arten wurden verworfen, die dritte Alternative wurde in der Bridge-CA realisiert.

Eine typische Public-Key-Infrastruktur besteht aus einer Stelle für die Bearbeitung von Zertifikatsanträgen, der Registration Authority, einer Stelle, die Zertifikate erstellt, der Certification Authority, einem Verzeichnisdienst für die Veröffentlichung von Zertifikaten und Sperrlisten sowie organisatorischen Regeln, dem Certificate LifeCycle. Jeder Public-Key-Infrastruktur liegt ein Vertrauensmodell zugrunde. Das Vertrauensmodell im engeren Sinne ist die Zertifikathierarchie. Dadurch, dass Zertifikate unterschrieben sind und zur Überprüfung dieser Unterschrift wieder Zertifikate herangezogen werden, wird bei der Überprüfung eine Zertifikathierarchie durchlaufen, bis ein Zertifikat angetroffen wird, dem das Vertrauen ausgesprochen wurde und dessen Unterschrift deshalb nicht weiter überprüft zu werden braucht.

Die Zertifikathierarchie legt fest, wie Zertifikaten „implizit“ das Vertrauen ausgesprochen wird. Mit implizit ist gemeint, dass ein Zertifikatspfad existiert zu einem Zertifikat, dem explizit das Vertrauen ausgesprochen wurde. Man könnte auch indirekt und direkt sagen. Zum Beispiel könnte die Bridge-CA Hierarchie so aussehen, dass die Bridge-CA zunächst ein selbstsigniertes Zertifikat ausstellt und anschließend Zertifikate für die Certification Authorities der teilnehmenden Public-Key-Infrastrukturen. Alle, die dem Zertifikat der Bridge-CA das Vertrauen aussprechen, sprechen damit implizit den von der Bridge-CA ausgestellten Zertifikaten das Vertrauen aus, und damit den Zertifikaten der anderen Public-Key-Infrastrukturen. Diese Architektur hat zur Konsequenz, dass allen Public-Key-Infrastrukturen gleichzeitig vertraut wird oder keiner. Da dieses Modell eine hierarchische Unterordnung bedeutet, die von vielen Organisationen nicht akzeptiert wird, wurde die Bridge-CA **nicht** hierarchisch aufgebaut.

Bridge-CA your connection to the network of trust

## Die Bridge-CA basiert nicht auf n:n Cross-Zertifizierung...

- Komplexe und unökonomische Administration
- Fehlende gemeinsame Standards
- Multiple Vertragsverhandlungen sowie abweichende Verträge und Vereinbarungen

Organisations CA  
Mitarbeiter  
Mitarbeiter  
Mitarbeiter

Bänder des Vertrauens

Organisations CA  
Mitarbeiter  
Mitarbeiter  
Mitarbeiter

Bridge-CA Initiative, Mai 2001, Seite 8

Bei einer n:n Cross-Zertifizierung muß jeder mit jedem die Vertrauenswürdigkeit aushandeln, was bei einer grossen Anzahl von n Teilnehmer-PKIs zu komplex wird.

Es gibt drei Verfahren, die CA-Zertifikate einer fremden PKI den Endbenutzern zur Verfügung zu stellen:

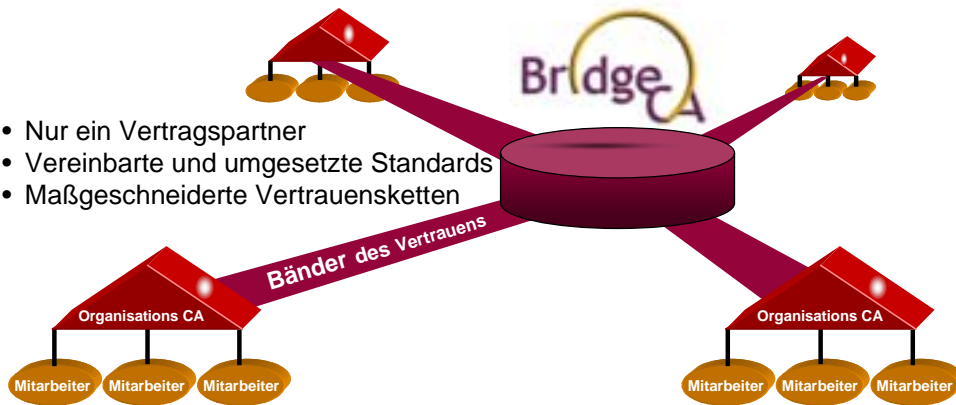
- Die Nutzer importieren die Certification Authority Zertifikate in ihren E-Mail Client und setzen sie auf vertrauenswürdig. Bei dieser Architektur kann für jeden Nutzer festgelegt werden, welcher Public-Key-Infrastruktur er vertraut.
- Die Netzwerk-Administratoren verteilen die Zertifikate via Netzwerk- und Systemmanagement-Software auf jeden Client.
- Die Administratoren stellen die entsprechenden CA-Zertifikate in ein eigenes Directory, auf das die Clients zugreifen, wenn das CA-Zertifikat nicht das eigene ist.

