DFN-PKI

Erklärung zum Zertifizierungsbetrieb der DBTG-CA in der DFN-PKI

- Sicherheitsniveau: Global -

Deutscher Bundestag

CPS der DBTG-CA

Version 1.5

März 2010

1 Einleitung

Die DBTG-CA ist eine Zertifizierungsstelle des DFN-Anwenders Deutscher Bundestag innerhalb der DFN-PKI. In der DFN-PKI wird eine Zertifizierungshierarchie verwendet, bei der das Zertifikat der DBTG-CA von der DFN-PCA ausgestellt wird.

Für den Betrieb der DBTG-CA gelten die folgenden Dokumente:

- CP der DFN-PKI: "Zertifizierungsrichtlinie der DFN-PKI – Sicherheitsniveaus: Global, Classic und Basic -", Version 2.2, April 2009, OID 1.3.6.1.4.1.22177.300.1.1.5.2.2
- CPS der DFN-PCA: "Erklärung zum Zertifizierungsbetrieb der obersten Zertifizierungsstelle der DFN-PKI – Sicherheitsniveaus: Global, Classic und Basic -", Version 2.1, Dezember 2006, OID 1.3.6.1.4.1.22177.300.2.1.5.2.1

Die vom CPS der DFN-PCA abweichenden Regelungen für die DBTG-CA sind in Kapitel 3 dieses Dokuments beschrieben.

Die DBTG-CA stellt ausschließlich Zertifikate im Sicherheitsniveau "Global" aus.

2 Identifikation des Dokuments

- Titel: "Erklärung zum Zertifizierungsbetrieb der DBTG-CA in der DFN-PKI"
- Version: 1.5

3 Abweichungen vom CPS der DFN-PCA

Nachfolgend sind die Abschnitte des CPS der DFN-PCA aufgeführt, in denen für die DBTG-CA abweichende Regelungen getroffen werden.

Zu CPS der DFN-PCA: "1.3.1 Zertifizierungsstellen"

Die Anschrift der DBTG-CA lautet:

Deutscher Bundestag	Telefon: +49 30 277-35081
Referat IT 5	Telefax: +49 30 227-36458
DBTG-CA	
11011 Berlin	WWW: www.bundestag.de
GERMANY	

Zu CPS der DFN-PCA: "1.3.2 Registrierungsstellen"

Die ausgezeichnete Registrierungsstelle für die zuvor genannte Zertifizierungsstelle befindet sich in den Räumen der DBTG-CA.

Darüber hinaus sind keine weiteren Registrierungsstellen verfügbar.

Zu CPS der DFN-PCA: "1.5.1 Organisation"

Die Verwaltung dieses CPS erfolgt durch die in Abschnitt 1.3.1 genannte Einrichtung.

Der Betrieb der DBTG-CA erfolgt durch:

DFN-Verein	Telefon: +49 30 884299-955
Alexanderplatz 1	E-Mail: pki@dfn.de
10178 Berlin	WWW: www.pki.dfn.de
GERMANY	

Zu CPS der DFN-PCA: "1.5.2 Kontaktperson"

Die verantwortliche Person für das CPS der DBTG-CA ist:

Deutscher Bundestag	Angela Brückner
Referat IT 5	Telefon: +49 30 277-35088
DBTG-CA	
Platz der Republik 1	Telefax: +49 30 227-36458
11011 Berlin	E-Mail: vorzimmer.it5@bundestag.de
GERMANY	

Zu CPS der DFN-PCA: "2.2 Veröffentlichung von Informationen"

Alle gemäß CP, Abschnitt 2.2, erforderlichen Informationen werden bereitgestellt unter:

http://www.pki.dfn.de/teilnehmer

Zu CPS der DFN-PCA: "3.1.1 Namensform"

Die DNs aller Zertifikatnehmer unterhalb der DBTG-CA enthalten die Attribute "C=DE" und "O=Deutscher Bundestag".

Optional können die Attribute "ST=Berlin" und "L=Berlin" aufgenommen werden.

Das variable Attribut "OU=<Organisationseinheit>" muss mindestens einmal angegeben werden.

Das optionale Attribut "UID=<Benutzername>" kann einmalig vorhanden sein und enthält die eindeutige Benutzerkennung des Zertifikatnehmers aus dem zentralen Verzeichnisdienst des Deutschen Bundestages.

Wenn eine E-Mail Adresse angegeben wird, so kann diese über das Attribut "emailAddress" in den Namen aufgenommen werden. Die E-Mail Adresse sollte allerdings bevorzugt in der Zertifikaterweiterung "subjectAlternativeName" aufgenommen werden.

