DFN-PKI

Erklärung zum Zertifizierungsbetrieb der TUB CA in der DFN-PKI

- Sicherheitsniveau: Global -

Technische Universität Berlin

CPS der TUB CA

V1.3

20.07.2010

1 Einleitung

Die TUB CA ist eine Zertifizierungsstelle des DFN-Anwenders Technische Universität Berlin innerhalb der DFN-PKI. In der DFN-PKI wird eine Zertifizierungshierarchie verwendet, bei der das Zertifikat der TUB CA von der DFN-PCA ausgestellt wird.

Für den Betrieb der TUB 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 TUB CA sind in Kapitel 3 dieses Dokuments beschrieben.

Die TUB CA stellt ausschließlich Zertifikate im Sicherheitsniveau "Global" aus.

2 Identifikation des Dokuments

- Titel: "Erklärung zum Zertifizierungsbetrieb der TUB CA in der DFN-PKI"
- Version: 1.3

3 Abweichungen vom CPS der DFN-PCA

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

Zu CPS der DFN-PCA: "1.3.1 Zertifizierungsstellen"

Die Anschrift der TUB CA lautet:

Technische Universität Berlin	Telefon: +49 30 314-0
Zentrales IT-Dienstleistungszentrum (tubIT)	Telefon: +49 30 314-22703
	Telefax: +49 30 314-21060
Trustcenter	
Einsteinufer 17	E-Mail: ca@TU-Berlin.DE
10587 Berlin	WWW: http://ca.tu-berlin.de/
GERMANY	

Zu CPS der DFN-PCA: "1.3.2 Registrierungsstellen"

Die ausgezeichneten Registrierungsstellen für die zuvor genannten Zertifizierungsstellen befinden sich in den Räumen der TUB 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 TUB CA erfolgt durch:

DFN-Verein	Telefon: +49 30 884299-955
Alexanderplatz 1	Telefax: +49 30 884299-70
10178 Berlin	E-Mail: pki@dfn.de
GERMANY	WWW: www.pki.dfn.de

Zu CPS der DFN-PCA: "1.5.2 Kontaktperson"

Die verantwortliche Person für das CPS der TUB CA ist:

Technische Universität Berlin	Gerd Schering
Zentrales IT-Dienstleistungs-zentrum (tubIT)	Telefon: +49 30 314-24383
Trustcenter	
Einsteinufer 17	Telefax: +49 30 314-21060
10587 Berlin	E-Mail: ca@TU-Berlin.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 TUB CA enthalten die Attribute "`C=DE`" und "`O=Technische Universitaet Berlin`".

Das optionale Attribut "`OU=<Organisationseinheit>`" kann mehrfach angegeben werden.

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.

Es werden verschiedene Namensformen verwendet. Die folgenden Schemata sind zulässig (Optionale Attribute werden in eckigen Klammern angegeben. Spitze Klammern symbolisieren Platzhalter.):

1. Zertifikate für Registrierungsstellen, Server und sonstige Zwecke:

   C=DE

   [ST=Berlin

   L=Berlin]

   O=Technische Universitaet Berlin

   [OU=<Organisationseinheit>]

   CN=<Eindeutiger Name>

   [emailAddress=<E-Mail Adresse>]

2. Zertifikate für die Verschlüsselung, gespeichert auf PKI-Token:

   C=DE

   O=Technische Universitaet Berlin

   serialNumber=<Unterscheidende Nummer>

   CN=<Vorname Name>

3. Zertifikate für die Authentifizierung, gespeichert auf PKI-Token:

   C=DE

   O=Technische Universitaet Berlin

   serialNumber=<Unterscheidende Nummer>

   CN=PN:<TU Berlin ID> (Portalzugang)

4. Zertifikate für die Signatur, gespeichert auf PKI-Token:

   C=DE

O=Technische Universitaet Berlin

serialNumber=<Unterscheidende Nummer>

CN=<Vorname Name>

Der Parameter <Unterscheidende Nummer> enthält eine fortlaufende Nummer, die dazu dient, die vergebenen DN über die gesamte Laufzeit des CA-Zertifikats eindeutig zu halten.

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

Die TUB CA bietet ihre Dienstleistungen allen Angehörigen und Mitarbeitern des DFN-Anwenders Technische Universität Berlin an.

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

Eine Dienstvereinbarung der TU Berlin legt fest, dass private Schlüssel grundsätzlich auf einem PKI-Token (Chipkarte oder USB-Token) zu speichern sind. Einzige Ausnahme sind die privaten Chiffrierschlüssel, die aus dienstlichen Erfordernissen für eine Schlüsselwiederherstellung sicher hinterlegt werden müssen.