Wie aufwendig der Verteilprozess der CA-Zertifikate ist und ob die einzelnen Nutzer involviert sind, hängt neben der Architektur davon ab, was die jeweiligen E-Mail Clients technisch unterstützen.

Es ist nach Möglichkeit zu vermeiden, es einem Nutzer zu überlassen, CA-Zertifikate oder auch nur Nutzer-Zertifikate auf vertrauenswürdig zu setzen, da dabei Fehler passieren können, die das Vertrauensmodell kompromittieren. Stattdessen sollten die Betreiber der Public-Key-Infrastruktur das Vertrauensmodell definieren. Dafür gibt es Kreuzzertifikate (Cross certificates), die innerhalb der jeweiligen Teilnehmer-PKI eingesetzt werden können.

## Die Bridge-CA ist ein nicht-hierarchischer 1:n Netz-knoten für gleichrangige PKIs

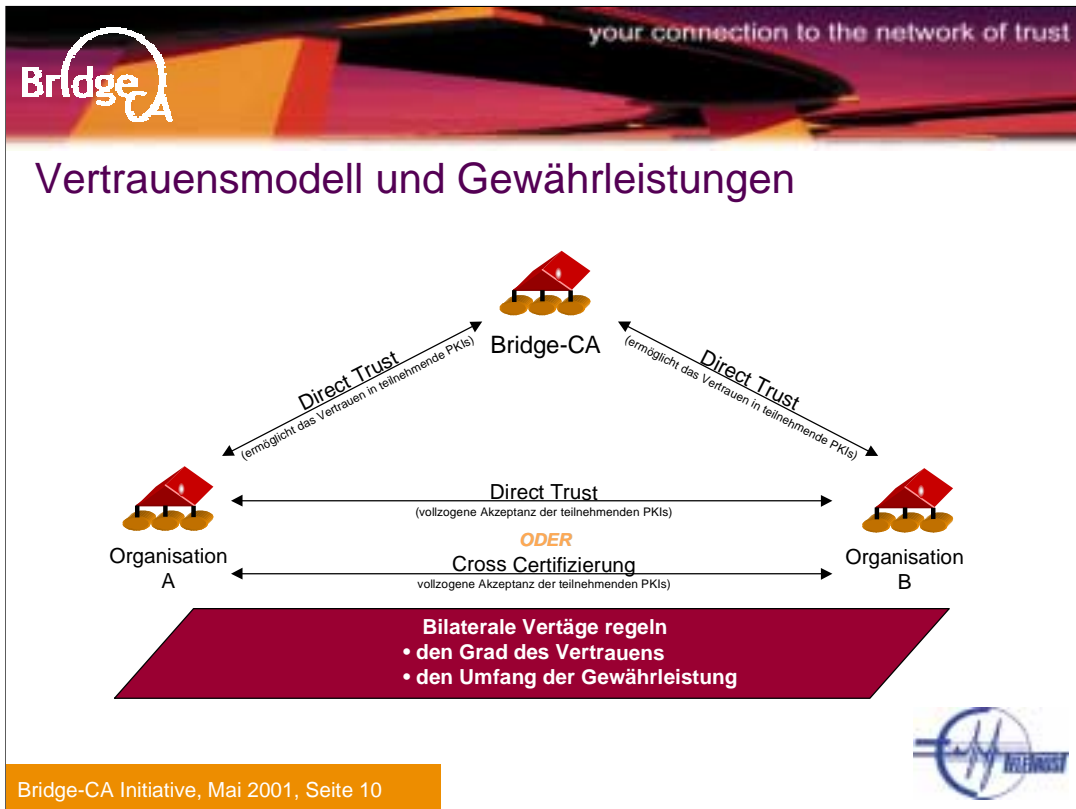
- Nur ein Vertragspartner
- Vereinbarte und umgesetzte Standards
- Maßgeschneiderte Vertrauensketten



Die Bridge-CA stellt Administrator-Zertifikate aus, mit denen eine Liste unterschrieben wird, in der die CA-Zertifikate der Teilnehmer-PKIs aufgeführt sind, die für vertrauenswürdig befunden wurden. Die Liste wird an die Verwalter der teilnehmenden Public-Key-Infrastrukturen verteilt, die dann nochmal entscheiden können, welchen von den aufgeführten Public-Key-Infrastrukturen sie das Vertrauen aussprechen.

Auf der Ebene der Bridge-CA selbst wurde bewusst keine 1:n Cross-Zertifizierung realisiert.

