



## **Prozessbeschreibung**

**Version:** 2.0  
**Datum:** 10. August 2009

## Inhaltsverzeichnis

Historie der Dokumentversionen .....	2
0 Einleitung.....	3
1 Vorbereitung, Anmeldung.....	4
2 Interoperabilitätstest .....	4
3 Registrieren einer PKI zur Teilnahme an der EB-CA.....	5
4 Vertrauenswürdige Bereitstellung von Root-/CA-Zertifikaten.....	6
4.1 Root-Zertifikate .....	6
4.2 CA-Zertifikate (Sub-Root-Zertifikate) .....	6
4.3 Sperrliste .....	6
5 Vertrauenswürdige Bereitstellung von Mitarbeiter-Zertifikaten .....	7
5.1 Verzeichnisdienst .....	7
5.2 Validierungsdienst .....	8
6 Sicherer E-Mail-Verkehr zwischen EB-CA-Teilehmerorganisationen .....	9
7 Veränderungen bei registrierten Root Zertifikaten .....	9
8 Beendigung der Teilnahme an der EB-CA.....	10

## Historie der Dokumentversionen

Version	Datum	Autor	Änderungsgrund / Bemerkungen
1.0-1.2	2001 - 2005	Peter Steiert	Ersterstellung
1.3	18.04.2008	Helmut Schütze	Aktualisierung
1.4	06.05.2008	Helmut Schütze	Änderungsvorschläge von Dr. Welsch eingefügt
1.4.1	20.01.2009	Helmut Schütze	Logos und Layout aktualisiert
1.5	22.02.2009	Helmut Schütze	Aktualisierung
2.0	10.08.2009	Helmut Schütze	Anpassung an veränderte CA-Situation

## 0 Einleitung

Gegenwärtig sind in Europa unterschiedliche Zertifikatshierarchien bereits vorhanden oder in der Entstehung begriffen. Ziel der von der Deutschen Telekom AG und der Deutschen Bank AG initiierten und von TeleTrusT Deutschland e.V. betriebenen European Bridge-CA (EB-CA) ist es, eine Infrastruktur zu realisieren, mit der die teilnehmenden Organisationen Interoperabilität zwischen ihren Public-Key Infrastrukturen (PKIs) erreichen können. Als Brücke zwischen den Beteiligten prüft die European Bridge-CA die Root-CA-Zertifikate der teilnehmenden Organisationen und erlaubt damit unter anderem den organisationsübergreifenden, sicheren (signierten und verschlüsselten) E-Mail-Austausch, ohne dass die Beteiligten untereinander Vereinbarungen treffen müssen. Statt dessen erkennen die Beteiligten die European Bridge-CA als vertrauenswürdige Vermittlungsinstanz an.

Die Teilnahme an der European Bridge-CA ist einfach und unkompliziert.

Grundvoraussetzung ist eine bereits vorhandene Public-Key Infrastruktur (PKI). Dabei sind eigene Public-Key Infrastrukturen oder auch Zertifikate, die durch öffentliche Trust Center ausgestellt werden, zulässig. Die Aufnahme in die European Bridge-CA erfolgt nach Unterzeichnung einer Teilnehmererklärung und Durchführung eines anwendungsorientierten Interoperabilitätstests. Im Anschluss entscheidet ein Gremium (Board), das sich aus Teilnehmern der European Bridge-CA zusammensetzt, über die endgültige Aufnahme.

Dieses Dokument beschreibt die EB-CA-Prozesse:

1. Vorbereitung
2. Interoperabilitätstest
3. Registrieren einer PKI zur Teilnahme an der EB-CA
4. Vertrauenswürdige Bereitstellung von Root-/CA-Zertifikaten
5. Vertrauenswürdige Bereitstellung von Mitarbeiterzertifikaten
6. Sicherer E-Mail-Verkehr zwischen EB-CA-Teilnehmerorganisationen
7. Veränderungen bei registrierten Root Zertifikaten
8. Beendigung der Teilnahme an der EB-CA

Diese Version der Prozessbeschreibung stellt die gegenwärtige Realisierung des Dienstes dar. Weiterentwicklungen sind möglich und würden zu gegebener Zeit in einer aktuelleren Version dokumentiert werden.

