

Michael Werzowa, IT-MS

## CPS der Portalverbund-CA

*Certificate Practice Statement der Portalverbund-CA. Stand 2002-10-27*

Dieses Dokument ist online unter <http://portal.bmi.gv.at/ref/pki/portalCA/PortalV-CPS.pdf> in aktueller Form verfügbar.

Sämtliche aktuellen Dokumente rund um das Thema Portalverbund sind gesammelt unter der Adresse <http://portal.bmi.gv.at/ref/pki/portalCA/index.html> verfügbar, alternativ unter dem sicheren Link <https://portal.bmi.gv.at/ref/pki/portalCA/index.html>.

---

### Überblick

Das vorliegende „Certificate Practice Statement“ der Portalverbund-CA dient dazu, die Umsetzung der Ausgabe, Administration und Anwendung der PortalV-CA Zertifikate festzulegen und zu beschreiben.

Weitere Dokumente zu der Portalverbund-CA sind

- 1) das Überblicksdokument zum Portal: [http://portal.bmi.gv.at/ref/pki/portalCA/Ueberblick\\_PortalV-CA.pdf](http://portal.bmi.gv.at/ref/pki/portalCA/Ueberblick_PortalV-CA.pdf)
- 2) Das „Certificate Policy“ Dokument, das die Richtlinien für die Verwendung der Zertifikate beinhaltet, und zwar im Sinne von Erfordernissen, Einschränkungen und Nutzungsvorschriften.  
<http://portal.bmi.gv.at/ref/pki/portalCA/PortalV-CP.pdf>
- 3) Die „CA-Administrator’s Documentation“ die eine interne, vertrauliche Dokumentation ist. Da darin auch detaillierte Hinweise über Implementierung und Sicherungsmaßnahmen gibt, ist dieses Dokument nur für an Entwicklung, Betrieb und Revision beteiligte Personen zugänglich.

CPS und CP sind Dokumente, die derzeit von unterschiedlichen Stellen unterschiedlich definiert werden. In den kommenden Jahren wird sich möglicherweise eine einheitliche Verwendung herausstellen. Die von uns vorgenommene Definition der Dokumente ist eine Verwendungsform, die uns besonders plausibel erscheint.

Das vorliegende Dokument ist im Vergleich zu CPS-Dokumenten von kommerziellen Anbietern kurz gefasst, da einige Einschränkungen für das Portal bestehen, die die Anforderungen reduzieren.

---

### Identifikation des CPS

Dieses Dokument hat eine offizielle OID-Nummer: 1.2.40.0.10.1.2.3.1

OID 1	iso
OID 1.2	iso member body
OID 1.2.40	Austria (ÖNORM Institut)
OID 1.2.40.0.10	Österreichische Verwaltung
OID 1.2.40.0.10.1	Organisation

OID 1.2.40.0.10.1.2 Bundesministerium für Inneres

OID 1.2.40.0.10.1.2.3 Standarddokumente

OID 1.2.40.0.10.1.2.3.1 CPS Portalverbund

Sollte beizeiten eine Versionsnummer nötig werden, so ist diese an die OID anzuhängen.

---

## Anwendungsgebiete der Portalverbund-CA

Die Portalverbund-CA ist eine Sub-CA einer BMI-eigenen Certificate Authority „Portal-Root-CA“.

Die Zertifikate der Portal-Verbund Server-CA dienen ausschließlich dem Zweck der Authentisierung und Verschlüsselung von Kommunikation zwischen Servern. Der CN ist der vollqualifizierte Servername. Zertifikate für natürliche Personen werden mit dieser CA nicht erstellt.

Pro Servername ist ein eigenes Zertifikat nötig, also auch für jeden virtuellen Server.

---

## Zertifizierungs-Infrastruktur

Die Zertifikate werden ausschließlich von der Zertifizierungsstelle der Abteilung IT-MS ausgestellt, die im Referat IV/2/e angesiedelt ist.

Der Ablauf der Zertifikatserstellung unterliegt einer ausreichend hohen Sicherheitsstufe. Die CA-Rechner werden als stand-alone Geräte in einem physisch gesicherten Bereich betrieben, die Daten werden mittels Disketten übertragen.