Innerhalb der PKI der Teilnehmer ist die beste Lösung der in den Notizen der vorherigen Folie beschriebene Fall c) - eine hausinterne uni-laterale Cross-Zertifizierung für die fremden CA-Zertifikate, die man in ein eigenes Directory stellt.



Die Signatur der Bridge-CA bestätigt die folgenden Sachverhalte:

- Das CA-Zertifikat ist tatsächlich das für das es sich ausgibt.
- Die signierte CA ist interoperabel.
- Die signierte CA verhält sich konform zu definierten Standards.

Zur Validierung der Bridge-CA-Signatur ist es notwendig das Bridge-CA-Zertifikat mittels ‚direct trust‘ in der überprüfenden Applikation selbst als vertrauenswürdig zu deklarieren.

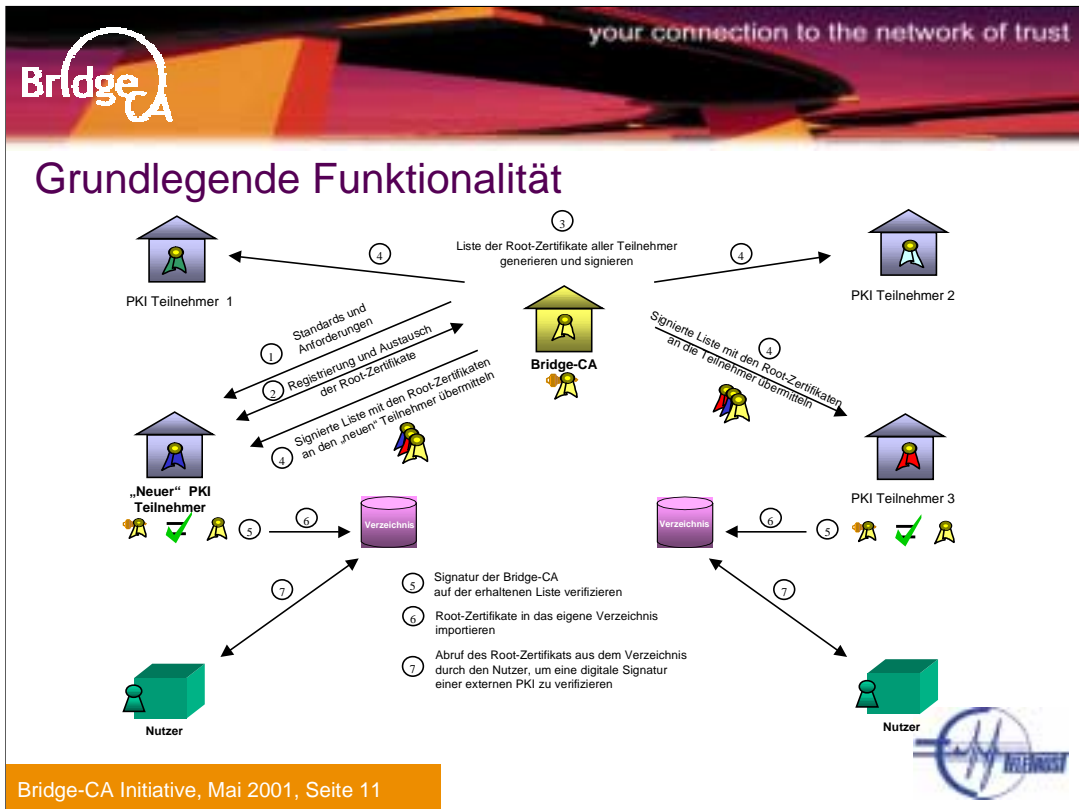
Selbstverständlich muss hierbei das Zertifikat auf eine sichere Art und Weise übermittelt worden sein und die Echtheit durch Überprüfung des Fingerprints sichergestellt worden sein.

Erst auf diese Grundlage hin kann die Entscheidung gefällt werden ob und in welchem Umfang einzelnen CAs vertraut wird. Die technische Zuordnung von Vertrauen kann durch zwei Verfahren erfolgen.

Für eine überschaubare Anzahl von interagierenden PKIs/CAs, beteiligter User und betroffenen Applikationen kann das bereits skizzierte manuelle Verfahren analog zur Bridge-CA angewandt werden. Schnell aber wächst der administrative Aufwand für die dezentrale Pflege und Verwaltung der CA-Zertifikate an.

Alternativ kann auch eine Cross-Zertifizierung erfolgen. Hierbei stellt die Organisation A der Organisation B ein Zertifikat aus. Dieses wird in das Verzeichnis der Organisation A eingestellt und steht als vertrauenswürdiges Zertifikat allen Clients zur Verfügung. Die Administration erfolgt zentral.