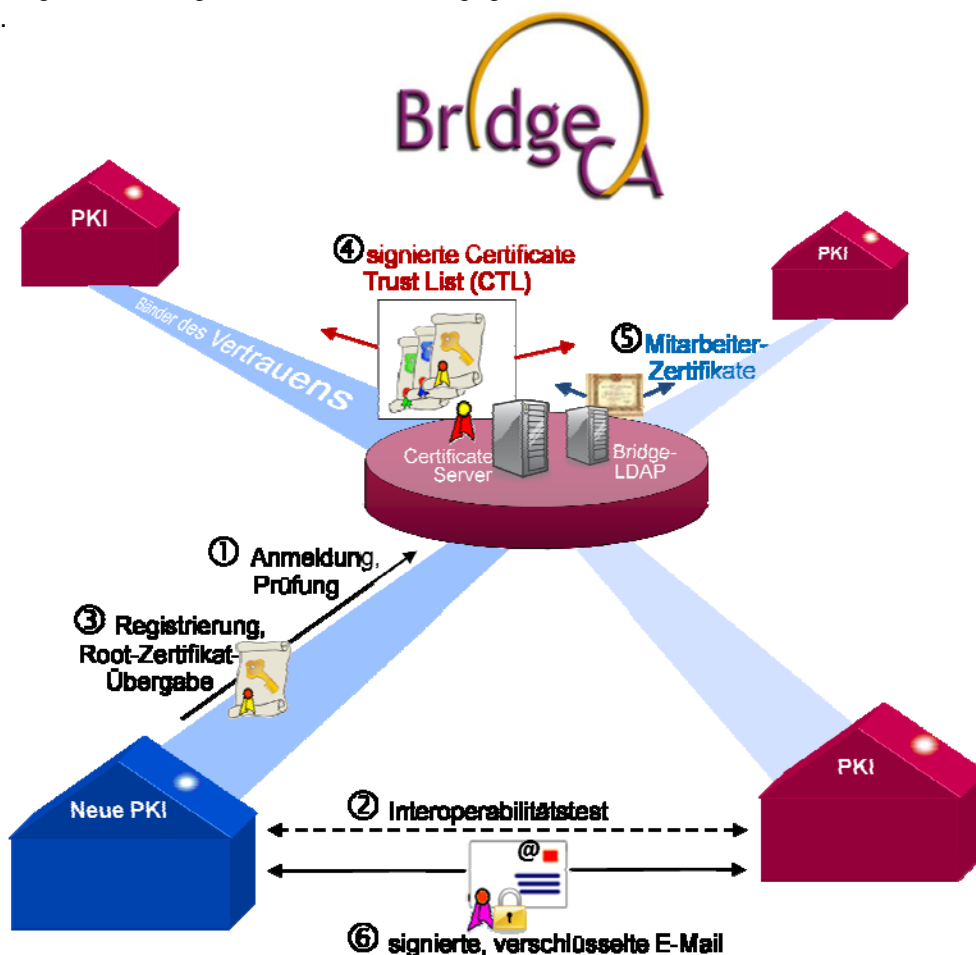


Bild 1: Übersicht zum EB-CA –Anmeldeprozess und -Verteildienst

## 1 Vorbereitung, Anmeldung

Eine zukünftige neue Teilnehmerorganisation (Unternehmen, Behörde oder Institutionen)

- **erhält** vom EB-CA-Betreiber TeleTrust folgende Unterlagen zur Information (① in Bild 1):
  - EBCA-Satzung.pdf <sup>1)</sup>
  - EBCA-Preisliste.pdf <sup>1)</sup>
  - EBCA-Selbsterklärung.pdf <sup>1)</sup>
  - EBCA-Certificate-Policy.pdf (CP) <sup>1)</sup>
  - EBCA-Registrierung-Deregistrierung.pdf <sup>1)</sup>
  - EBCA-Prozessbeschreibung.pdf (dieses Dokument) <sup>1)</sup>
  - EBCA-Teilnehmervertrag.pdf (auch Kooperationsvertrag genannt) <sup>2)</sup>
- und **gibt** TeleTrust erforderliche Informationen über die eigene PKI, die eigenen Zertifikate und benennt Ansprechpartner.

## 2 Interoperabilitätstest

Notwendige technische Voraussetzungen an eine neue EB-CA-Teilnehmerorganisation sind

- das Vorhandensein einer eigenen Public Key Infrastructure (PKI), die gewisse Mindeststandards der EB-CA-Zertifikatsrichtlinien erfüllt,
- mit **X.509**-Standard (ITU-T-Standard für eine PKI)
- und mit Signatur und Verschlüsselung von E-Mails im **S/MIME**-Format (Secure / Multipurpose Internet Mail Extensions).

