

Ekkehard Diedrich

TeleTrust European Bridge CA: Die Brücke für sichere E-Mail Kommunikation

Als die TeleTrust European Bridge CA vor nunmehr fast 10 Jahren ins Leben gerufen wurde, waren die Beweggründe dafür nahezu identisch mit denen, die anzuführen sind, wenn sich heute Unternehmen mit ihren Public Key Infrastructures (PKI) diesem Netzwerk anschließen: die deutliche Vereinfachung sicherer E-Mail-Kommunikation zwischen Unternehmen und Behörden durch praktikable Lösungen. Verschlüsseln, Signieren, Verifizieren – alles Schlagwörter, die vor dem Hintergrund allgemein zunehmenden Bewusstseins bezüglich der Schwächen und Gefahren im Internet häufig zu hören sind, allein die verbreitete Anwendung von Technologien für sicheren E-Mail-Verkehr ist nicht zuletzt durch die Fülle unterschiedlicher Verfahren nicht so voran gekommen, wie es wünschenswert wäre. Insofern versteht sich dieser Beitrag als ein Plädoyer dafür, die TeleTrust European Bridge CA als eine verlässliche Brücke zu betrachten, die den Austausch sicherer E-Mails fördert und zudem für die teilnehmenden Organisationen den Aufwand beherrschbar hält.

1 Einleitung

Mit der TeleTrust European Bridge CA (EBCA) steht den teilnehmenden Organisationen eine kostengünstige und verlässliche Dienstleistung zur Verfügung, die auf einfache Weise die gegenseitige Anerkennung von Zertifikaten der teilnehmenden Unternehmen, Behörden und Institutionen ermöglicht. Als Brücke zwischen den Beteiligten prüft die European Bridge CA die Root-CA-Zertifikate der teilnehmenden Organisationen, unterstützt den Austausch von Mitarbeiterzertifikaten und gewährleistet damit unter anderem den organisationsübergreifen-

den, sicheren (signierten und verschlüsselten) E-Mail-Austausch, ohne dass die Beteiligten untereinander bilaterale Vereinbarungen zu treffen haben. Stattdessen erkennen die Beteiligten die European Bridge CA als vertrauenswürdige Vermittlungsinstanz an. Damit ist einer der wichtigsten Punkte adressiert, der die gegenwärtigen Schwierigkeiten verdeutlicht, die Nutzern begegnen, wenn sie per E-Mail sicher kommunizieren wollen: die dafür notwendige Prozesse müssen automatisch im Hintergrund ablaufen. Es ist dem Nutzer im Allgemeinen nicht zuzumuten, dem Kommunikationspartner z.B. zunächst das eigene Zertifikat mit Hilfe eigener Bedienschritte zur Verfügung zu stellen, um die notwendige Interoperabilität zwischen Sender und Empfänger herzustellen. In [1] wird sehr deutlich, dass es auf der einen Seite für Unternehmen sehr schwierig wird, eine Vielzahl unterschiedlichster Systeme gleichzeitig zu administrieren, dass es auf der anderen Seite für die Nutzer um so schwieriger in der Anwendung wird, je mehr unterschiedliche Lösungen zur Verfügung stehen.

Um die notwendige Interoperabilität aller an der EBCA beteiligten Public Key Infrastructures (PKIs) zu gewährleisten, muss jede neu teilnehmende Organisation vor der Aufnahme an einem Konformitätstest teilnehmen. Anhand einer eigens dafür entwickelten Spezifikation werden diese Tests gemeinsam mit einem oder mehreren Partnern aus dem bestehenden EBCA-Verbund durchgeführt. Der Aufwand hierfür ist überschaubar, so dass entsprechende Verabredungen schnell zu treffen sind. Sollte sich im Ergebnis des Tests herausstellen, dass zur Interoperabilität noch technische oder organisatorische Anpassungen erforderlich sind, so ist der potenziell neue Teilnehmer gehalten, die entsprechenden Anpassungen vorzunehmen. Darüber hinaus wird generell die Bereitschaft zur Anpassung von Komponenten gewünscht, falls dies für die EBCA-Gemeinschaft zur Aufrechterhaltung der Interoperabilität, z.B. infolge technischer Weiterentwicklung oder anderer veränderter Anforderungen erforderlich wird.



**Dipl. Ing.
Ekkehard Diedrich**

Referent und
Projektsteuerer
in der Bundesge-
schäftsstelle des

IT-Sicherheitsverbandes TeleTrust
E-Mail: Ekkehard.Diedrich@teletrust.de

2 Wichtige organisatorische und technische Anforderungen

2.1 Anforderungen an eine teilnehmende PKI und deren Architektur

- persönliche Identifikation und Registrierung des Zertifikatsinhabers,
- Zugriff auf Rückruf-Daten seitens der EBCA und dessen Teilnehmer (Certificate Revocation Lists (CRLs) in eigenen bzw. über replizierte Directories oder von einem Webserver abrufbar oder durch Einsatz eines OCSP-Servers),
- Sicherstellung der Eindeutigkeit von gewählten Domain Names (DNs) über alle beteiligten Infrastrukturen hinweg.