---

## Registration Authority

Der Antrag wird wie folgt geprüft:

- Der Antragsteller muss laut Geschäftseinteilung eine approbationsbefugte Person der Verwaltungseinheit (Behörde, Gebiets- oder Selbstverwaltungskörperschaft) sein.
- Der Verwendungszweck im Antrag muss einer der folgenden sein:
  - A) Teilnahme am Portalverbund (hat Portalverbundvereinbarung unterzeichnet)
  - B) Verwendung zur Client- oder Server-Authentisierung für E-Government-Applikationen zwischen Verwaltungseinheiten.
  - C) Verwendung zur Client- oder Server-Authentisierung für E-Government-Applikationen innerhalb von Verwaltungseinheiten.
- Der Antrag muss die Kontaktinformationen (Adresse, E-Mail und Telefon) des Antragstellers und des technischen Ansprechpartners und die Zustelladresse für das Zertifikat erhalten.
- Dem Antrag muss entweder ein Certificate Request (PKCS10-Format) oder ein Antrag auf die Ausstellung eines Schlüsselpaars durch das BMI beiliegen.
- Im Antrag muss das gewünschte Zertifikats-Format (PKCS12 oder Java Key Store) angegeben werden.
- Der Antrag muss in schriftlicher Form per Brief übermittelt werden. (Ausnahme: Wenn das BMI auch das Schlüsselpaar erzeugen soll – Alternativvariante, siehe nächster Abschnitt– reicht die Übermittlung per Fax.)

Der Antrag ist an folgende Adresse zu richten:

Bundesministerium für Inneres  
Referat IV/2/e  
Berggasse 43  
1090 Wien

Fax: (01) 90600 39629

Liegt ein bewilligter Antrag in geeigneter Form vor, wird der Antragsteller über den Ablauf, der zur Ausstellung eines Zertifikats führt, informiert.

---

## Certificate Request (Zertifikats-Antrag in CA-lesbarer Form)

Es sind zwei Wege vorgesehen, um zu einem Zertifikat zu kommen. Der bevorzugte Weg ist die Erstellung eines certificate request durch den Antragsteller, ein alternativer Weg ist die Erzeugung von Schlüsseln und Zertifikat durch die CA anhand der Daten aus dem Antrag.

### Daten im Antrag

In jedem Fall sind folgende Daten nötig, die in den certificate request eingebracht werden müssen:

Country Name	(C)	= AT
State	(ST)	= Bundesland
Locality	(L)	= Ort
Organisation	(O)	= Behörde
Org. Unit	(OU)	= Organisationseinheit
Common Name	(CN)	= Servername
email address		= Email des technischen Kontakts

### Antrag mit selbst erstelltem Schlüsselpaar

Anhand einer genauen Beschreibung kann der Antragsteller unter Zuhilfenahme von openssl die Schlüssel erstellen und einen Request generieren.

Dieses Dokument liegt als gesonderte Anleitung bereit unter <http://portal.bmi.gv.at/ref/pki/portalCA/openssl.html>

Darin wird beschrieben, wie openssl installiert, konfiguriert und verwendet wird, um Schlüssel und Request zu erzeugen. Der Arbeitsaufwand für diese Schritte beläuft sich auf etwa einen halben Tag, inklusive Vorbereitungen.

Der Vorteil dieser Vorgehensweise ist, dass Standardwerkzeuge zum Einsatz kommen, die in einer zuverlässigen und vorhersagbaren Form funktionieren und für die Support verfügbar ist. Weiters werden keine Ressourcen durch eine Eigenentwicklung gebunden.

Alternativ können auch andere Werkzeuge verwendet werden, um Schlüssel und Zertifikatsantrag zu generieren. Voraussetzung ist, dass der Antrag standardkonform ist.

Der Certificate-Request ist auf einer 3,5“ Diskette mit FAT-Filesystem zu senden.

### Schlüssel/Antrag/Zertifikate bei CA erstellt

Dabei werden anhand der Daten des Antragstellers Schlüssel, Request und Certificate in einem Ablauf erstellt.

In diesem Fall werden die Schlüssel 14 Tage aufgehoben, um im Falle der Unlesbarkeit der Zertifikats-Diskette eine neuerliche Aussendung des Zertifikats samt Schlüssel zu ermöglichen.