Grad des Vertrauens und Umfang der Gewährleistung bezüglich der Zertifikatsnutzung sind ausschliesslich zwischen der Organisation A und B vertraglich zu regeln. Die Bridge-CA übernimmt hier keine Verantwortung.



Nachdem eine Organisation die Aufnahme beantragt, erhält sie Informationen zur Vorgehensweise für den technischen Interoperabilitätstest. Für die Durchführung dieser Tests steht den Interessenten einer der Bridge-CA Mitarbeiter persönlich zur Verfügung. In den meisten Fällen sind nur kleine Anpassungen, z.B. Konfiguration der Mailer oder Einsatz eines Plugins erforderlich, die sich ohne großen Aufwand in kurzer Zeit durchführen lassen.

Abschließend wird ein Teilnahmevertrag unterschrieben und das CA-Zertifikat mit der Bridge-CA ausgetauscht.

## Die Bridge-CA...

- ... ist eine gemeinnützige Initiative, offen für alle interessierten Organisationen.
- ... ist die Brücke zwischen bestehenden und neuen Sicherheits-Insel-lösungen von Unternehmen und der öffentlichen Verwaltung weltweit.
- ... ist die Vernetzung bestehender Infrastrukturen bereits etablierter Datennetze. Pragmatische Ergänzungen und Adaptionen dieses Netzwerks werden mit minimalem Aufwand gemeinsam verabschiedet und getragen.
- ... ist eine Interessengemeinschaft, die den Austausch von Erfahrungen und Wissen bezüglich der Konzeption und der Implementierung einer PKI zwischen ihren Teilnehmern fördert.



Die Bridge-CA steht europaweit allen Firmen und Behörden offen. Die Industrieverbände TeleTrust und BITKOM unterstützen die Bridge-CA. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beteiligt sich stellvertretend für Bundesministerien und Bundesbehörden. Die vom BSI aufgebaute Bundes-PCA (Sphinx-CA) ist in die Bridge-CA eingebunden. Erfahrungen über die Interoperabilität von S/MIME fähigen E-Mail Clients aus dem BSI-Projekt "SPHINX" flossen in den Aufbau der Bridge-CA ebenso ein wie die Erfahrungen der amerikanischen Federal-B-CA.

Ein neutrales Gremium entscheidet über die Anbindung einer Teilnehmer-Public-Key-Infrastruktur an die Bridge-CA. Sowohl Hardware- als auch Software-Zertifikate sind zulässig. Langfristig wird ein Übergang auf qualifizierte Zertifikate nach dem neuen Signaturgesetz oder auf Chipkarten-Einsatz angestrebt.

Das Gremium vertritt pragmatisch die Interessen der Mitglieder und Anwender.



## 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.

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

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

**Netzwerkeffekt:** Je mehr Organisationen sich an der Initiative beteiligen, desto größer wird der Nutzen und desto größer werden die Synergien des Einsatzes einer PKI.

**Innovationen:** Standards für die organisationsübergreifende sichere Kommunikation.



Die Bridge-CA schafft kalkulierbare Rahmenbedingungen. Der branchenübergreifende Ansatz steht allen Firmen offen, ist standardisiert und global ausgerichtet. Die Bridge-CA verbindet Unternehmen, indem sie die Zertifikate verschiedener PKIs einbindet. Neben dem ganz praktischen Nutzen der schnellen Kommunikation bekommen Teilnehmer zusätzlich die Möglichkeit, ihre Partner- oder Kundenbindung durch diese Vertrauensmassnahme zu stärken.

Die Teilnahme erfolgt schnell, einfach und flexibel. Weder der Austausch einzelner Benutzerzertifikate noch eine Über-Kreuz-Zertifizierung sind notwendig. S/MIME-fähige Systeme können sofort eingebunden werden.

Als Brücke zwischen Sicherheitsinfrastrukturen erweitert die Bridge-CA deren Einsatzbereich. Mit der Bridge-CA stellt sich ein Netzwerkeffekt ein: Je mehr Public-Key-Infrastrukturen über die Bridge-CA verknüpft sind, desto höher ist der Nutzen für die angeschlossenen Nutzer, desto attraktiver ist es, die eigene Public-Key-Infrastruktur anzuschließen und desto vorteilhafter ist es, überhaupt eine Public-Key-Struktur zu haben.

Als Organisation ermöglicht die Bridge-CA den Austausch von Erfahrungen beim Aufbau und Betrieb von Public-Key-Infrastrukturen, auch für solche Unternehmen und Institutionen, die noch keine PKI haben. Die Bridge-CA gibt die ganz konkreten Erfahrungen vieler Unternehmen weiter und helfen so, Fehler zu vermeiden und Investitionen zu schützen.