Eine Kopie dieser Chiffrierschlüssel wird in einem gesonderten Stahlschrank im Tresorraum (Lampertz-Zelle) des IT-Service-Centers (tubIT) der TU Berlin aufbewahrt. Zutritt zu diesem Raum hat ausschließlich einer kleiner Kreis von Schließberechtigten, der vom tubIT Leiter per Dienstanweisung festgelegt wird. Inbesondere gehören RA Mitarbeiter diesem Kreis nicht an.

Den Chiffrierschlüssel erhalten nur Zertifikatnehmer, die auch Beschäftigte der TU Berlin sind. Die Verwendung dieses Schlüssels innerhalb der TU Berlin ist allein zum dienstlichen Gebrauch bestimmt. Zertifikatnehmer können den Chiffrierschlüssel zwar auch für private Zwecke nutzen, jedoch nur im privaten Bereich außerhalb der TU Berlin. Dadurch ist ausgeschlossen, dass innerhalb der TU Berlin durch die Wiederherstellung des privaten Schlüssels auch private Daten betroffen sein können.

Eine Schlüsselwiederherstellung ist nur dann gerechtfertigt, wenn einer der folgenden Fälle vorliegt:

- Mit Erlaubnis des Zertifikatnehmers und, wenn sonst keine andere Möglichkeit besteht, die Daten zu entschlüsseln,
  - bei Beschädigung des PKI-Tokens,
  - bei Verlust des PKI-Tokens.
- Der Zugriff auf den privaten Schlüssel erfolgt auf Verlangen einer autorisierten Person, die nicht mit dem Zertifikatnehmer identisch ist:
  - bei längerer Abwesenheit und gleichzeitiger Nichterreichbarkeit des Zertifikatnehmers, um zwingend erforderliche Aufgaben oder Vorgänge durchführen zu können,
  - bei Tod oder unvorhergesehenem Ausscheiden des Zertifikatnehmers, wenn eine Entschlüsselung von Daten zur ordnungsgemäßen Weiterbearbeitung von Vorgängen, Aufgaben usw. notwendig ist,
  - zur Behebung eines Beweisnotstandes, wenn ein begründeter Verdacht auf Missbrauch von TU-Eigentum oder eines sonstigen rechtlich zu verfolgenden Fehlverhaltens eines Zertifikatnehmers (TU-Beschäftigten) besteht.

Die Vorgehensweise bei der Bearbeitung des Ersuchens auf Wiederherstellung des privaten Chiffrierschlüssels hängt von der Begründung des Ersuchens ab.

- Bei Beschädigung des PKI-Tokens wird das Vieraugenprinzip angewendet: Zwei Beschäftigte der TUB CA suchen den Archivraum auf. Dort übertragen sie das betreffende Schlüsselpaar vom Archivierungsmedium auf einen geeigneten Datenträger. Anschließend wird dieses auf ein neues PKI-Token aufgebracht und der Kartenausgabestelle (angesiedelt in der Registrierungsstelle) zur weiteren Verarbeitung ausgehändigt. Der Vorgang wird geeignet protokolliert (Uhrzeit, beteiligte Personen).
- Bei Verlust des PKI-Token kann die Wiederherstellung von Daten beantragt werden, die mit dem alten Token verschlüsselt sind. Dies ist im Zusammenhang mit der Ausstellung

eines Ersatz-Tokens möglich. Dazu muss der Zertifikatnehmer die verschlüsselten Daten den Mitarbeitern der TUB CA übergeben. Der wiederhergestellte Schlüssel wird nach der Entschlüsselung der Daten umgehend vernichtet. Der Vorgang wird geeignet protokolliert (Uhrzeit, beteiligte Personen).

- Bei Nichterreichbarkeit eines Zertifikatnehmers (Krankheit, Ausscheiden, Tod), Missbrauch, dem Verdacht auf Missbrauch oder bei Strafverfolgung wird ein Antrag auf Schlüsselwiederherstellung über die Hochschulleitung an die TUB CA gestellt. Antragsberechtigt ist die Person, die die Daten zur Erfüllung dienstlicher Zwecke benötigt.