2.2 Anforderungen an die zum Einsatz kommenden Zertifikate

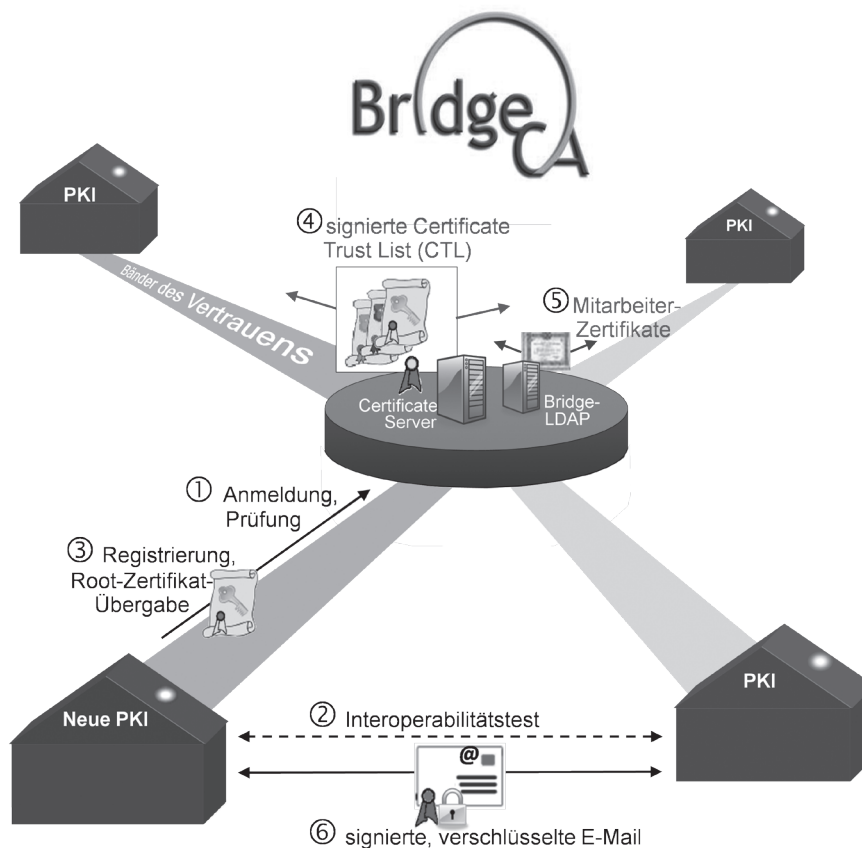
- Zertifikate konform zum Standard X.509v3,
- Private Key als RSA-Schlüssel mit Schlüssellänge von mindestens 1024 Bit,
- Key Usage-Attribut auf Signatur und/oder Verschlüsselung gesetzt,
- Zertifikate müssen als Datei im Format .crt, .der oder .p7b vorliegen.

2.3 Anforderungen an den PKI-Client

- Import von Root-Zertifikaten in einem Standardformat (z.B. PKCS#7),
- Unterstützung des Formats S/MIMEv2,
- signierte E-Mails müssen grundsätzlich im Opaque signed-Modus ausgetauscht werden können; d.h., dass die E-Mail signiert wird und insgesamt als signiertes File gesendet wird, der Textbody ist damit Teil des .p7-Files.

Auf diese grundsätzlichen Anforderungen für den Betrieb einer PKI haben sich die Teilnehmer der EBCA geeinigt. Damit sind die wesentlichen Sicherheitsanforderungen im Hinblick auf sichere E-Mail Kommunikation in Geschäftsprozessen dargelegt, deren Einhaltung sich sämtliche Teilnehmerorganisationen mit Ihrem Beitritt in Form einer Selbsterklärung gegenseitig versichern [2].

Bild 1 | Übersicht zum EBCA – Anmeldeprozess und -Verteildienst



3 Der EBCA-Anmeldeprozess und Verteildienst

Die Grafik in Bild 1 veranschaulicht in knapper Form die einzelnen Prozesse, die mit einer neuen Teilnehmerorganisation zur Integration vorgenommen werden. Im ersten Schritt (1) in Bild 1 erhält ein Interessent Unterlagen zur Information, wie z.B. die bereits genannte Selbsterklärung, die Certificate Policy, einen Kooperationsvertrag und eine Preisliste. Schritt 2 (2) in Bild 1 umfasst die bereits erwähnten Interoperabilitätstests, die jeweils gegen sogenannte Testreferenzen vorzunehmen sind, die aus dem Kreis der EBCA-Mitglieder benannt werden. Mit der eigentlichen Registrierung (3) in Bild 1 übergibt der neue Teilnehmer u.a. sein Root-Zertifikat (X.509-Zertifikat) mit zugehöriger Policy, seine Sub-CA-Zertifikate sowie die Mitarbeiterzertifikate der benannten Ansprechpartner, mit denen künftig signierte und verschlüsselte E-Mails ausgetauscht werden sollen. Nach der erfolgten Registrierung wird das Root-Zertifikat der neuen Teilnehmerorganisation im .cer-Format