## Aktuelle Teilnehmer & Interessenten



Deutsche Telekom



Lufthansa



Deutsche Bank



Bosch



Siemens



IBM



Giesecke & Devrient



BASF



TC TrustCenter



BMW



Sparkassen Informations Zentrum



Bundesamt für Sicherheit in der Informationstechnik



Daimler Chrysler



Die Bridge-CA wurde von der Deutschen Bank und der Deutschen Telekom ins Leben gerufen. Gesteuert wird diese Kooperation durch ein internationales Board mit Vertretern aus Wirtschaft, Verwaltung und Wissenschaft. Neben den beiden Gründern sind DaimlerChrysler, TeleTrust, die Sparkassenorganisation (SIZ) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) Mitglied im Board. Das BSI beteiligt sich stellvertretend für Bundesministerien und Bundesbehörden. Industrieverbände wie TeleTrust und BITKOM unterstützen diese Initiative. Die Ausdehnung auf weitere Organisationen wird aktiv betrieben und schreitet zügig voran. Erfolgreiche Interoperabilitätstests sind bereits mit internationalen Unternehmen durchgeführt worden. Interesse bekundeten viele weitere Großorganisationen.

## Elemente der E-Mail Interoperabilität einiger Teilnehmer

Organisation	E-Mail Client	S/MIME Lösungen (Unveränderter E-Mail Client oder mit Plug-in)	CA-Produkte
BMW AG	Netscape Messenger 4.7.2	Unverändert	TC TrustCenter
Deutsche Bank AG	Lotus Notes 4.5/4.6	Lotus MailProtect 1.3.4 a	TC TrustCenter (Produktion) SECUDE CA (Test, Development)
Deutsche Telekom AG	MS Outlook 98	SECUDE AuthentEmail (customized)	Cybertrust CA
Dresdner Bank AG	MS Outlook 2000	Unverändert	Netscape/Baltimore
Secartis AG	MS Outlook 98	G&D TrustedMail	GDDTrust CA
Siemens AG	MS Outlook 98	SSE TrustedMime	Trusted CA
TC Trust Center GmbH	Netscape Messenger 4.7.6	Unverändert	TC TrustCenter

**Interoperabilität mittels des Austausches signierter und signiert/verschlüsselter S/MIME-Mails demonstriert.**



Die Matrix ist ein Ausschnitt aus den Interoperabilitätstests einigen der Teilnehmer Ende Februar 2001. Sie zeigt, daß selbst die Mailingsysteme verschiedener Hersteller (Lotus Notes und Microsoft Outlook) mittels S/MIME-fähigen Plugins (Lotus MailProtect und SECUDE AuthentEmail) 100%-ig kompatibel verbunden werden können.

Nicht alle Client-Anwendungsprogramme sind derzeit auf die technisch notwendige Verzweigung im Zertifikatspfad vorbereitet, obgleich das konzeptionell nichts Neues ist. Der aktuelle Entwicklungsstand der verwendeten Software wird bei der Bridge-CA berücksichtigt. Mit Hilfe von Plug-ins (z.B. Lotus MailProtect und SECUDE AuthentEmail) sind aber alle Standard-Mailer dazu in der Lage.

In einer ersten Stufe wird eine sternförmig eingebundene Bridge-CA aufgesetzt, die zunächst nur Administrator-Zertifikate für den Betreiber ausstellt. An die Bridge-CA Teilnehmer wird eine Liste verteilt mit den Certification Authority Zertifikaten der Teilnehmer, die vom Bridge-CA Gremium genehmigt wurden, unterschrieben mit dem Bridge-CA Administrator-Zertifikat. Die Betreiber der Firmen- und Behörden-Public-Key-Infrastrukturen entscheiden, welchen Public-Key-Infrastrukturen sie das Vertrauen aussprechen und wie sie es tun, per uni-lateralem Kreuzzertifikat, oder über die Verteilung der Zertifikate an die Nutzer, und können so ihren Bedürfnissen und ihren technischen Möglichkeiten Rechnung tragen.

In der Zukunft ist es vorstellbar, daß die Bridge-CA die CA-Zertifikate der Teilnehmer gleich zertifiziert. Die genaue Architektur dazu wird festgelegt, wenn Erfahrungen aus der ersten Stufe vorliegen.

## Anwendungsbeispiel: Bankbürgschaften der Deutschen Bank ‚just in time‘

Im täglichen Geschäftsverkehr sind Bankbürgschaften eine gängige Form zu erbringende Leistungen (Zahlungen, Lieferungen oder sonstige Ansprüche) abzusichern.

PKI-Technologie ermöglicht die sichere elektronische Bereitstellung relevanter Geschäftsdaten zur Bürgschaftsprüfung als auch die digitale Signatur von Bürgschaftsanträgen und –erklärungen. Unberechtigte Dritte können diese Daten nicht einsehen oder manipulieren. Der Prozess kann vollständig automatisiert werden, die Bürgschaftszusage kann binnen kürzester Zeit erteilt werden.

