DFN-PKI

Erklärung zum Zertifizierungsbetrieb der TU Dortmund Chipcard CA in der DFN-PKI

- Sicherheitsniveau: Global -

Technische Universität Dortmund

CPS der TU Dortmund Chipcard CA

V1.1

18.08.2008

1 Einleitung

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

Für den Betrieb der TU Dortmund Chipcard CA gelten die folgenden Dokumente:

- CP der DFN-PKI: "Zertifizierungsrichtlinie der DFN-PKI – Sicherheitsniveaus: Global, Classic und Basic -", Version 2.1, Dezember 2006, OID 1.3.6.1.4.1.22177.300.1.1.5.2.1
- 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 TU Dortmund Chipcard CA sind in Kapitel 3 dieses Dokuments beschrieben.

Die TU Dortmund Chipcard CA stellt ausschließlich Zertifikate im Sicherheitsniveau "Global" aus.

2 Identifikation des Dokuments

- Titel: "Erklärung zum Zertifizierungsbetrieb der TU Dortmund Chipcard CA in der DFN-PKI"
- Version: 1.1

3 Abweichungen vom CPS der DFN-PCA

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

Zu CPS der DFN-PCA: "1.3.1 Zertifizierungsstellen"

Die Anschrift der TU Dortmund Chipcard CA lautet:

TU Dortmund	Telefon: +49 231 755 2347
ITMC	Telefax: +49 231 755 2731
TU Dortmund Chipcard CA	
August-Schmidt-Str. 12	E-Mail: chipcard-ra@pki.tu-dortmund.de
D – 44227 Dortmund	WWW: www.pki.tu-dortmund.de/chipcard

Zu CPS der DFN-PCA: "1.3.2 Registrierungsstellen"

Die ausgezeichneten Registrierungsstellen für die zuvor genannten Zertifizierungsstellen befinden sich in den Räumen der TU Dortmund Chipcard CA.

Darüber hinaus sind keine weiteren Registrierungsstellen verfügbar.

Zu CPS der DFN-PCA: "1.4.1 Geeignete Zertifikatsnutzung"

Die im Rahmen der DFN-PKI ausgestellten Zertifikate können u.a. für Authentifizierung und elektronische Signatur verwendet werden. Der private Schlüssel des Zertifikatsnutzers darf nur für Anwendungen benutzt werden, die in Übereinstimmung mit den im Endnutzerzertifikat angegebenen Nutzungsarten (*keyUsage*) stehen.

Folgende Nutzungsarten sind vorgesehen:

- Authentifizierung von Benutzer- oder Anwendungsdaten (Nutzungsart *digital-Signature*)

- Kennzeichnung der Verbindlichkeit (Nutzungsart *nonRepudiation*) einer elektronischen Signatur durch den Zertifikatsnehmer.

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 TU Dortmund Chipcard CA erfolgt durch:

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

Zu CPS der DFN-PCA: "1.5.2 Kontaktperson"

Die verantwortliche Person für das CPS der TU Dortmund Chipcard CA ist:

TU Dortmund	Stefan Rapp
ITMC	Telefon: +49 231 755 4668
TU Dortmund Chipcard CA	
August-Schmidt-Str. 12	Telefax: +49 231 755 2731
D – 44227 Dortmund	E-Mail: stefan.rapp@tu-dortmund.de

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 TU Dortmund Chipcard CA enthalten die Attribute "`C=DE`" und "`O=Technische Universitaet Dortmund`".

Das optionale Attribut "`OU=<Organisationseinheit>`" kann mehrmals 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 drei unterschiedliche Zertifikate ausgegeben. Folgende Schemata sind zulässig:

1. Zertifikate für die Registrierungstelle:

   C=DE

   O=Technische Universitaet Dortmund

   [OU=<Organisationseinheit>]

   CN=<Eindeutiger Name>

Das Attribut "CN=" enthält den Bezeichner "Registrierungsstelle der Tu Dortmund Chipcard CA", optional wird der CN durch eine fortlaufende Nummerierung ergänzt.

2. Zertifikat für den Zweck der **digitalen Signatur** durch den Zertifikatnehmer:

   C=DE

   O=Technische Universität Dortmund

   OU= TU Dortmund Chipkarten CA

OU=<Organisationseinheit>

CN=<Eindeutiger Name>

emailAddress=<E-Mail Adresse>

Das Attribut "CN=" enthält den natürlichen Namen bestehend aus Vorname, Nachname.

3. Zertifikat für den Zweck der **Authentifizierung** des Zertifikatnehmers:

   C=DE

   O=Technische Universität Dortmund

   OU=<Organisationseinheit>

   CN=<Eindeutiger Name>

   UID=<Login ID>

   [emailAddress=<E-Mail Adresse>]

   Das Attribut "CN=" enthhält das Kennzeichen "PN:" gefolgt vom Wort „Anmeldung:" und schließt mit dem natürlichen Namen ab. Beispiel: "CN=PN: Anmeldung: Markus Mustermann".

   Das Attribut "UID=" enthält die eindeutige LoginID des Zertifikatnehmers aus dem Identity Management System der TU Dortmund.

Zu CPS der DFN-PCA: "3.2.1 Verfahren zur Überprüfung des Besitzes des privaten Schlüssels"

Die RA erzeugt die Schlüssel auf Kryptochipkarten in einem speziellen Verfahren selbst. Der CSR wird durch den auf der Karte erzeugten privaten Schlüssel signiert.

Die Antragsdaten des CSR werden dem Zertifikatnehmer zu Prüfzwecken ausgehändigt. Dieses Dokument ist Teil einer ganzen Dokumentenmappe, die der Zertifikatnehmer mit einer Unterschrift zur Kenntnis nimmt und bestätigt.

Die Schlüsselgenerierung erfolgt durch autorisierte Mitarbeiter an speziell eingerichteten Arbeitsplätzen ausschließlich auf Kryptochipkarten. Der private Schlüssel kann per Spezifikation der verwendeten Karten den Kryptochip nicht verlassen.

Die PIN zum Nutzen der privaten Schlüssel wird dem Zertifikatnehmer vertraulich übergeben.

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

Die TU Dortmund Chipcard CA bietet ihre Dienstleistungen allen Angehörigen und Mitarbeitern des DFN-Anwenders Technische Universität Dortmund sowie im Auftrag der Technische Universität Dortmund handelnden Personen an. Dabei ist die Regelung aus CP 1.3.3 "Zertifikatnehmer" zu berücksichtigen.

Zu CPS der DFN-PCA: "4.1.2 Registrierungsprozess"

Der Zertifizierungsprozess ist so angelegt, dass ausschließlich digitale Dokumente entstehen. Der Zertifikatsantrag wird von der RA als PDF digital signiert und sodann archiviert.

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

Die TU Dortmund Chipcard CA veröffentlicht die gemäß den Zertifizierungsrichtlinien der DFN-PKI geforderten Zertifikate über die oben angegebenen Informationssysteme.

Die in 3.1.1 angegebenen Zertifikate für natürliche und juristische Personen werden nicht veröffentlicht.

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

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

Schlüssel für Nutzerzertifikate werden bei der Registrierungsstelle auf einer Kryptochipkarte erzeugt.

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

Die Übermittlung von privaten Schlüsseln an Zertifikatnehmer erfolgt durch die persönliche Übergabe einer Kryptochipkarte. Die Übermittlung der PIN erfolgt durch ein gesichertes Verfahren (z.B. Aushändigung eines speziellen PIN-Briefes).

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

Die durch die TU Dortmund Chipcard CA ausgestellten Nutzerzertifikate haben standardmäßig eine Laufzeit von drei Jahren.