

# TeleTrust European Bridge CA – Sichere Kommunikation jenseits von Organisationsgrenzen

*Dr. Guido von der Heidt, Siemens AG, TeleTrust-Vorstand und Sprecher des EBCA-Boards*

Die TeleTrust European Bridge CA (EBCA), [www.ebca.de](http://www.ebca.de), ist ein Projekt des IT-Sicherheitsverbandes TeleTrust Deutschland e.V. zur Förderung der sicheren Kommunikation und der Nutzung von Public Key Infrastrukturen (PKI) über Organisationsgrenzen hinweg. Im folgenden werden die hierbei auftretenden Problemstellungen und der Beitrag der EBCA zur Lösung erörtert. Der Schwerpunkt liegt auf sicherer E-Mail, die Fragen und Lösungsansätze sind aber auch auf andere Kommunikationsformen anwendbar.

Die Absicherung externer Kommunikationsbeziehungen und Geschäftsprozesse ist ein wesentlicher Bestandteil heutiger Informationssicherheits-Managementsysteme. Die Grenzen von Organisationen und Unternehmen verwischen, und es werden sichere Verfahren zur Anbindung externer Dritter wie Kunden, Bürger, Lieferanten, Dienstleister oder allgemein Kooperationspartner über öffentliche Netze benötigt.

E-Mail ist ein Hauptmedium elektronischer Kommunikation und wird insbesondere für den Austausch unstrukturierter Daten und Adhoc-Kollaboration genutzt. Zum Schutz von E-Mail-Kommunikation existieren verschiedene Verfahren, wobei der Standard S/MIME (Secure Multipurpose Internet Mail Extensions) sehr weit verbreitet und universell einsetzbar ist. S/MIME bietet Verschlüsselung und digitale Signatur von E-Mails auf Basis von PKI-Zertifikaten. Im Gegensatz zur Verschlüsselung zwischen E-Mail-Servern (z.B. Transport Layer Security - TLS) bietet S/MIME Ende-zu-Ende-Sicherheit, was mit aufweichenden Netzwerksgrenzen und der individuellen Anbindung von End-Anwendern über das Internet von wachsender Bedeutung ist.

## Die Problemstellung

Bei der organisationsübergreifenden sicheren E-Mail-Kommunikation mittels S/MIME begegnet man üblicherweise folgenden Fragestellungen und Problemen:

1. PKI: Verfügen die Kommunikationspartner über digitale Zertifikate?

2. Interoperabilität: Sind die verwendeten Verschlüsselungssysteme und PKI-Lösungen kompatibel zueinander?  
3. Trust: Kann man den Sicherheits-Policies und den (PKI-)Betriebsprozessen des Partners vertrauen?

4. Infrastruktur: Wie kann gegenseitig auf die Zertifikate aus den PKI-Systemen der Partner zugegriffen und deren Gültigkeit geprüft werden?

5. Know-How: Häufig verfügen die einzelnen Kommunikationspartner nicht über ausreichende Kenntnisse, um eine sichere Kommunikation zu etablieren.

Während die reine Verfügbarkeit von digitalen Zertifikaten durch die Services öffentlicher Trust Center sowie vorhandene PKI Implementierungen großer Organisationen und Unternehmen heute weitgehend gegeben ist, adressiert die EBCA vornehmlich die unter den Punkten 2. - 4. aufgeführten Prozess- und Infrastruktur-Fragen.

## Die TeleTrust European Bridge CA

Die EBCA ist eine 2001 unter dem Dach von TeleTrust gegründete Projektpartnerschaft öffentlicher und privater Organisationen, die eine PKI betreiben und organisationsübergreifend nutzen. Gegenwärtige Mitwirkende sind: Deutsche Bank, Deutsche Bundesbank, E.ON, Landesbetrieb für Statistik und Kommunikationstechnologie Niedersachsen, Microsoft Deutschland, PKI-1 der Verwaltung, Rundfunk und Telekom Regulierungs-GmbH Österreich, Signaturlösung Niedersachsen, Siemens, Siemens Enterprise Communications und TC Trust Center.

Die EBCA bildet eine Vertrauensgemeinschaft, eine „Trust Community“, in der ein definiertes Mindest-Sicherheitsniveau der beteiligten PKIen herrscht und damit die Grundlage für Trust-Beziehungen zwischen Mitgliedern und Dritten gegeben ist. Mit Aufnahme eines Mitgliedes (oder bei Veränderungen) erfolgen Interoperabilitätstest, um die Kompatibilität der PKI-Systeme und S/MIME-Lösungen sicherzustellen. Die Infrastruktur der EBCA sorgt für eine sichere Verteilung der Root-Zertifikate

der Mitglieder-PKIs und eine zentrale Bereitstellung der Anwender-Zertifikate im Internet. Über den EBCA sind aktuell über 700.000 Anwender-Zertifikate abgedeckt.

Die Steuerung der EBCA erfolgt durch das EBCA Board und die technische Arbeitsgruppe. Die technische Arbeitsgruppe ist offen für TeleTrust-Mitglieder und alle interessierten Kreise und bildet ein breites Forum zum Wissens- und Informationsaustausch. Ergebnisse, Dokumentation und Prozessbeschreibungen werden auf der EBCA-Website veröffentlicht.