---

## Zertifikatserstellung

Die Zertifikatserstellung wird durch persönlichen Eingriff eines CA-Administrators gestartet. Dieser Generierungslauf findet in einem vierzehntägigen Rhythmus statt. Die requests werden mittels Diskette eingelesen und die Zertifikate auf Diskette ausgegeben.

Bei der kompletten Generierung von keys/request/certificate werden die Daten durch den Administrator händisch in eine Frontend-Anwendung eingetragen.

Die keystores (pkcs#12, jks) werden auf Diskette ausgegeben.

Die CA wird auf CD-ROM gesichert, wobei die allfälligen Zertifikats-Schlüssel der Server-Zertifikate von der Sicherung ausgenommen sind.

---

## Gültigkeitsdauer der Zertifikate

Die Server-Zertifikate werden mit zweijähriger Gültigkeit ausgestellt. Die Schlüssel erfordern normalerweise keine Erneuerung, können aber im Falle technologisch bedingter Notwendigkeiten im gleichen Rhythmus wie die Zertifikate erneuert werden.

Spezielle zeitliche Vorgaben für Key-Rollover-Prozesse sind nicht nötig, da die Schlüssel ihre Gültigkeit nicht zeitgesteuert verlieren, sondern nur die Zertifikate ungültig werden.

Bei der Zertifikatserneuerung sind die notwendigen Laufzeiten durch den vierzehntägigen Rhythmus der Generierungen zu beachten.

Das Wurzelzertifikat hat eine Gültigkeit von zehn Jahren.

---

## Sperrung von Zertifikaten

Die Sperrung von Zertifikaten muss telefonisch und per e-mail durch den Zertifikatseigner (=Administrator des betroffenen Systems) veranlasst werden. Die Telefonnummer und e-mail Adresse dafür werden mit dem Zertifikat übermittelt.

Innerhalb von 24 Stunden wird das Zertifikat dann in der CRL eingetragen.

---

## Verlängerung von Zertifikaten

Zertifikate werden auf Antrag verlängert. Das Antragsformular ist unter

<http://portal.bmi.gv.at/ref/pki/portalCA/cert-verlaengerung.html>

verfügbar.

Die Verlängerung muss bis spätestens ein Monat vor Ablauf des Zertifikats beantragt werden.

---

## Verwendung und Verwahrung der private keys der CA

Die privaten Schlüssel der BMI-Root-CA werden ausschließlich zum Signieren der Sub-CA root certificates verwendet. Die Portalverbund CA signiert ausschließlich Server Zertifikate des Portalverbundes.

Die privaten Schlüssel sind nur auf den CA-Rechnern und auf Backup-CDs, die im Tresor verwahrt werden, gespeichert.

---

## Verwendung und Verwahrung der privaten Schlüssel der Portalverbund-Rechner

Die privaten Schlüssel, die zu den Portalverbund Zertifikaten gehören, sind ausschließlich zum Aufbau der Serververbindungen zu verwenden.

Die Systeme, auf denen die Schlüsseln installiert sind, müssen eine dokumentierte Installation und Wartung aufweisen, und folgenden Kriterien genügen:

Es dürfen keine normalen Anwender-Accounts auf den Systemen geführt werden. Die Rechner dürfen ausschließlich der Funktion als Server dienen.

Es darf keine Anwendungssoftware für Bürogebrauch und sonstigen Endanwender-Bedarf, insbesondere Internetbrowser wie Internet Explorer, Email-Client wie Outlook oder Outlook Express auf dem System installiert sein oder verwendet werden.

Sämtliche Funktionen des Systems müssen dokumentiert sein, so etwa die Funktion als Gateway-Rechner, Firewall, Email Server.

Die Zugriffsrechte auf die Verzeichnisse, in denen die Schlüssel verwahrt werden, müssen möglichst restriktiv gesetzt sein.

Backup der Schlüssel darf nur unabhängig von anderen Backups gemacht werden, um durch unberechtigtes Einspielen eines Backups nicht in den Besitz der Schlüssel zu gelangen.

Das Backup der Schlüssel hat entweder in verschlüsselter Form zu erfolgen oder die Medien müssen in einem Tresor verwahrt werden, wobei über jedes Medium Buch zu führen ist.