Durch den Beitritt zur Bridge-CA ist die Anzahl potentieller Kunden für den automatisierten Bürgschaftsantrag um ein Vielfaches gestiegen. Die Bank ist nicht mehr gezwungen für jeden Kunden ein neues Zertifikat auszustellen, vielmehr kann der Kunde sein Zertifikat jetzt für eine weitere Anwendung nutzen.



### **Problemstellung:**

Im täglichen Geschäftsverkehr sind Bankbürgschaften eine gängige Form zu erbringende Leistungen (Zahlungen, Lieferungen oder sonstige Ansprüche) abzusichern. Schnelligkeit und Flexibilität sind bei der Bürgschaftsvereinbarung essentiell, um das zugrundeliegende Kundengeschäft nicht unnötig zu verzögern. Die papiergebundene Übermittlung sensibler Kundendaten und eindeutiger Willenserklärungen in Form von Unterschriften erschwerte bisher die Prozeßautomatisation und damit die zügige Erteilung einer Zu- oder Absage.

### **Lösung:**

Mittels digitaler Zertifikate können heute E-Mails und E-Dokumente digital verschlüsselt und signiert werden. Darüber hinaus sind die Zertifikate eine Art elektronischer Ausweis und identifizieren den Inhaber eindeutig. Das Softwareprodukt der Deutschen Bank AG ‚db-order‘ nutzt diese Technologie und ermöglicht damit die sichere elektronische Bereitstellung relevanter Geschäftsdaten zur Bürgschaftsprüfung als auch die digitale Signatur von Bürgschaftsanträgen und –erklärungen. Unberechtigte Dritte können diese Daten nicht einsehen oder manipulieren. Der Prozess kann vollständig automatisiert werden, die Bürgschaftszusage kann binnen kürzester Zeit erteilt werden.

### **Nutzen der Bridge-CA:**

Seit einiger Zeit ist die Deutsche Bank Mitglied der Bridge-CA Initiative. Damit bekennt sie sich zu Standards, die es ermöglichen auch die digitalen Ausweise anderer Teilnehmer anzuerkennen. Die Anzahl potentieller Kunden für den automatisierten Bürgschaftsantrag ist damit um ein Vielfaches gestiegen. Die Bank ist damit nicht mehr gezwungen für jeden Kunden ein neues Zertifikat auszustellen, der Kunde kann sein Zertifikat für mehrere Anwendungen nutzen.

## Anwendungsbeispiel: Bedarfsgerechte Verwaltung von Leitungskapazitäten

Daten und Informationen mit Filialen, Kunden und Lieferanten im Bedarfsfall schnell und fehlerfrei auszutauschen muß jederzeit möglich sein. Kostenintensive Leitungskapazitäten wurden hierfür stets bevorratet, denn Kapazitätserweiterung waren stets langwierig und aufwendig.

Mittels digital signierter E-Mails können künftig die Mitarbeiter der Deutschen Bank AG Bestellungen und Kündigungen von Leitungskapazitäten direkt an Ihre Ansprechpartner seitens der Deutschen Telekom AG übermitteln. Aufwendige administrative Prozesse des Ausdrucks, der Freigabe, der Übermittlung und Eingabe lassen sich dadurch auf Minuten reduzieren.

Dadurch, daß beide Organisationen Mitglied in der Bridge-CA sind, ist die Interoperabilität der Mailingsysteme und das gegenseitige Vertrauen in die Mitarbeiterzertifikate gewährleistet.



### **Problemstellung:**

Kommunikation ist zu einem der zentralen Wettbewerbsfaktoren in der heutigen Wissensgesellschaft geworden. Daten und Informationen mit Filialen, Kunden und Lieferanten im Bedarfsfall schnell und fehlerfrei auszutauschen muß jederzeit möglich sein. Kostenintensive Leitungskapazitäten wurden hierfür stets bevorratet, denn Kapazitätserweiterung waren stets langwierig und aufwendig.

### **Lösung:**

Mittels digital signierter E-Mails können künftig die Mitarbeiter der Deutschen Bank AG Bestellungen und Kündigungen von Leitungskapazitäten direkt an Ihre Ansprechpartner seitens der Deutschen Telekom AG übermitteln. Darüber hinaus liegen die spezifizierenden Daten –verschlüsselt übermittelt- beiden Seiten in einer verarbeitbaren elektronischen Form vor. Aufwendige administrative Prozesse des Ausdrucks, der Freigabe, der Übermittlung und Eingabe lassen sich dadurch auf Minuten reduzieren. Leitungskapazitäten können deutlich bedarfsgerechter Bereitgestellt werden.

