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

V1.3

01.10.2011

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 2.2, 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 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: 1.3

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 2414
ITMC	Telefax: +49 231 755 2731
TU Dortmund Chipcard CA	
August-Schmidt-Str. 12	E-Mail: chipcard-ra@pki.tu-dortmund.de
44227 Dortmund	WWW: unicard.tu-dortmund.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 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 für Authentifizierung, elektronische Signatur und Verschlüsselung verwendet werden. Die privaten Schlüssel des Zertifikatnutzers dürfen 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 *digitalSignature*)
- Kennzeichnung der Verbindlichkeit (Nutzungsart *nonRepudiation*) einer elektronischen Signatur durch den Zertifikatnehmer.
- Verschlüsselung von Dokumenten (Nutzungsart *dataEncipherment*)

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
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 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
44227 Dortmund	E-Mail: stefan.rapp@tu-dortmund.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 TU Dortmund Chipcard CA enthalten die Attribute "`C=DE`" und "`O=Technische Universitaet Dortmund`".

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 vier 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 Universitaet Dortmund

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 Universitaet Dortmund

   OU=<Organisationseinheit>

   CN=<Eindeutiger Name>

   UID=<Login ID>

   [EmailAddress=<E-Mail Adresse>]

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

   Das Feld "subjectAlternativeName" enthält die E-Mail Adresse, den User Principal Name und die eindeutige LoginID des Zertifikatnehmers aus dem Identity Management System der TU Dortmund.

4. Zertifikat für den Zweck der **Verschlüsselung**:

   C=DE

   O=Technische Universitaet Dortmund

   OU=<Organisationseinheit>

   CN=<Eindeutiger Name>

   [EmailAddress=<E-Mail Adresse>]

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

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

Die Registrierungsstelle 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.

Zur Übermittlung des privaten Schlüssels an den Zertifikatnehmer siehe 6.1.2.

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 Registrierungsprozess für Zertifikate für Authentifizierung, digitale Signatur und Verschlüsselung besteht aus den folgenden Schritten, die in dieser Reihenfolge durchlaufen werden:

1. Eintrag der Daten des Zertifikatnehmers in das Hochschul-Verwaltungssystem.

2. Kontrolle der Daten des Zertifikatnehmers anhand der Unterlagen, die für die Immatrikulation bzw. Einstellung eingereicht werden müssen. Für Studierende erfolgt die Kontrolle insbesondere anhand von beglaubigten Kopien der Hochschulzugangsberechtigung. Bei Mitarbeiter/innen ist die Vorlage der Geburtsurkunde sowie eines amtlichen Führungszeugnisses Einstellungsvoraussetzung.

3. Erstellung von privaten Schlüsseln und Zertifikaten anhand der kontrollierten Daten aus dem Hochschul-Verwaltungssystem.

> 3.1 Für Studierende wird die Kryptochipkarte mit den privaten Schlüsseln des Zertifikatnehmers in der Registrierungsstelle vor unbefugtem Zugriff geschützt aufbewahrt. Der Brief mit der PIN zum Zugriff auf die privaten Schlüssel wird verschlüsselt in einer Datenbank aufbewahrt und erst bei Übergabe der Kryptochipkarte entschlüsselt, gedruckt und ausgehändigt. Eine Entschlüsselung des PIN-Briefs ist ausschließlich den Mitarbeitern der Registrierungsstelle möglich, welche die Kryptochipkarten aushändigen. Eine ständige Speicherung des entschlüsselten PIN-Briefs findet nicht statt.
>
> 3.2 Für Mitarbeiter/innen wird die Kryptochipkarte mit den privaten Schlüsseln des Zertifikatnehmers an das zuständige Dekanat/Dezernat oder die zuständige zentrale Einrichtung versandt und dort bis zur Übergabe an den Mitarbeiter / die Mitarbeiterin vor unbefugtem Zugriff geschützt aufbewahrt. Der Versand des Briefs mit der PIN zum Zugriff auf den privaten Schlüssel erfolgt gesondert. Eine ständige Speicherung des entschlüsselten PIN-Briefs findet nicht statt.