  Der Antragsteller hat die Daten, welche für den Nachweis des Missbrauchs oder der Straftat von Bedeutung sind, den Mitarbeitern der TUB CA auf einem geeigneten Datenträger vor Wiederherstellung des Schlüssels zu übergeben. Zwischen den übergebenen Daten und dem zur Last gelegten Vorgang muss ein eindeutiger zeitlicher Zusammenhang bestehen. Keinesfalls dürfen pauschal sämtliche Daten des Zertifikatnehmers dechiffriert werden. Darüber hinaus sind bei Missbrauch oder bei Verdacht auf Missbrauch Personalvertretung, Datenschutzbeauftragter und der betroffene Zertifikatnehmer zu beteiligen. Der Zertifikatnehmer hat das Recht, dem Verfahren beizuwohnen. Personalvertretung und Datenschutzbeauftragter haben ebenfalls das Recht, dem Verfahren beizuwohnen. Nach Wiederherstellung des Schlüssels werden die übergebenen Daten dann unter Einhaltung des Vieraugenprinzips dechiffriert. Die wiederhergestellten Daten werden von einem der beteiligten Beschäftigten der TUB CA signiert, um ihre Integrität zu gewährleisten, und der berechtigten Person bzw. der Strafverfolgungsbehörde übergeben. Der wiederhergestellte Schlüssel wird danach umgehend vernichtet. Der Vorgang wird geeignet protokolliert (Uhrzeit, beteiligte Personen).

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

Die TUB CA wird durch den DFN-Verein im Auftrag des DFN-Anwenders Technische Universität Berlin bei der DFN-PCA betrieben. Daher sind für die TUB 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"

Alle Schlüssel mit Ausnahme des Chiffrierschlüssels werden im Rahmen des Produktionsprozesses der PKI-Token erzeugt. Sie befinden sich ausschließlich im Speicher der PKI-Token.

Das Chiffrierschlüssel wird auf einem IT-System ohne Netzwerkanschluss erzeugt. Es wird eine Kopie des Schlüssels zur potentiellen Schlüsselwiederherstellung auf einem Archivmedium im Tresorraum der TUB CA sicher verwahrt.

Vor der Einspielung in den Speicher des PKI Tokens werden die noch keiner Person zugeordneten Chriffrierschlüssel mit einer Transportverschlüsselung versehen. Nach erfolgter Einspielung in den Speicher des PKI Tokens werden die Schlüssel auf den Datenträgern gelöscht.

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

Zu jedem PKI-Token wird dem Inhaber je eine initiale PIN und PUK in Form eines PIN/PUK-Briefes übergeben. Die Erstellung der PIN/PUK-Briefe erfolgt vor und völlig unabhängig von der Personalisierung des PKI-Tokens. Die Briefe sind verschlossen und können von den RA-Mitarbeitern nicht ohne Beschädigungen gelesen werden.

Zu CPS der DFN-PCA: "6.2.3: Hinterlegung (Key Escrow) privater Schlüssel"

Die TUB CA kann Kopien von privaten Chiffrierschlüsseln hinterlegen. Die Datenträger mit den Schlüsseln werden im Tresorraum der TUB CA verwahrt. Die Wiederherstellung der Schlüssel ist nur nach dem, mit Personalrat und Datenschutz der TU Berlin vereinbarten, Verfahren zulässig (siehe "4.12.1 Richtlinien u. Praktiken zur Schlüsselhinterlegung und -wiederherstellung").

Sind die Voraussetzungen zur Wiederherstellung gegeben, werden vorab der Leiter von tubIT, der Datenschutz der TU Berlin und der Personalrat der TU Berlin informiert.

Schlüsselwiederherstellungen werden ausschließlich von RA-Mitarbeitern vorgenommen. Da ein RA-Mitarbeiter zum Betreten des Tresorraums die Begleitung einer Person mit Zutrittsberechtigung (Schließberechtigter) benötigt, wird das Vieraugenprinzip gewahrt.

Zu CPS der DFN-PCA: "6.2.4 Backup der privaten Schlüssel"

Ein Backup privater Chiffrierschlüssel von Zertifikatnehmern kann in zwei Fällen erfolgen:

- Mit Erlaubnis des Zertifikatnehmers und bei Beschädigung seines PKI-Tokens wird das betreffende Schlüsselpaar mit Hilfe eines IT-Systems ohne Netzwerkanschluss auf ein neues PKI-Token aufgebracht. Dieses PKI-Token wird im Rahmen eines Personalisierungsvorgangs dem Zertifikatnehmers als Ersatz für seinen beschädigten Token ausgehändigt.
- Auf Verlangen des Zertifikatnehmers oder einer autorisierten Person kann ein privater Chiffrierschlüssel zur Wiederherstellung verschlüsselter Daten temporär dem Archivmedium entnommen werden. Nach der Wiederherstellung ist der private Chiffrierschlüssel umgehend zu vernichten. Die Gründe, die eine Wiederherstellung verschlüsselter Daten erlauben, sind in "4.12.1 Richtlinien u. Praktiken zur Schlüsselhinterlegung und -wiederherstellung" beschrieben.
  In beiden Fällen ist der Vorgang geeignet zu protokollieren (Uhrzeit, beteiligte Personen).

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

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