### **Nutzen der Bridge-CA:**

Dadurch, daß beide Organisationen Mitglied in der Bridge-CA sind, ist die Interoperabilität der Mailingsysteme und das gegenseitige Vertrauen in die Mitarbeiterzertifikate gewährleistet.

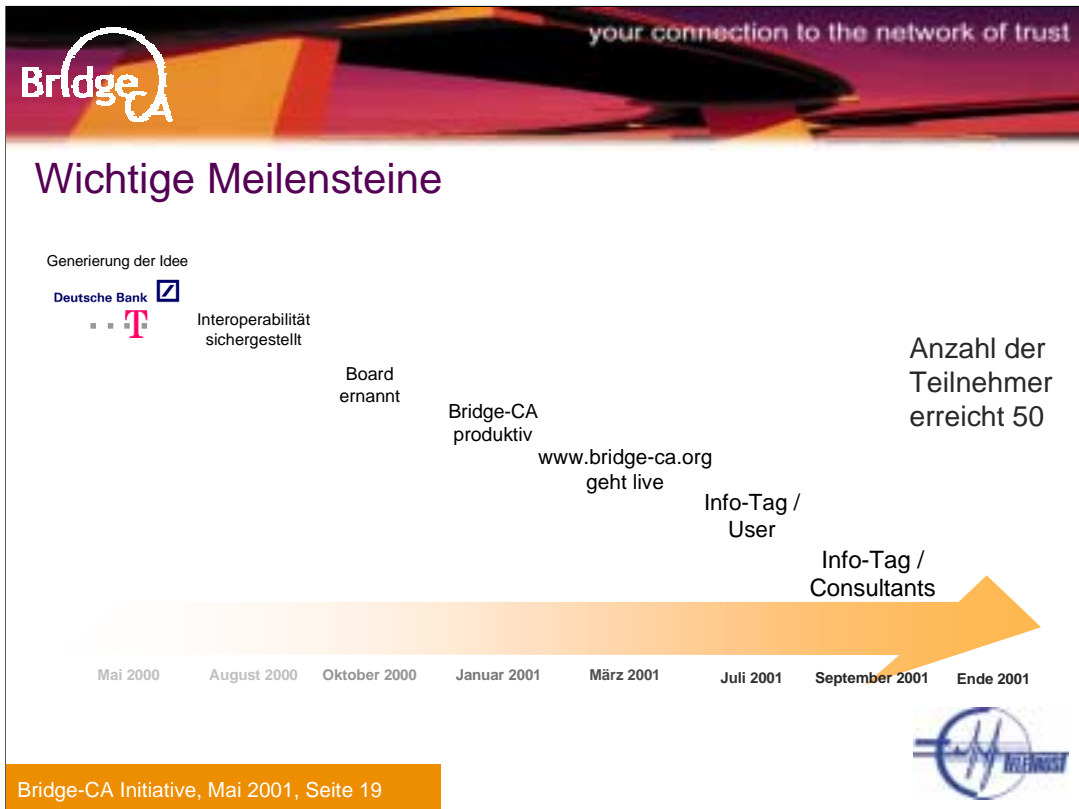
## Aktuelle Aufgaben

- Zertifikatsstandards (bspw. AuthorityKeyId, SubjectKeyId, critical/non-critical values) => Aufklärung
- Behebung kleinerer Probleme mit den getesteten Clients
- Zugang zu und Interoperabilität zwischen den unternehmensspezifischen Verzeichnisdiensten
- Verifikation und Anpassung der Zertifikatsketten
- Schalenmodell der Gültigkeitszeiträume innerhalb von Microsoft-Produkten
- BasicConstraints - Länge der Vertrauenskette
- Test der Verschlüsselung und des Policy Mapping
- Kontrollierte Ausbreitung des Vertrauens



Die bisherigen Interoperabilitätstests haben ergeben, daß es für alle aufgetretenen Probleme einfache Lösungen oder Work-arounds gibt.

Die oben aufgeführte Liste dient eher dazu, auf die Fragestellungen aufmerksam zu machen, die man am besten gleich beim Aufbau einer firmeninternen PKI klärt.



Die Deutsche Telekom und die Deutsche Bank haben im Mai 2000 eine Initiative zur Sicherung der elektronischen Kommunikation in und zwischen Organisationen gestartet.

Am 16. Januar 2001 ging die Bridge-CA live, die als Dach für vorhandene PKIs genutzt werden kann und die so die Einschränkungen der bisherigen PKI-Inseln auflöst.

TeleTrust e.V. erbringt den Bridge-CA Service.