## EBCA Trust Model und Infrastruktur

Kernelemente der EBCA sind das „Trust Model“ und die EBCA Infrastruktur, umgesetzt durch:

- \_\_\_\_\_ Die „Certificate Policy“ (basierend auf RFC 3647),
- \_\_\_\_\_ die „Certificate Trust List“,
- \_\_\_\_\_ den „Certificate Download Service“ und
- \_\_\_\_\_ den EBCA Verzeichnisdienst.

Alle Mitglieder bestätigen durch Selbsterklärung, den Anforderungen und Vorgaben der EBCA Certificate Policy zu entsprechen, und dokumentieren dies in einer zur EBCA-Policy konformen Certificate Policy für ihre PKI. Dadurch wird ein Minimum-Sicherheitsniveau und Vergleichbarkeit für den Betrieb, die Prozesse und die zugrundeliegenden IT-Infrastrukturen der Teilnehmer-PKIs sichergestellt. Die Mitgliedschaft in der EBCA ist somit eine Art Qualitätssiegel, auf der Mitglieder und andere Organisationen Vertrauensbeziehungen zu EBCA-Mitgliedern bilden können.

Die Root-Zertifikate der Teilnehmer-PKIs werden gesichert

registriert und in einer von der EBCA digital signierten Certificate Trust List (CTL) bereitgestellt, [http://www.bridge-ca.de/html/ct\\_liste.html](http://www.bridge-ca.de/html/ct_liste.html). Um den Download, die Prüfung der CTL und den Import der enthaltenen Root-Zertifikate in Anwender-PC-Systeme zu vereinfachen, wird aktuell der Certificate Download Service entwickelt. Hierbei handelt es sich um Software-Tools, die diesen Vorgang automatisieren. Ein Tool für Mozilla Firefox / Thunderbird ist verfügbar, ein Plug-in für Microsoft-Outlook folgt.

Über den EBCA-Verzeichnisdienst werden Anwender-Zertifikate von Teilnehmer-PKIs zentral im Internet bereitgestellt. Der EBCA-Verzeichnisdienst kann als LDAP-Verzeichnis in E-Mail-Verschlüsselungssystemen von beliebigen Nutzern für den automatischen Zertifikatsdownload konfiguriert werden ([dir.bridge-ca.org](http://dir.bridge-ca.org)), alternativ können Zertifikate manuell über ein Web-Interface bezogen werden, [http://www.bridge-ca.de/html/verz\\_dienst.html](http://www.bridge-ca.de/html/verz_dienst.html). S. Abbildung 1 für

eine entsprechende Referenzarchitektur.

## Ausblick

Schwerpunkte der EBCA sind die Mitwirkungsbasis auszubauen und das Trust Model sowie die Infrastruktur auf weitere Kommunikations- und Nutzungsformen auszudehnen. Auch für Authentisierung, „Identity Federation“ und (fortgeschrittene) digitale Signaturen ist Trust zwischen den beteiligten Organisationen entscheidend und oft nicht genügend adressiert. Bzgl. der Infrastruktur gilt es, mobile Systeme (Smart Phones, PDAs,...) besser zu integrieren, wobei aktuelle Plattformen und Produkte PKI und S/MIME vielfach noch nicht ausreichend unterstützen. Nur durch zusätzliche (internationale) Teilnehmer kann der Nutzen der EBCA als Trust Community vergrößert und die Infrastruktur weiter ausgebaut werden. Die EBCA ist offen für Organisationen / PKIs aller Größe und dieser Artikel soll auch zum Mitwirken in der EBCA anregen. ■

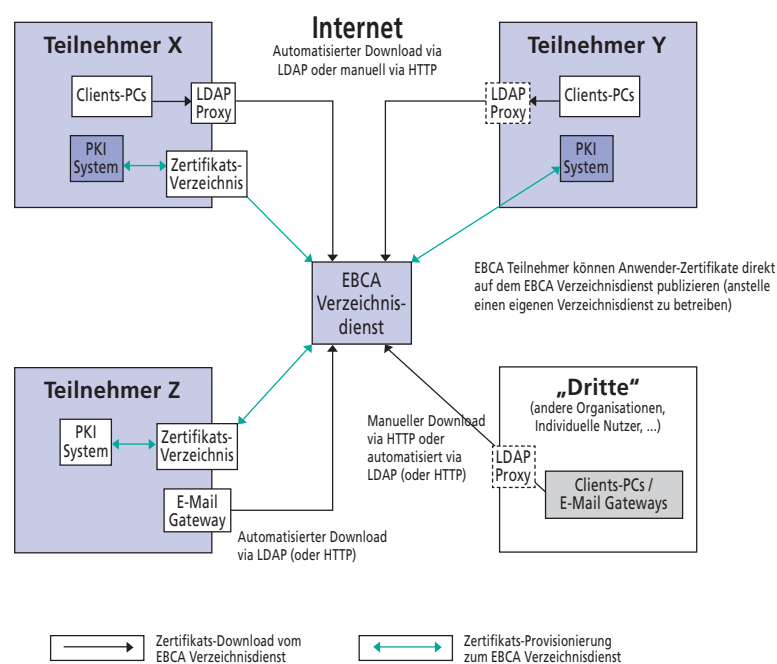


Abbildung 1: EBCA Referenzarchitektur für sichere E-Mail-Kommunikation