



## **Selbsterklärung** zur Teilnahme an der European Bridge-CA

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

## 1. Ziel

Der Verband TeleTrusT Deutschland e.V. stellt teilnehmenden Organisationen mit der European Bridge-CA (EB-CA) eine kostengünstige und verlässliche Dienstleistung bereit, 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 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.

## 2. Konformität

Um die notwendige Interoperabilität aller beteiligten Public Key Infrastructures (PKIs) zu gewährleisten, muss jede neu teilnehmende Organisation vor der Aufnahme an einem Konformitätstest teilnehmen. TeleTrusT kann die Registrierung ablehnen, wenn die Konformität nicht durch den Test nachgewiesen ist. Sollte sich im Ergebnis des Tests herausstellen, dass zur Interoperabilität noch technische oder organisatorische Anpassungen erforderlich sind, muss der neue Teilnehmer bereit sein, die entsprechenden Anpassungen vorzunehmen. Darüber hinaus muss auch später noch die Bereitschaft zur Anpassung von Komponenten bestehen, falls dies für die EB-CA-Gemeinschaft zur Aufrechterhaltung der Interoperabilität, z.B. infolge technischer Fortentwicklung oder anderer veränderter Anforderungen erforderlich wird. Die Anforderungen, die in der Anlage dargestellt sind, können durch TeleTrusT aktualisiert und überarbeitet werden. Umzusetzen ist die jeweils aktuelle Anlage. TeleTrusT informiert die Teilnehmer über derartige Veränderungen rechtzeitig und wird eine angemessene Frist für die Migration vorsehen.

## 3. Veröffentlichung

Die teilnehmende Organisation stimmt der Veröffentlichung ihrer Teilnahme an der EB-CA und der Veröffentlichung ihres Root-Zertifikats zu. Die teilnehmende Organisation erklärt außerdem ihr Einverständnis, die den Betrieb der PKI betreffenden Teile ihrer Certificate Policy (CP) oder ihres Certificate Practice Statements (CPS) sowohl TeleTrusT als Betreiber der EB-CA als auch den anderen teilnehmenden Organisationen zugänglich zu machen.

## 4. Identifikation

Die Nutzer der PKI müssen zuverlässig zu identifizieren sein. Der Charakter anderer Zertifikate (Server-, Rollen-, Organisations-Zertifikate) muss für die Empfänger eindeutig erkennbar sein. Ein als Pseudonym ausgestelltes Zertifikat muss als solches ebenfalls kenntlich sein.

## 5. Ordnungsgemäßer Betrieb

Die teilnehmende Organisation erbringt die Zertifizierungsdienstleistungen im Rahmen ihrer CP ordnungsgemäß und orientiert sich an dem aktuellen Stand der Technik. Dabei müssen die Mindestanforderungen der EB-CA (s. Anhang) für die eigene PKI umgesetzt sein. Begründete Abweichungen sind möglich.

## 6. Information im Fall einer Betriebseinstellung

Die teilnehmende Organisation zeigt die Beendigung ihrer Zertifizierungsdienstleistungen der EB-CA rechtzeitig an.

## 7. Deregistrierung

Der EB-CA-Gemeinschaft ist berechtigt, eine teilnehmende Organisation, die diese Mindestverpflichtungen nicht einhält, zu deregistrieren.

## 8. Entgelt

TeleTrust kann für die Dienstleistung des EB-CA-Betriebs ein Entgelt nehmen. Das Entgelt wird gesondert vereinbart.

.....  
Name der teilnehmenden Organisation

.....  
Unterschrift für die teilnehmende Organisation

.....  
Ort und Datum

## Anhang:

### Organisatorische und technische Anforderungen für die Teilnahme an der European Bridge-CA (EB-CA)

#### A) Anforderungen an eine teilnehmende PKI und deren Architektur

- Persönliche Identifikation und Registrierung des Zertifikatsinhabers
- Zugriff auf Rückruf-Daten seitens der EB-CA und dessen Teilnehmer (Certificate Revocation Lists (CRLs) in eigenen bzw. über replizierte Directories oder von einem Webserver abrufbar oder durch Einsatz eines OCSP-Servers)
- Bei der Vergabe von Namen (für Nutzer- oder PKI-Zertifikate) muss sichergestellt sein, dass die gewählten Domain Names (DNs) über alle beteiligten Infrastrukturen hinweg eindeutig sind.

#### B) Anforderungen an die zum Einsatz kommenden Zertifikate

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

Darüber hinaus ist es von Vorteil, wenn

- möglichst wenig Attribute des Zertifikats als ‚critical‘ angesehen werden.

#### C) Anforderungen an die CA-Produkte

- Grundsätzlich existieren keine zwingenden Anforderungen für die CA-Produkte, da sie nicht an dem Verteilungsprozess beteiligt sind.

#### D) Anforderungen an den PKI-Client

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