Presseerklärungen dazu:

- Deutsche Bank und Deutsche Telekom, Okt. 2000:  
[www.deutsche-bank.de/presse](http://www.deutsche-bank.de/presse) oder  
<http://public.deutsche-bank.de/deuba/db/navigate.nsf/Frameset/DEVP-42MLXQ?OpenDocument>  
<http://www.telekom.de/dtag/presse/index/0,1014,D,00.html>
- TeleTrust, Jan. 2001:  
<http://212.185.192.36/presse.asp?id=70140>
- CeBIT-Presseerklärungen von  
 TeleTrust, Deutscher Bank, Deutscher Telekom, Giesecke&Devrient, ...

## Anforderungen für die Teilnahme an der Bridge-CA bezüglich E-Mail

- Persönliche Identifikation und Registrierung des Zertifikatsinhabers
- Zugriff auf Rückruf-Daten seitens der Bridge-CA und dessen Teilnehmer (CRLs im eigenen bzw. über replizierte Directories)
- Bei der Vergabe von Namen (Nutzer- oder CA-Zertifikaten) muß sichergestellt sein, daß die gewählten DNS über alle beteiligten Infrastrukturen hinweg eindeutig sind
- Zertifikate sind konform zum Standard X.509v3
- Der Private Key der CA ist ein RSA-Schlüssel mit einer Schlüssellänge von mindestens 1024 Bit
- Die Zertifikate müssen als Datei im Format .crt, .der oder .p7c vorliegen.
- Das Attribut KeyUsage im CA-Zertifikat ist auf Signatur und/oder Verschlüsselung gesetzt



Bei der Festlegung der Anforderungen für die Teilnahme an der Bridge-CA standen pragmatische Überlegungen im Vordergrund. Möglichst viele Interessen waren dabei zu berücksichtigen ohne die grundlegende Vertrauensstruktur zu gefährden.

## TeleTrusT Deutschland e.V. - Betreiber der 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), Bridge-CA].
  - Förderung innovativer Technologien (z.B. biometrische Verfahren)
- Internationale Aktivitäten (gemeinsam mit EEMA und PKI-Forum; Ausrichten der ISSE-Konferenzen, etc.)



TeleTrusT wurde von den Initiatoren und dem Board als Betreiber und Owner ausgewählt, weil TeleTrusT von Beginn an mitarbeitete und um die Neutralität der Bridge-CA-Initiative zu unterstreichen.

Die Mitglieder von TeleTrusT umfassen ca. 100 Unternehmen und Behörden, darunter das Bundeskriminalamt Wiesbaden, DATEVeG, Deutsche Telekom AG, Siemens AG etc.

Relativ früh konzentrierte sich TeleTrusT e.V. auf das Internet mit seinen Online-Diensten, die zunehmende Anwendung kryptographischer Verfahren und die internationalen Wechselwirkungen.

TTT arbeitet daran mit, die gesellschaftliche und rechtliche Akzeptanz digitaler Signaturen zu schaffen, zu der neben standardisierten technischen Lösungen und einer Sicherungsinfrastruktur auch die Rechtsgrundlagen gehören.

Erfahrungen aus dem täglichen Umgang mit bestimmten Sicherungsverfahren wie beispielsweise der Verwendung von PIN und Passwort zur Freischaltung anderer Funktionalitäten machten deutlich, dass an der Ergänzung oder Ablösung solcher Verfahren durch neue innovative Lösungen (z.B. Biometrie) kein Weg vorbei führt.

Es geht um komplexe Sichtweisen mit ausreichender Flexibilität, die auch internationale Entwicklungen wie die steigende Attraktivität des Internet und die immer stärker um sich greifende Globalisierung von Kommunikations- und Geschäftsprozessen beachten und auf sie Einfluß nehmen.

Aus diesen Gründen vertritt TeleTrusT als Kompetenzverbund für angewandte Kryptographie und Biometrie die für den Anwender relevanten Leistungen dieser "Schlüsseltechnologien". Die politische und wirtschaftliche Unabhängigkeit von TeleTrusT war und ist die Basis für die Glaubwürdigkeit dieses Anliegens.



your connection to the network of trust

Kontakte: [www.bridge-ca.org](http://www.bridge-ca.org)

Helmut Reimer  
Geschäftsführer TeleTrusT  
Eichendorfstr. 16  
99096 Erfurt  
Germany  
email: [teletrust@t-online.de](mailto:teletrust@t-online.de)

Bernhard Esslinger  
Deutsche Bank AG  
Director eID-Solutions  
Frankfurter Str. 84  
65760 Eschborn  
Germany  
email: [bernhard.esslinger@db.com](mailto:bernhard.esslinger@db.com)  
[b.esslinger@eudoramail.com](mailto:b.esslinger@eudoramail.com)

Bernd Kowalski  
Deutsche Telekom AG  
Geschäftsführer T-Telesec  
Untere Industriestr. 20  
57250 Netphen  
Germany  
email: [bernd.kowalski@telekom.de](mailto:bernd.kowalski@telekom.de)