Die Teilnahme bei der European Bridge-CA setzt die Durchführung eines Interoperabilitätstests voraus.

Zur Vermeidung von zeitaufwendigen "Jeder-gegen-Jeden"-Tests werden regelmäßig zwei Testreferenzen benannt (z.B. Siemens AG und BSI). Neue Mitglieder testen ihre Anwendungen dann gegen diese Testreferenzen (② in Bild 1). Am Ende der Tests erhält dann die European Bridge-CA und das neue Mitglied von den Testreferenzen ein ausführliches Protokoll. Sollten dann noch Interoperabilitätsprobleme existieren, können diese geklärt und mit Hilfe der Technischen Arbeitsgruppe der EB-CA geklärt werden.

Um die gewünschte Kompatibilität der jeweiligen Public Key Infrastruktur (PKI) zu erreichen, muss der neue Teilnehmer die aufgrund der Ergebnisse des Tests erforderlichen technischen und organisatorischen Anpassungen vornehmen. Weiterhin muss die Bereitschaft zur Anpassung der Komponenten bestehen, falls dies für die EB-CA aus Gründen der Interoperabilität, der technischen Fortentwicklung oder anderer Anforderungen erforderlich wird. Für die Teilnahme an der EB-CA ist es unbedingt erforderlich, dass der durchgeführte Interoperabilitätstest erfolgreich verlaufen ist. TeleTrust kann die Registrierung ablehnen, wenn die Konformität nicht durch den Test nachgewiesen ist.

(Anm.: Da in der Praxis keine 100 %-ige Interoperabilität mit allen Teilnehmern getestet werden kann, wäre das Testverfahren mit 3 Teilnehmern eigentlich als „Konformitätstest“ zu bezeichnen, der aber in etwa eine 95%-ige Interoperabilitätsgewissheit liefert.)

<sup>1)</sup> auch über <https://www.bridge-ca.org> → Services → Downloads verfügbar

<sup>2)</sup> bei Anmeldung oder auf Anfrage

### 3 Registrieren einer PKI zur Teilnahme an der EB-CA

Die eigentliche Registrierung zur Teilnahme an der European Bridge-CA wird durch den EB-CA-Betreiber TeleTrust (als Registrierungsstelle = Registration Authority (RA) ) selbst vorgenommen.

Adresse: TeleTrust Deutschland e.V.  
Chausseestraße 17  
10115 Berlin  
Telefon: +49 30 / 40 05 43 10  
Fax: +49 30 / 40 05 43 11  
E-Mail: registrierung@bridge-ca.org



Die erstmalige Registrierung erfordert eine sichere Übergabe der Anmeldedokumente bei der die Legitimation und Authentizität des Vertreters der neuen PKI durch TeleTrust geprüft und beglaubigt werden kann (z.B. durch Personalausweis oder durch ein unterschriebenes, beglaubigtes Mandat). Die Registrierung wird vorzugsweise in den Geschäftsräumen von TeleTrust vorgenommen, ist aber nach entsprechender Absprache auch an anderen Orten oder nach vorangegangenen persönlichen Kontakten auch mittels signierter, verschlüsselter Datenübertragung möglich.

Die Registrierung erfolgt in folgenden Schritten (③ in Bild 1):

