

Erklärung zum Zertifizierungsbetrieb der UniBwM CA in der DFN-PKI

- Sicherheitsniveau: Global -

1 Einleitung

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

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

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

2 Identifikation des Dokuments

- Titel: "Erklärung zum Zertifizierungsbetrieb der UniBwM CA in der DFN-PKI"
- Version: 2.0

3 Abweichungen vom CPS der DFN-PCA

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

Zu CPS der DFN-PCA: "1.3.1 Zertifizierungsstellen"

Die Anschrift der UniBwM CA lautet:

Universität der Bundeswehr München	Telefon: +49 89 6004-5555
Rechenzentrum	Telefax: +49 89 6004-3254
UniBwM CA	
Werner-Heisenberg-Weg 39	E-Mail: pki@unibw.de
85577 Neubiberg	WWW: www.unibw.de/rz/pki
GERMANY	

Zu CPS der DFN-PCA: "1.3.2 Registrierungsstellen"

Die ausgezeichneten Registrierungsstellen für die zuvor genannten Zertifizierungsstellen befinden sich in den Räumen der UniBwM 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, elektronische Signatur und Verschlüsselung verwendet werden. Der private Schlüssel des Zertifikatsnutzers darf nur für Anwendungen benutzt werden, die in Übereinstimmung mit den im Endnutzertifikat angegebenen Nutzungsarten (keyUsage) stehen.

Darüber hinaus dürfen

- Signatur- oder Authentifizierungszertifikate nicht für Verschlüsselung verwendet werden.

- Zertifikate für Personengruppen (Gruppenzertifikate) nicht für die Nutzungsart (keyUsage) Signatur ausgestellt werden.

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 UniBwM 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 UniBwM CA ist:

Universität der Bundeswehr München	Ludwig Bayer
Rechenzentrum	Telefon: +49 89 6004-3219
UniBwM CA	
Werner-Heisenberg-Weg 39	Telefax: +49 89 6004-3254
85577 Neubiberg	E-Mail: Ludwig.Bayer@unibw.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 UniBwM CA enthalten die Attribute "C=DE", "ST=Bayern", "L=Muenchen" und "O=Universitaet der Bundeswehr Muenchen".

Das optionale Attribut "OU=<Organisationseinheit>" darf nicht angegeben werden.

Wenn eine E-Mail Adresse angegeben wird, so kann diese über das Attribut "emailAddress" in den Namen aufgenommen werden.

Damit entspricht der Name jedes Zertifikatnehmers dem folgenden Schema:

```
C=DE
ST=Bayern
L=Muenchen
O=Universitaet der Bundeswehr Muenchen
CN=<Eindeutiger Name>
[ emailAddress=<E-Mail Adresse>@unibw.de ]
```

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

Die UniBwM CA bietet ihre Dienstleistungen allen Angehörigen und Mitarbeitern des DFN-Anwenders Universität der Bundeswehr München an. Die UniBwM CA behält sich vor, Zertifizierungswünschen nicht nachzukommen.

Zu CPS der DFN-PCA: "4.12.1 Richtlinien und Praktiken zu Schlüssel hinterlegung und -wiederherstellung"

Die UniBwM CA fordert für Zertifikate von persönlichen Schlüsseln, die zur Verschlüsselung genutzt werden, die Hinterlegung des privaten Schlüssels, des Verschlüsselungsschlüssels.

Private Schlüssel von Signatur- oder Authentifizierungszertifikaten werden nicht hinterlegt.

Private Schlüssel von Signaturzertifikaten werden auf einem Krypto-Gerät erzeugt.

Im Rahmen der Zertifikatbeantragung in der Registrierungsstelle der UniBwM CA wird ein verschlüsseltes Backup der Verschlüsselungsschlüssel erzeugt und in einer Datenbank gespeichert, die sich auf Servern in einbruchsgesicherten Räumen der RA befindet. Der Schlüssel für dieses Backup wird als eine mit einer Passphrase geschützten Datei erzeugt und auf ein mit PIN geschütztes Krypto-Gerät übertragen. Die Eingabe und Verwahrung von Passphrase und PIN wird gemeinsam von zwei durch die Hochschulleitung bestimmten Personen vorgenommen, die nicht der RA angehören. Die Datei und das Krypto-Gerät verbleiben in den Räumen der RA. Für dieses Krypto-Gerät ist kein PIN-Recovery möglich. Über diesen Vorgang wird ein Protokoll angelegt. Die Nutzung des Backupsschlüssels durch eine einzelne Person ist damit ausgeschlossen.