Damit entspricht der Name jedes Zertifikatnehmers dem folgenden Schema:

C=DE

[ST=Berlin

L=Berlin]

O=Deutscher Bundestag

OU=<Organisationseinheit>

CN=<Eindeutiger Name>

[UID=<Benutzername>]

[emailAddress=<E-Mail Adresse>]

Zu CPS der DFN-PCA: "3.2.3. Authentifizierung einer natürlichen Person"

Gemäß Kapitel 3.2.3. Absatz b) der DFN-PKI Zertifizierungsrichtlinie wird die Authentifizierung einer natürlichen Person durch den Polizei- und Sicherungsdienst des Deutschen Bundestages vorgenommen.

Zu CPS der DFN-PCA: "4.1.1 Wer kann ein Zertifikat beantragen"

Die DBTG-CA bietet ihre Dienstleistungen allen Abgeordneten des Deutschen Bundestages, deren Mitarbeitern, allen Mitarbeitern der Verwaltung des Deutschen Bundestages, allen Mitarbeitern der Fraktionen des Deutschen Bundestages sowie im Auftrag des Deutschen Bundestages handelnden Personen an.

Zu CPS der DFN-PCA: "4.1.2 Registrierungsprozess"

Um ein Zertifikat zu erhalten, sind zwei verschiedene Abläufe möglich. Entweder wird das Original eines ausgefüllten und unterschriebenen Papierantrages bei der Registrierungsstelle abgegeben oder es wird über ein Auftragsmanagement (Call-Verfahren) ein Auftrag bei der Registrierungsstelle ausgelöst. In beiden Fällen sind folgende Voraussetzungen notwendig:

- Der Zertifikatnehmer muss einen aktivierten Eintrag sowie eine E-Mail-Adresse im zentralen LDAP-Verzeichnisdienst des Deutschen Bundestages besitzen,
- der Zertifikatnehmer verfügt über einen vom Polizei- und Sicherungsdienst des Bundestages ausgestellten Hausausweis.

Zu CPS der DFN-PCA: "4.4.2 Veröffentlichung des Zertifikates"

Die DBTG-CA veröffentlicht die gemäß Zertifizierungsrichtlinie der DFN-PKI geforderten Zertifikate über die im Kapitel 2.2 angegebenen Informationssysteme.

Ausgewählte Zertifikate, z.B. für Abgeordnete und Vorzimmer der Verwaltung werden nur dann in eigenen Informationssystemen durch die DBTG-CA veröffentlicht, wenn es sich um Zertifikate für die Signierung und Verschlüsselung von E-Mails handelt. Zertifikate für andere Einsatzzwecke werden aus it-sicherheitsrelevanten Aspekten nicht veröffentlicht.

Die veröffentlichten Zertifikate sind unter dem Link

`http://adressbuch.bundestag.de/adressbuch`

und allgemeine Informationen sowie die CA-Zertifikate unter

`http://www.bundestag.de/mdb/emailzertifikat/index.html`

abrufbar.

Zu CPS der DFN-PCA: "4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung"

Die DBTG-CA bietet eine Schlüsselhinterlegung von privaten Schlüsseln an, wenn die privaten Schlüssel auf Systemen der ausgezeichneten RA generiert wurden. Diese Möglichkeit gilt jedoch nur für E-Mail-Zertifikate und Zertifikate für die Dateiverschlüsselung, nicht aber für Signatur-, Authentifizierungs- und Serverzertifikate.

Bei der Schlüsselhinterlegung wird ein Backup des verschlüsselten privaten Schlüssels auf einem internen Datenbank-Server hinterlegt, der sich in den Liegenschaften des Deutschen Bundestages befindet. Die Verschlüsselung des Backups wird über ein Key-Backup-Zertifikat, das mit einer PIN belegt ist, realisiert.

Der Zugriff auf den in der Datenbank befindlichen verschlüsselten privaten Schlüssel des Zertifikatnehmers kann nur im vier Augen-Prinzip erfolgen. Ein autorisierter Mitarbeiter der DBTG-CA (CAO1) ist im Besitz des Tokens auf dem sich das Key-Backup-Zertifikat befindet. Die PIN des Key-Backup-Zertifikates ist nur einer verantwortlichen Person der DBTG-CA (PIN-Geber (CAO2)) bekannt und ist, wie auch das Zertifikat, in je einem Safe hinterlegt. Ein Zugriff auf das verschlüsselte Backup durch einzelne Personen ist damit ausgeschlossen.

Die Schlüsselwiederherstellung erfolgt in Form einer PIN-geschützten p12-Datei (PKCS#12 Standard), die den privaten Schlüssel und mehrere Zertifikate enthält, sowie eines neuen nicht einsehbaren PIN-Briefes. Die Übermittlung des Backups des privaten Schlüssels an den Zertifikatnehmer erfolgt wie in Punkt 6.1.2 beschrieben.