- TeleTrust und die neue EB-CA-Teilnehmerorganisation (im folgenden kurz „neuer Teilnehmer“ genannt) schließen einen **Kooperationsvertrag** ab, in dem insbesondere Rechte und Pflichten der Zusammenarbeit aber auch z.B. die Kündigungsbedingungen geregelt sind. Beide Vertragsparteien erhalten je ein unterschriebenes Exemplar des Kooperationsvertrages (EBCA-Teilnehmervertrag.pdf).
- Der neue Teilnehmer übergibt an TeleTrust eine ausgefüllte **Selbsterklärung** (EBCA-Selbsterklärung.pdf), in der die Einhaltung gewisser Mindest-Qualitäts- und -Sicherheitsstandards für den Betrieb der eigenen PKI und der eigenen Sicherheits-Policy (gemäß EBCA-Certificate-Policy.pdf) zugesichert wird. Auf dieser Grundlage versichert der EB-CA-Betreiber den anderen EB-CA-Teilnehmern, dass sie dem neuen Teilnehmer sicherheitsmäßig vertrauen können, ohne dass sie das selbst nochmals überprüfen müssten (Bridge-CA-Prinzip).
- Der neue Teilnehmer übergibt an TeleTrust die ausgefüllten **Registrierungsformulare** (EBCA-Registrierung-Derregistrierung.pdf) zur Registrierung der PKI und Registrierung eines Zertifikats.
- Der neue Teilnehmer übergibt an TeleTrust :
  - **Root-Zertifikat** (X.509-Zertifikat im der- oder cer-Format) sowie die zugehörige Policy und/oder CPS (im doc oder pdf Format) auf einem digitalen Datenträger. Zwar muss ein Policy-Dokument zum Nachweis einer ordentlich geführten PKI vorliegen, jedoch werden die Inhalte der gelieferten Policies nicht kontrolliert (insb. nicht durch aufwendige Audits). Die EB-CA übernimmt deshalb keine rechtliche Gewähr für die Einhaltung der Policies der neuen Roots. An diese Stelle tritt die Selbsterklärung des neuen Teilnehmers mit dessen Gewährleistung.
  - **Sub-CA-Zertifikate** (im der- oder cer-Format) zum erforderlichen Schließen der Zertifikatskette.
  - **Mitarbeiterzertifikate** der benannten Ansprechpartner, damit mit diesen künftig signierte und verschlüsselte E-Mails ausgetauscht werden können.
- Der legitimierte Ansprechpartner des neuen Teilnehmers erhält im Gegenzug von TeleTrust das European Bridge-CA **Signierzertifikat** (auf sicherem Wege, vorzugsweise auf einem digitalen Datenträger). Das EB-CA Signierzertifikat inklusive Fingerprint ist vom Ansprechpartner an die Administration der neuen Teilnehmer-PKI weiterzugeben.

## 4 Vertrauenswürdige Bereitstellung von Root-/CA-Zertifikaten

### 4.1 Root-Zertifikate

Nach erfolgter Registrierung wird das Root-Zertifikat der neuen Teilnehmerorganisation (im .cer-Format) in die **Certificate Trust List** (CTL) der EB-CA aufgenommen. Die CTL ist als PKCS#7-Container im p7b-Format angelegt, aus dem sich alle Root-Zertifikate direkt in Zertifikatsverzeichnisse installieren lassen. Die EB-CA signiert die CTL zur Sicherung der Authentizität und Integrität mit einem Signierzertifikat, das T-Systems/TeleSec als Certificate Authority (CA) der EB-CA ausgestellt hat. Durch diese Signatur bestätigt die EB-CA die Herkunft der Zertifikate und die Einhaltung des geforderten Sicherheitsniveaus durch die Teilnehmer.

a) Die signierte CTL wird mittels einer signierten und verschlüsselten E-Mail direkt an die benannten Ansprechpartner der Teilnehmerorganisationen geschickt und damit auch an den Ansprechpartner der neu hinzugekommenen Teilnehmerorganisation (④ in *Bild 1*).

b) Außerdem wird die signierte CTL auf einem Web-Server öffentlich und kostenlos zum Download bereitgestellt (ebenfalls ④ in *Bild 1*). Dort ist die CTL unter

[https://www.bridge-ca.org/html/ct\\_liste.html](https://www.bridge-ca.org/html/ct_liste.html) (SSL-Link) oder

[http://www.bridge-ca.org/html/ct\\_liste.html](http://www.bridge-ca.org/html/ct_liste.html) oder

[http://www.bridge-ca.de/html/ct\\_liste.html](http://www.bridge-ca.de/html/ct_liste.html) oder

[http://www.bridge-ca.com/html/ct\\_liste.html](http://www.bridge-ca.com/html/ct_liste.html)

jederzeit für jedermann erreichbar.

c) Später wäre als dritter Verteilweg denkbar, das sich jeder PC-Nutzer, Bürger, kleiner oder mittlerer Betrieb ohne eigene PKI und ohne besondere IT-Kenntnisse, alle EB-CA-Root-Zertifikate gleichzeitig durch einfachen Download eines Browser-Add-ons in den Zertifikatsspeicher auf seine Festplatte laden kann. Ein Pilotprojekt für diesen Certificate Download Service (CDS) läuft zur Zeit.

Die Erstellung, Signierung, Bereitstellung und Verteilung der CTL wird durch die EB-CA-Administration erbracht. Derzeit wird dieser Dienst von TeleTrusT (in Berlin) geleistet. Das qualifizierte EB-CA-Signierzertifikat (von TeleSec) befindet sich auf einer SmartCard, die unter Verschluss aufbewahrt wird und ausschließlich zur CTL-Signierung auf einem speziellen PC, der nach der Neuinstallation noch nie mit einem LAN und noch nie mit dem Internet verbunden war, eingesetzt.