4. Abschluss der Registrierung durch eine persönliche Identifizierung mit Übergabe der privaten Schlüssel und der Zertifikate nach Kapitel 6.1.2 „Übermittlung des privaten Schlüssels an den Zertifikatnehmer"

Für Zertifikate, die nicht innerhalb einer Frist von vier Wochen abgeholt werden, werden der zugehörige private Schlüssel vernichtet und das Zertifikat gesperrt.

Der Registrierungsprozess ist so angelegt, dass ausschließlich digitale Dokumente entstehen. Der Zertifikatantrag wird von der Registrierungsstelle als PDF digital signiert und sodann archiviert.

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

Die in 3.1.1 angegebenen Zertifikate werden im Identity Management System sowie im zentralen Active Directory der TU Dortmund veröffentlicht.

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

Für die Verschlüsselungsschlüssel findet eine Schlüsselhinterlegung statt. Dabei werden die Schlüssel in Form eines Softwarezertifikats verschlüsselt bei der Registrierungsstelle abgelegt. Zur Wiederherstellung eines Verschlüsselungsschlüssels müssen zwei RA-Administratoren die Entschlüsselung bestätigen ("Vier-Augen-Prinzip"). Technisch wird dieses Vorgehen mittels eines Secret-Sharing-Verfahrens (Shamir's Secret Sharing) sichergestellt.

Die Herausgabe der hinterlegten Schlüssel kann auf zwei Arten erfolgen:

> 1. Herausgabe an den Zertifikatsnehmer
>
> Auf Antrag können die Verschlüsselungsschlüssel in Form eines Softwarezertifikats an den Zertifikatsnehmer ausgehändigt werden. Dazu ist eine unabhängige Prüfung des Antrags und der Identität des Zertifikatnehmers durch zwei RA-Administratoren erforderlich.
>
> 2. Herausgabe an Dritte

Im Falle des Ausscheidens eines Zertifikatsnehmers aus der TU Dortmund, länger andauernder Krankheit, Tod oder zum Zweck der Beweissicherung bei strafrechtlichen Ermittlungsverfahren kann der Schlüssel auf Antrag auch an andere Personen als den Zertifikatsnehmer herausgegeben werden. Hierzu muss von berechtigten Personen ein Antrag bei der Registrierungsstelle gestellt werden. Die Registrierungsstelle informiert vorab den Datenschutzbeauftragten der TU Dortmund, der Zertifikatnehmer wird ebenfalls über die Wiederherstellung informiert.

Die Wiederherstellung des Schlüssels wird von der Registrierungsstelle und einem Vertreter eines zweiten Personenkreises (Personalabteilung oder Datenschutzbeauftragter) in Anwesenheit des Antragsstellers und eines Protokollführers durchgeführt. Der Schlüssel wird in Form eines Softwarezertifikats an den Antragsteller übergeben.

Der Protokollführer erstellt ein Protokoll des Vorgangs, das beim Datenschutzbeauftragten und in Kopie in der Registrierungsstelle hinterlegt wird.

Wurde ein Schlüssel an eine andere Person als den Zertifikatnehmer herausgegeben, so werden alle zugehörigen Zertifikate gesperrt.

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"

Die Schlüssel für Signatur und Authentifizierung werden durch die Registrierungsstelle an speziell eingerichteten Arbeitsplätzen auf einer Kryptochipkarte erzeugt. Die privaten Schlüssel können per Spezifikation der verwendeten Karten den Kryptochip nicht verlassen.

Die Verschlüsselungsschlüssel werden in einer Softwarekomponente erzeugt und sowohl auf der Kryptochipkarte als auch in verschlüsselter Form in der Registrierungsstelle hinterlegt. Der private Verschlüsselungsschlüssel kann nach PIN-Eingabe aus der Karte ausgelesen werden.

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 Kryptochipkarte wird ausschließlich im Rahmen einer persönlichen Identifizierung unter Vorlage eines amtlichen Lichtbildausweises übergeben. Die Identifizierung und Übergabe werden schriftlich dokumentiert.

Für den privaten Schlüssel zur Verschlüsselung sind zusätzlich das Auslesen aus der Kryptochipkarte und somit auch die Nutzung in Form eines Software-Zertifikats vorgesehen.

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

Es wird ein Backup der privaten Verschlüsselungsschlüssel gemäß Kapitel 4.12.1 durchgeführt.

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.