Ein Key-Recovery ist nur auf Grundlage eines schriftlichen Antrages des Zertifikatsnehmers vorzunehmen.

Für den Umgang mit Signatur- und Authentifizierungszertifikaten, die auf Krypto-Geräten generiert wurden, gelten die folgenden Regelungen:

- Der private Schlüssel wird nicht in der DBTG-CA hinterlegt.
- Die DBTG-CA speichert lediglich die PUK (Personal Unblocking Key) für den Zugriff auf das Krypto-Gerät.

- Der Zugriff auf die in der Datenbank hinterlegte verschlüsselte PUK des Krypto-Gerätes kann nur im vier Augen-Prinzip erfolgen. Autorisierte Mitarbeiter der DBTG-CA sind im Besitz eines Krypto-Gerätes auf dem sich das PIN-Reset-Zertifikat befindet. Die PIN des PIN-Reset-Zertifikates ist nur anderen autorisierten Personen der DBTG-CA (PIN-Geber) bekannt. PIN bzw. Krypto-Gerät für bzw. mit dem PIN-Reset-Zertifikate sind in je einem Safe hinterlegt, zu dem nur die jeweils für den Zugriff darauf autorisierten Mitarbeiter Zugang haben. Ein Zugriff auf die verschlüsselte PUK durch einzelne Personen ist damit ausgeschlossen.
- Die Zugriffswiederherstellung auf ein gesperrtes Krypto-Gerät erfolgt nach dessen Vorlage bei der DBTG-CA durch Generierung eines neuen nicht einsehbaren PIN-Briefes.
- Der Verlust, Diebstahl oder Defekt eines Gerätes ist unverzüglich vom Benutzer anzuzeigen. Daraufhin wird durch die Mitarbeiter der DBTG-CA die sofortige Sperrung der Zertifikate veranlasst.

Zu CPS der DFN-PCA: "5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen" und "6 Technische Sicherheitsmaßnahmen"

Die DBTG-CA wird durch den DFN-Verein im Auftrag des DFN-Anwenders Deutscher Bundestag bei der DFN-PCA betrieben. Daher sind für die DBTG-CA dieselben infrastrukturellen, organisatorischen, personellen und technischen Sicherheitsmaßnahmen umgesetzt, wie für die DFN-PCA (siehe CPS der DFN-PCA).

Zu CPS der DFN-PCA: "6.1.1 Schlüsselerzeugung"

Das kryptographische Schlüsselpaar für Benutzer- und Serverzertifikate wird softwaremäßig in der Registrierungsstelle generiert. Die Systeme der RA befinden sich in Liegenschaften des Deutschen Bundestages und sind mit einem PIN-geschützten RA-Zertifikat gesichert. Das RA-Zertifikat ist auf einem Token mit Smartcard hinterlegt und nur Mitarbeitern der DBTG-CA (CAO1) zugänglich, ebenso wie die PIN. Bei Nichtgebrauch wird das Token im Safe aufbewahrt.

Schlüssel für Serverzertifikate können auch beim Zertifikatnehmer erzeugt werden.

Bei der Verwendung von Krypto-Geräten erfolgt die Generierung des privaten und öffentlichen Schlüssels für die Signatur- und Authentifizierungszertifikate direkt auf dem PIN-geschützten Krypto-Gerät.

Zu CPS der DFN-PCA: "6.1.2 Übermittlung des privaten Schlüssels an den Zertifikatnehmer"

Die Übermittlung des privaten Schlüssels an den Zertifikatnehmer erfolgt per E-Mail in einer PIN-geschützten P12-Datei (PKCS#12 Standard). Die E-Mail wird nur auf internen Systemen (Intranet) des Deutschen Bundestages mit internen E-Mail-Adressen versendet. Der entsprechende verschlossene PIN-Brief wird persönlich an den Benutzer ausgehändigt. Er wird nur einmal generiert und ist nicht einsehbar. Die PIN-Briefe sind so ausgestaltet, dass eine Offenlegung der geschützten PIN durch unbefugte Dritte erkannt werden kann, da hierbei Teile des PIN-Briefschutzes irreparabel zerstört werden.

Falls der private Schlüssel von der DBTG-CA auf einem Krypto-Gerät generiert wurde, erfolgt die Übergabe des PIN-geschützten Krypto-Gerätes sowie die Auslieferung des verschlossenen PIN-Briefes an den Benutzer persönlich und gegen Quittung. Für die Gestaltung der einmalig erzeugten PIN-Briefe gelten die o.g. Merkmale.

Zu CPS der DFN-PCA: "6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren"

Die durch die DBTG-CA ausgestellten Serverzertifikate haben standardmäßig eine Laufzeit von fünf Jahren, die Nutzerzertifikate von drei Jahren.