Später wäre es auch denkbar, dass diese Signieraufgabe unmittelbar durch T-Systems/TeleSec oder einem anderen beauftragten, vertrauenswürdigen Betreiber in sicherer Rechenzentrum-Betriebsumgebung erledigt wird.

### 4.2 CA-Zertifikate (Sub-Root-Zertifikate)

Zum Schließen der Vertrauenskette zwischen einem Mitarbeiterzertifikat und dem Root-Zertifikat sind meist noch Zwischenzertifikate (Sub-Root-Zertifikate, CA-Zertifikate) erforderlich. Die Teilnehmerorganisationen der EB-CA sind nicht unbedingt verpflichtet, alle ihre existierenden Zwischenzertifikate über den EB-CA-Dienst verteilen zu lassen. Das ist auch technisch nicht unbedingt erforderlich, weil die Zwischenzertifikate meist bereits vom E-Mail-Client automatisch einer signierten E-Mail beigefügt werden. Wenn aber eine Teilnehmerorganisation das gerne möchte und der EB-CA-Administration die Zwischenzertifikate auf sicherem Wege (z.B. als Anhang in einer verschlüsselten E-Mail) zur Verfügung stellt, dann veröffentlicht die EB-CA auch diese Zwischenzertifikate. Dazu werden die Sub-Root-Zertifikate zunächst in einer zip-Datei gesammelt und diese anschließend mit dem EB-CA-Zertifikat signiert und die signierte „Sub-CA Certificate List“ auf dem selben Web-Server, auf dem auch die CTL abgelegt ist (s.o.), öffentlich zum Download bereitgestellt.

### 4.3 Sperrliste

Eine Sperrliste (Certificate Revocation List, CRL) wird von der European Bridge-CA bisher aus folgenden Gründen noch nicht angeboten:

- Wenn ein registriertes Root-Zertifikat regulär abläuft, dann müssen das alle PKI-Anwendungen selbstständig erkennen. Deshalb wird in diesem Fall keine extra Informations-E-Mail an die Teilnehmerorganisationen verschickt. In der nächsten E-Mail, die ohnehin an alle teilnehmenden PKIen verschickt wird, um eine aktuelle Änderung bei den Registrierungen anzuzeigen, sind abgelaufene Zertifikate einfach nicht mehr enthalten. Außerdem wäre das reguläre Ende der Gültigkeitsdauer auch kein Grund, ein Root-Zertifikat auf eine Sperrliste zu setzen.
- Die EB-CA verwendet selbst z.Z. kein eigenes EB-CA-Root-Zertifikat, dessen vorzeitige Sperrung man notfalls über eine eigene CRL anzeigen müsste. Sollte das z.Z. eingesetzte T-Systems/TeleSec-Signierzertifikat einmal vorzeitig gesperrt werden müssen, dann gehörte es ohnehin nicht auf eine EB-CA-CRL, sondern eher auf eine TeleSec-CRL, aber die Gültigkeit des EB-CA-Signierzertifikats lässt sich ohnehin viel aktueller über den dazugehörigen OCSP-Responder von TeleSec online prüfen. Die technische Voraussetzung zur Gültigkeitsprüfung ist hier also (auch ohne CRL) optimal gegeben und die praktische Verantwortung für die Prüfung der Gültigkeit eines Zertifikats (ob mit CRL oder OCSP) liegt ohnehin bei den jeweiligen PKIen.
- Es ist bisher noch nie vorgekommen, dass ein Root-Zertifikat einer EB-CA-Teilnehmerorganisation vorzeitig gesperrt oder aus dem Verkehr gezogen werden musste. Falls dieser Fall doch einmal eintreite, dann würde die EB-CA dieses Zertifikat schnellstens entsprechend des in Kap. 7 beschriebenen Deregistrierungs-Prozesses aus der CTL entfernen und die Teilnehmer mittels einer aktuellen CTL informieren, aber keine EB-CA-CRL veröffentlichen. Die Verantwortung für die Veröffentlichung über eine CRL liegt bei der jeweils betroffenen Teilnehmerorganisation.