in die Certificate Trust List (CTL) aufgenommen. Die CTL ist als PKCS#7-Container im p7b-Format angelegt, aus dem sich alle Root-Zertifikate direkt in Zertifikatsverzeichnisse installieren lassen. Die EBCA signiert die CTL zur Sicherung der Authentizität und Integrität mit einem Signierzertifikat, das T-Systems/TeleSec als Certificate Authority (CA) der EBCA ausgestellt hat. Durch diese Signatur bestätigt die EBCA die Herkunft der Zertifikate und die Einhaltung des geforderten Sicherheitsniveaus durch die Teilnehmer. Die signierte CTL wird mittels einer signierten und verschlüsselten E-Mail direkt an die benannten Ansprechpartner der Teilnehmerorganisationen geschickt, damit auch an den Ansprechpartner der neu hinzugekommenen Teilnehmerorganisation (4) in Bild 1). Außerdem wird die signierte CTL auf einem Web-Server öffentlich und kostenlos zum Download bereitgestellt.

Die TeleTrusT European Bridge CA stellt über einen Verzeichnisdienst Mitarbeiterzertifikate (X.509-Zertifikate mit den öffentlichen Schlüsseln der Mitarbei-

ter) der EBCA-Teilnehmerorganisationen zur Verfügung (⑤ in Bild 1). Diese werden benötigt, um den betreffenden Mitarbeitern verschlüsselte E-Mails (im S/MIME-Format) schicken zu können. Der EBCA-Verzeichnisdienst arbeitet als LDAP-Proxy, d.h. er hält nicht selbst alle aktuellen Mitarbeiterzertifikate sämtlicher Teilnehmerorganisationen bereit, sondern er verfügt über eine Liste mit den entsprechenden Links zu den LDAP-Servern der EBCA-Teilnehmerorganisationen. Somit leitet z.B. der LDAP-Proxy eine eingehende Anfrage von Teilnehmerorganisation A an den entsprechenden richtigen LDAP-Server der angefragten Teilnehmerorganisation B weiter. Dieser gibt dann das gewünschte Mitarbeiterzertifikat an den LDAP-Proxy zurück, dieser reicht es dann weiter an den ursprünglich anfragenden Teilnehmer der Organisation A.

Durch den oben beschriebenen vertrauensvollen Austausch von Root-/CA- und Mitarbeiter-Zertifikaten können die EBCA-Teilnehmerorganisationen untereinander sichere, signierte und verschlüsselte E-Mails austauschen (⑥ in Bild 1). Der EBCA-Verbund wirkt dabei im Prinzip wie eine einzige große PKI, trotzdem behalten die einzelnen Unternehmen/Behörden ihre PKI-Eigenständigkeit und müssen sich nicht einer übergeordneten CA-Autorität unterordnen. Außerdem behalten sie ihre Investitionssicherheit, da nur gemeinsame, vorab geprüfte internationale Standards einzuhalten sind, aber keine Zwänge hinsichtlich der Hard- und Software bestehen.

Eine besondere Rolle für die Herstellung gegenseitigen Vertrauens innerhalb der EBCA nimmt die Certificate Policy (CP) ein. Diese Zertifikatsrichtlinie enthält Vorgaben und Anforderungen an die teilnehmenden Public Key Infrastructures (PKI) sowie an die zum Einsatz kommenden Zertifikate. Darin sind technische und organisatorische Konformitätsanforderungen formuliert, die zur Schaffung organisationsübergreifender Vertrauensbeziehungen zwischen den Mitgliedern der EBCA dienen. Die CP orientiert sich am RFC3647, der als international anerkanntes Rahmenwerk gilt. Somit erhalten die teilnehmenden Organisationen geeignete Unterstützung bei der Erstellung der eigenen PKI-Richtlinien gemäß RFC3647, was deren Vergleichbarkeit deutlich erleichtert. Hiernach erklärt der EBCA-Teilnehmer, dass seine CA den Vorgaben und Anforderungen der Certificate Policy entspricht, dass er eine eige-

ne Teilnehmer-CP erstellt hat und diese die Vorgaben der EBCA-CP umsetzt und dass die technische Konformität in Form erfolgreich durchgeführter Interoperabilitätstests nachgewiesen wurde.

