Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

TeleTrusT EBCA
European Bridge Certificate Authority

Selbsterklärung

zur Teilnahme an der
TeleTrusT European Bridge CA

Informationen zum Dokument

Version 2.7

26.02.2019

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
D-10115 Berlin

Tel. +49 30 / 400 54 310
Fax +49 30 / 400 54 311

info@ebca.de
http://www.ebca.de

Inhaltsübersicht

Historie

Ver-sion	Datum	Änderung	Autor
2.2	01.12.2010	Anpassung Begrifflichkeiten	Dr. Holger Mühlbauer
2.3	11.01.2012	Anpassung des Verbandsnamens	Dr. Holger Mühlbauer
2.4	08.02.2012	Anpassung Erscheinung, Anpassung Begrifflichkeiten	Marieke Petersohn
2.5	17.07.2014	Neues EBCA-Logo eingefügt	Martin Fuhrmann
2.6	28.06.2016	Inhaltliche Anpassung "Ort der PKI"	Marieke Petersohn
2.7	26.02.2019	Anpassung des Verbandsnamens	Morad Abou Nasser

1 Ziel

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) bietet Organisationen mit der "European Bridge CA" (EBCA) eine kostengünstige und verlässliche Gelegenheit, die gegenseitige Prüfung von Zertifikaten der teilnehmenden Unternehmen, Behörden und Institutionen zu ermöglichen. 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. Stattdessen erkennen die Beteiligten die European Bridge CA als vertrauenswürdige Vermittlungsinstanz an.

2 Interoperabilität

Um die notwendige Interoperabilität aller beteiligten Public Key Infrastrukturen (PKIen) zu gewährleisten, muss jede neu teilnehmende Organisation vor der Aufnahme an einem Interoperabilitätstest 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 EBCA-Gemeinschaft zur Aufrechterhaltung der Interoperabilität, z.B. infolge technischer Fortentwicklung oder anderer veränderter Anforderungen erforderlich wird. TeleTrusT kann die Anforderungen, die in der Anlage dargestellt sind, aktualisieren und überarbeiten. 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 EBCA und der Veröffentlichung in ihrer Kontrolle befindlichen Root- und Sub-CA-Zertifikate als Vertrauensanker zu. Änderungen der Root-CA und Sub-CA-Zertifikate (Ablaufen/Erneuerung) sind der EBCA unmittelbar mitzuteilen. 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 EBCA 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 EBCA (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 EBCA rechtzeitig an.

7 Deregistrierung

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

8 Zuwendungen

TeleTrusT kann für die Dienstleistung des EBCA-Betriebs Zuwendungen empfangen, die gesondert vereinbart werden.

.....,	.....,
Datum, Ort	Datum, Ort
.....	.....
Bundesverband IT-Sicherheit e.V. (TeleTrusT)	Teilnehmende Organisation

Anhang

Organisatorische und technische Anforderungen für die Teilnahme an der European Bridge CA (EBCA):

A) 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)
- 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.
- Die PKI muss in Europa (EU + EFTA) betrieben werden. Abweichungen bei Teilnehmern, die die PKI von einem professionellen Trustcenter betreiben lassen, sind möglich und erfordern eine Zustimmung des EBCA-Lenkungsgremiums. Bezugspunkt für eine Entscheidung ist der Betriebsstandort für die EBCA-relevante Root- bzw. Sub-CA.

B) Anforderungen an die zum Einsatz kommenden Zertifikate

- Die Zertifikate sind konform zum Standard X.509v3
- Der Private Key ist ein Schlüssel mit einer Schlüssellänge nach aktuellem Stand der Technik gemäß Algorithmen-Katalog der Bundesnetzagentur, wie im Bundesanzeiger jeweils jahresaktuell veröffentlicht
- 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.