## 5 Vertrauenswürdige Bereitstellung von Mitarbeiter-Zertifikaten

### 5.1 Verzeichnisdienst

Die European Bridge-CA stellt über einen Verzeichnisdienst Mitarbeiterzertifikate (X.509-Zertifikate mit den öffentlichen Schlüsseln der Mitarbeiter) der EB-CA-Teilnehmerorganisationen zur Verfügung. ( ⑤ in *Bild 1*) Diese werden benötigt, um den betreffenden Mitarbeitern verschlüsselte E-Mails (im S/MIME-Format) schicken zu können.

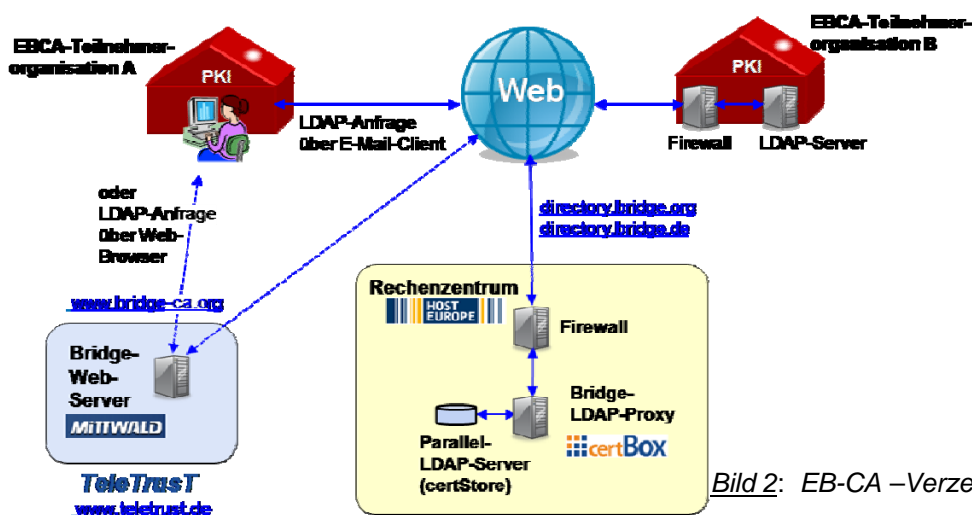


Bild 2: EB-CA – Verzeichnisdienst

Der EB-CA-Verzeichnisdienst arbeitet als LDAP-Proxy (s. *Bild 2*). D.h. er hält nicht selbst alle aktuellen Mitarbeiterzertifikate aller Teilnehmerorganisationen bereit, sondern hat eine Liste mit Links zu den LDAP-Servern der EB-CA-Teilnehmerorganisationen. Dem entsprechend leitet der LDAP-Proxy eine eingehende Anfrage (z.B. von Teilnehmerorg. A in *Bild 2*) an den entsprechenden richtigen LDAP-Server der angefragten Organisation (Teilnehmerorg. B in *Bild 2*) weiter. Dieser gibt dann das gewünschte Mitarbeiterzertifikat an den LDAP-Proxy zurück und dieser reicht es zurück an den ursprünglich Anfragenden (in Teilnehmerorg. A in *Bild 2*).

Falls eine EB-CA-Teilnehmerorganisation keinen eigenen LDAP-Server besitzt, kann sie ihre Mitarbeiterzertifikate auch per abgesicherten remote access auf einem Parallel-LDAP-Server (s. *Bild 2*) in der sicheren Umgebung des Rechenzentrums ablegen und hosten lassen.

Die Verantwortung für die Aktualität der Mitarbeiterzertifikate bleibt in jedem Fall bei den EB-CA-Teilnehmerorganisationen.

**E-Mail-Clients** (z.B. Outlook oder Thunderbird) können den EB-CA-Verzeichnisdienst selbsttätig unter dem Namen [dir.bridge-ca.org](http://dir.bridge-ca.org) abfragen, sofern er in ihrem Adresslistenverzeichnis eingetragen ist.

**Manuelle Abfragen** sind über die Webpage [http://www.bridge-ca.de/html/verz\\_dienst.html](http://www.bridge-ca.de/html/verz_dienst.html) möglich.

Wie schon die Root-/CA-Zertifikate werden auch die Mitarbeiterzertifikate öffentlich und kostenlos zur Verfügung gestellt. Alle EB-CA-Mitgliedsorganisationen sind gehalten, ihre Mitarbeiterzertifikate dem Verzeichnisdienst bereitzustellen, weil öffentliche Schlüssel sinnvollerweise auch öffentlich sein müssen, damit man sie zur Mail-Verschlüsselung verwenden kann.