Die Zertifikatsrichtlinie beschreibt Sicherheitsanforderungen an den Betrieb von Zertifizierungsstellen für die Ausstellung und Nutzung von X.509 konformen Zertifikaten. Darüber hinaus definiert die Richtlinie für Dritte einen Grundsatz für die Nutzung von Zertifikaten. Sie beschreibt damit ein transparentes Sicherheitsniveau für die Vertraulichkeit und Authentisierung von Nachrichten, wie z.B. beim Austausch von E-Mails im S/MIME-Format. Auch für andere Zertifikatszwecke wie die Authentisierung bei SSL/TLS sind diese Vorgaben innerhalb der EBCA bindend.

Mit der Zertifikatsrichtlinie wird damit der eigentliche Fokus der EBCA-Arbeit nachhaltig unterstützt, mit Hilfe von Public Key Infrastrukturen sichere organisationsübergreifende elektronische Geschäftsprozesse zu realisieren. Die dafür notwendigen Anforderungen lassen sich wie folgt zusammenfassen:

- technische Interoperabilität,
- Vergleichbarkeit der Sicherheitsniveaus
- geeignete Mindeststandards.

Die EBCA bietet damit eine Plattform für die technische Konformität durch Profilierung der technischen Standards sowie für die Durchführung von Tests zur Feststellung gegenseitiger Interoperabilität. Mit der Zertifikatsrichtlinie werden den Mitgliedern der EBCA Vorgaben für Mindeststandards an Sicherheit zum Betrieb einer EBCA konformen PKI gegeben. Der Aufbau nach RFC3647 ermöglicht eine nach außen transparente und vergleichbare Darstellung der Sicherheitsstandards der innerhalb der EBCA betriebenen PKI-en. Jedes Mitglied der EBCA ist gehalten, den Anforderungen dieser Richtlinie zu entsprechen. Für die Vergleichbarkeit verfügt jedes Mitglied über eine eigene CP, die die Mindeststandards aus der durch die EBCA vorgelegten CP in geeigneter Weise bestätigen.

4 Zertifikats Download Service

Dass die gemeinsame Arbeit der teilnehmenden Organisationen im Rahmen der TeleTrust European Bridge CA natürlich auch dem Erfahrungsaustausch der han-

delnden Akteure dient, ist nachvollziehbar. Auf diese Weise werden technische Fragestellungen aufgegriffen, die durch innovative Ansätze gegebenenfalls im Interesse aller teilnehmenden Organisationen zur Lösung geführt werden. So ist in jüngster Zeit in Kooperation mit dem Institut für Internetsicherheit – if(is) der Fachhochschule Gelsenkirchen der sogenannte „Certificate Download Service“ entwickelt worden, mit dem eine Thematik einer sinnvollen und praxistauglichen Lösung zugeführt wird, welche die Experten der Teilnehmerorganisationen längere Zeit beschäftigte: Die Tatsache, dass die Zertifikate der EBCA-Teilnehmer mit aktuellen Web-Browsern oder E-Mail-Clients nicht mit ausgeliefert werden. Somit können die entsprechenden Signaturen natürlich auch nicht verifiziert werden, vielmehr schlägt die Verifikation der Signatur eines EBCA-Teilnehmers fehl, da beim Anwender kein entsprechendes Zertifikat gefunden werden kann. Die gegenwärtig in der Umsetzung befindliche angestrebte Lösung besteht darin, dass man für eine Auswahl von Anwendungen jeweils ein Add-On auf der Website der EBCA zur Verfügung stellt, das folgende Schritte ausführt:

- aktuelle Zertifikatsliste von EBCA-Website herunterladen
- Signatur der Zertifikatsliste verifizieren
- nach erfolgreicher Verifizierung alle Zertifikate der Liste als Root-CA-Zertifikate in den Zertifikatsspeicher importieren.

Für Mozilla Firefox und Mozilla Thunderbird wurde hierzu ein Add-In entwickelt, Microsoft-Clients werden durch einen Plug-In-Agenten mit der aktuellen CA-Zertifikatsliste versorgt.

Auf diese Weise wird anschaulich, dass die TeleTrust EBCA, auf den ersten Blick als reines Zweckbündnis zur Vereinfachung des organisationsübergreifenden Austausches sicherer E-Mail-Kommunikation gegründet, als Brücke eben diese Funktion ausübt. Darüber hinaus greift sie – aus dem Bestreben der Gemeinschaft der EBCA-Teilnehmer nach Effizienzsteigerungen – Innovationen auf, die das Thema insgesamt voranbringen.

Literatur

- [1] DuD 5/2010, S. 318-322 Henrik Koy, Bernhard Esslinger: TeleTrust European Bridge CA
- [2] TeleTrust European Bridge CA <http://www.bridge.ca.de>