Die Herausgabe von hinterlegten privaten Verschlüsselungsschlüsseln erfolgt grundsätzlich nur an den jeweiligen Zertifikatnehmer und in jedem Fall auf einem Krypto-Gerät. Folgende Regelungen gelten dabei:

- a) Im Falle des Defektes eines Krypto-Gerätes werden hinterlegte private Verschlüsselungsschlüssel des betroffenen Zertifikatnehmers von der RA auf ein neues Gerät gespeichert, welches dem Zertifikatnehmer ausgehändigt wird. Das defekte Krypto-Gerät muss vorher der RA ausgehändigt werden und wird danach durch die RA unverzüglich vernichtet oder, falls ein Softwareproblem vorlag, neu initialisiert.
- b) Bei Verlust oder Diebstahl des privaten Verschlüsselungsschlüssels (durch Verlust oder Diebstahl des Krypto-Geräts) wird der hinterlegte Schlüssel auf einem neuen Krypto-Gerät an den betreffenden Zertifikatnehmer ausgehändigt. Das Verschlüsselungszertifikat sowie alle anderen Zertifikate, die sich auf dem Krypto-Gerät befanden, werden davon unabhängig unverzüglich gesperrt. Falls Zertifikate von Personengruppen betroffen sind, werden alle betroffenen Zertifikatnehmer informiert.
- c) Verschlüsselungsschlüssel werden ansonsten über die Gültigkeit von Verschlüsselungszertifikaten hinaus unbefristet aufbewahrt.
- d) Im Falle des Ausscheidens eines Zertifikatnehmers aus der Universität der Bundeswehr München, länger andauernder Krankheit, Tod oder zum Zweck der Beweissicherung bei Verdacht auf strafrechtliche Handlungen können Mitarbeiter der RA nach Genehmigung durch den Datenschutzbeauftragten der Universität der Bundeswehr München den oder die privaten Verschlüsselungsschlüssel des betreffenden Mitarbeiters zur Sicherstellung verschlüsselter Daten verwenden. Noch gültige Verschlüsselungszertifikate sowie alle anderen Zertifikate, die sich im Besitz des Mitarbeiters befanden, werden davon unabhängig unverzüglich gesperrt. Davon ausgenommen sind Zertifikate von Personengruppen, sofern das Krypto-Gerät dieses Zertifikatnehmers der RA übergeben wurde.

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

Die UniBwM CA wird durch den DFN-Verein im Auftrag des DFN-Anwenders Universität der Bundeswehr München bei der DFN-PCA betrieben. Daher sind für die UniBwM CA dieselben infrastrukturellen, organisatorischen, personellen und technischen Sicherheitsmaßnahmen umgesetzt, wie für die DFN-PCA (siehe CPS der DFN-PCA). Zur Erzeugung von Schlüsseln und Zertifikaten sowie deren Hinterlegung (vgl. 4.12.1) wird ausschließlich Software der DFN-PCA eingesetzt.

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

Die Übermittlung von privaten Schlüsseln an Zertifikatnehmer erfolgt ausschließlich auf Krypto-Geräten, die mit einer PIN gesichert sind. Die Übermittlung der PIN erfolgt durch Aushändigung bzw. Versand eines PIN-Briefes. Die Übergabe des Krypto-Gerätes erfolgt persönlich (Übergabe an Zertifikatnehmer) oder durch einen vom PIN-Brief getrennte Versand an den Zertifikatnehmer. Der Empfang des Krypto-Gerätes sowie des PIN-Briefes ist vom Zertifikatnehmer zu bestätigen.

Auf ein Krypto-Gerät können weitere Zertifikate der UniBwM CA übertragen werden. Dazu muss der Zertifikatnehmer die PIN (vor Einblicken o.ä.) geschützt eingeben. Ansonsten wird das Krypto-Gerät in den Räumen der RA mit denselben Geräten und Programmen wie beim ersten Zertifikat behandelt.

Es wird gewährleistet, dass Mitarbeiter der RA keine Kenntnis der jeweiligen PIN erlangen. Die PIN wird bei der initialen Ausgabe des Krypto-Gerätes auf ein sichtgeschütztes Feld eines PIN-Briefes gedruckt, das erst nach einer nachweisbaren Manipulation sichtbar wird.

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

Die UniBwM CA fordert von den Zertifikatnehmern den Backup der privaten Schlüssel, welche zur Verschlüsselung zertifiziert sind, bei der RA entsprechend Kapitel 4.12.1.

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

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