Unredliche Mail-Adresslisten-Scans durch Spammer/Phisher sind nicht zu befürchten, weil ausschließlich Anfragen mit Eingabe einer vollständigen, richtigen geschriebenen, gültigen E-Mail-Adresse und einer zusätzlichen Capture-Eingabe mit dem dazugehörigen Mitarbeiterzertifikat beantwortet werden. Wild-Card-Abfragen (z.B. nach „\*@siemens.com“) werden dagegen grundsätzlich nicht beantwortet.

## 5.2 Validierungsdienst

Die EB-CA-Gemeinschaft hat sich z.Z. dafür ausgesprochen, für Mitarbeiterzertifikate keinen Validierungsdienst mittels OCSP-Responder (Online Certificate Status Protocol, OCSP) zu betreiben. Sie hält unter den gegebenen Umständen eine Gültigkeitsprüfung über Sperrlisten (Certificate Revocation List, CRL) für ausreichend, weil für die meisten Teilnehmer z.Z. die sichere E-Mail-Verschlüsselung im Vordergrund steht, für die man nicht notwendigerweise eine Validierung braucht.

Zur Handhabung der **Sperrlisten** (CRLs):

- **E-Mail-Clients** (z.B. Outlook oder Thunderbird) sollten normalerweise von Hause aus in der Lage sein, Sperrlisten (CRLs) automatisch vom LDAP-Server des Herausgebers anzufordern und zu prüfen, sofern der Herausgeber im Zertifikat einen entsprechenden Link zur CRL eingetragen hat.
- **Manuellen Anfragen** nach CRLs sind über die Webpage [http://www.bridge-ca.de/html/verz\\_dienst.html](http://www.bridge-ca.de/html/verz_dienst.html) folgendermaßen möglich: Nach Eingabe einer gültigen E-Mail-Adresse wird auf der Webpage nicht nur das gefundene Mitarbeiterzertifikat zum Download angeboten, sondern es werden hier auch die Pfadangaben zur CRL angezeigt, die im Zertifikat eingetragen sind. Alternativ könnte man sich auch direkt das zu prüfende Zertifikat öffnen und sich dann in *Zertifikatseigenschaften* → *Details* → *Sperrlisten-Verteilungspunkte* den Pfad zur CTL selbst auslesen. Über die URL gelangt man mit seinem Browser zur passenden CRL (im crl-Format). In der CRL sind die Seriennummern der gesperrten Zertifikate zusammen mit dem Sperrdatum aufgelistet. Man kann hier nachschauen, ob die Seriennummer des zu überprüfenden Zertifikats als gesperrt gelistet ist.

Eine gemeinsame EB-CA-Sperrliste, die alle Sperrlisten aller EB-CA-Teilnehmerorganisationen tagesaktuell enthält, gibt es nicht.

Die Verantwortung für die Aktualität der einzelnen CRLs liegt bei den ausstellenden PKLen.

Die Verantwortung für die Gültigkeitsprüfung der empfangenen Mitarbeiterzertifikate (verwendet als Signaturschlüsselzertifikate) liegt bei den Empfänger-PKLen.

Als **spätere Optionen** wäre bei entsprechender Nachfrage denkbar, dass

- über die EB-CA-Webpage nach Eingabe einer E-Mail-Adresse auch gleich die passende CRL zum Download angeboten wird oder
- alle vom den LDAP-Proxy gelieferten Mitarbeiterzertifikate vorher automatisch auf Gültigkeit geprüft werden und nur gültige Zertifikate (die weder abgelaufen sind noch auf einer Sperrliste stehen) ausgeliefert werden oder
- die EB-CA einen eigenen OCSP-Responder betreibt.

## 6 Sicherer E-Mail-Verkehr zwischen EB-CA-Teilnehmerorganisationen

Durch den oben beschriebenen vertrauensvollen Austausch von Root-/CA- und Mitarbeiter-Zertifikaten können Die EB-CA-Teilnehmerorganisationen untereinander sichere, **signierte** und **verschlüsselte** E-Mails austauschen (© in *Bild 1*).

Der EB-CA-Verbund wirkt 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.

## 7 Veränderungen bei registrierten Root-Zertifikaten

Wenn eine Veränderung an der Liste der registrierten Root-Zertifikate (CTL) eintritt (z.B. durch Neuzugang, Abgang, Zertifikatserneuerung oder Zertifikatssperrung), dann wird die CTL dem entsprechend aktualisiert, signiert und analog zum Verfahren bei Neuzugang (s. Kap.4.1) folgendermaßen neu verteilt:

**a)** Die signierte CTL (im PKCS#7-Format) wird mittels einer signierten und verschlüsselten E-Mail direkt an die benannten Ansprechpartner der Teilnehmerorganisationen geschickt (④ in *Bild 1*).

**b)** Außerdem wird die signierte CTL (im PKCS#7-Format) auf einem Web-Server mit SSL-Zertifikat unter der Domain [bridge-ca.org](http://bridge-ca.org) öffentlich und kostenlos zum Download bereitgestellt (ebenfalls ④ in *Bild 1*).

Die Teilnehmer-PKlen sind selbst verantwortlich, die jeweils aktuellen CTLs in ihr System einzupflegen.

Wenn **zusätzliche Root-Zertifikate** einer EB-CA-Mitgliedsorganisation aufgenommen werden, z.B. als Ersatz für alte, abgelaufene Zertifikate oder aufgrund einer veränderten PKI-Struktur oder –Hierarchie, dann ist keine erneute Aufnahmeprüfung (gem. Kap. 1 bis 3) erforderlich, denn die Authentizität und die Interoperabilität sind ja bereits bekannt. Es ist lediglich der hier beschriebene Aktualisierungs- und Verteilungsprozess anzuwenden.

Für **regulär abgelaufene Root-Zertifikate** wird dieser Prozess nicht in Gang gesetzt, da PKlen und E-Mail-Clients selbstständig erkennen, wenn die Gültigkeitsdauer eines Root-Zertifikats überschritten ist und darauf richtig reagieren. Abgelaufene Root-Zertifikate werden stillschweigend aus der CTL entfernt und sind dann bei der nächsten Verteilung aus wichtigen Anlass einfach nicht mehr enthalten.

Die **Abmeldung eines Root-Zertifikats** (bei Mitgliederaustritt) wird nicht gesondert hervorgehoben oder separat gemeldet. Die bei der EB-CA abgemeldeten Root-Zertifikate sind i.d.R. weiterhin gültig, werden lediglich aus der CTL entfernt und sind dann bei der nächsten Verteilung aus wichtigen Anlass einfach nicht mehr enthalten.

Die **Deregistrierung eines Root-Zertifikats** wird dann erforderlich, wenn es wg. Kompromittierung oder aus anderen schwerwiegenden Gründen gesperrt oder vor Ablauf der regulären Gültigkeit aus anderen Gründen nicht mehr verteilt werden soll. Dieser Fall ist sehr selten und bei der EB-CA noch nie vorgekommen. Wenn dieser Fall jedoch tatsächlich einmal eintritt, muss die betroffene Teilnehmerorganisation die Deregistrierung mit einem entsprechend ausgefüllten und unterschriebenen Formular per Fax an TeleTrusT melden (erhältlich bei der Registrierungsstelle (RA) TeleTrusT oder vom Webserver der EB-CA unter [www.bridge-ca.org](http://www.bridge-ca.org) . Mit einem Rückruf beim registrierten technischen Ansprechpartner wird die Rechtmäßigkeit der Deregistrierung überprüft. Danach erhalten alle teilnehmenden PKlen schnellstmöglich eine entsprechend bereinigte, signierte CTL . Die Teilnehmerorganisation, welche die Deregistrierung veranlasst hat, erhält von TeleTrusT eine entsprechende schriftliche Bestätigung. Die betroffene Organisation trägt selbst die Verantwortung dafür, ihr gesperrtes Root-Zertifikat auf eine eigene Sperrliste zu setzen und diese zu veröffentlichen.

Die EB-CA führt selbst keine Sperrliste für Root-Zertifikate. Wenn überhaupt, dann würde darauf nur ein eigenes gesperrtes EB-CA-Root-Zertifikat gehören, aber die EB-CA verwendet seit Oktober 2008 kein eigenes Root-Zertifikat mehr und braucht dem entsprechend auch keine eigene Sperrliste.

## **8 Beendigung der Teilnahme an der EB-CA**

Wenn eine Teilnehmerorganisation ihre Teilnahme bei der European Bridge-CA beenden möchte, dann kann der Kooperationsvertrag mit einer Frist von drei Monaten jederzeit gekündigt werden. In diesem Fall reicht eine ganz normale, schriftliche, fristgemäße Kündigung an den EB-CA-Betreiber TeleTrust (Registrierungsstelle). Nach dem Vertragsende werden die Zertifikate der ausgeschiedenen Organisation aus der CTL herausgenommen.