Das Server-System hat den Erfordernissen entsprechende Sicherheitsanforderungen zu erfüllen, und zwar sowohl bezüglich der physischen Verwahrung, als auch der Erreichbarkeit über interne oder externe Netzwerkverbindungen.

Virusschutz, Firewall und Intrusion Detection sind Voraussetzung. Insbesondere Windows-Rechner sollen hinter einem Firewall-System, das ein unterschiedliches Betriebssystem verwendet, geschützt werden.

Die Schlüssel dürfen auf keinem zweiten Rechner, auch nicht zu Testzwecken, installiert werden.

Für den Fall, dass das Schlüsselpaar durch die IT-MS generiert werden, werden diese 14 Tage nach der Auslieferung auf dem CA-Server aufgehoben und danach gelöscht, sodass ab diesem Zeitpunkt nur der ausgelieferte Medium und das Server-System (samt allfälligem Backup) den privaten Schlüssel enthält.

---

## Überprüfung der Zertifikate

Der Anwender der Zertifikate (= Systemadministrator des Systems, auf dem das Zertifikat zum Einsatz kommt) muss den im Zertifikat enthaltenen „Fingerprint“ des Root-Certificate mit dem veröffentlichten Fingerprint unter <http://portal.bmi.gv.at/ref/pki/PortalCA/rootcerts.html> vergleichen. Die Fingerprints werden außerdem in der „Wiener Zeitung“ veröffentlicht und sind auf dem Website der „Wiener Zeitung“ verfügbar.

Auf der Webseite wird außerdem erklärt, wie die Prüfung durchgeführt werden kann.

In den Zertifikaten ist ein Link auf die CRL (Certificate Revocation List) eingetragen. Dadurch ist es möglich, Zertifikate als ungültig zu markieren, die gestohlen oder „geknackt“ wurden oder deren Server nicht mehr als vertrauenswürdig gilt.

---

## Gründe für die Sperre von Zertifikaten

Um den Missbrauch oder Diebstahl von Zertifikaten feststellen zu können, muss der Webserver, der sich durch ein Zertifikat identifiziert, über geeignete Schutzmaßnahmen und Überwachungsfunktionen verfügen.

### Sicherheitsmaßnahmen

Keystore, bzw. Keys dürfen nur lesbar sein durch den Administrator des Webservers. Dieser muss ein Benutzerkonto mit einer eigenen Gruppe haben, unabhängig von jedem anderen Konto auf dem System: z.B. User webserv mit Gruppe webserv. Dieser Benutzer webserv darf kein interaktives logon erlauben.

Auf dem Server muss, unabhängig von vorgeschalteten Firewalls, zumindest ein elementares IP-Filtering eingerichtet sein und jeden ungewöhnlichen Verkehr protokolliert werden. Am Server sind nur die notwendigen Dienste und Funktionen zu installieren, und die Installation ist mit angemessenem Aufwand zu härten.

Logs (Protokolle) müssen in angemessenem Umfang geführt und gespeichert werden. Dazu bietet sich an, auf einem eigenen Log-Server zu protokollieren, der ebenso ein sehr hohes Sicherheitsniveau benötigt. (Unix/Syslogd, Windows/Event Manager)

Eine (automatische) Auswertung der Logs und die Verständigung der Administratoren im Falle eines sicherheitsrelevanten Zwischenfalles ist vorzusehen.

dateisysteme und insbesondere Logs müssen geschützt werden, etwa durch Prüfsummen und erweiterte Filesystem Attribute (z.B. dass logs nur „append“ erlauben, kein modify oder delete)

Das System muss jährlich einem internen Audit unterzogen werden.

### **Sperre**

Bei einem System, das die entsprechenden Sicherheitsmaßnahmen beachtet, ist ein Einbruch meistens verhinderbar oder zu bemerken.

Im Falle eines erfolgreichen Einbruchs ist es nötig, das System mit Hilfe von vertrauenswürdigen Software-Quellen und Konfigurationsdaten zu bereinigen. Weiters muss die IT-MS (BMI) über den Einbruch informiert werden, und zwar sowohl telefonisch als auch schriftlich, damit das Zertifikat gesperrt wird.

Das Zertifikat wird umgehend in der CRL publiziert.

Bis zur Ausstellung und Installation eines neuen Zertifikats ist der Server nur über http, nicht über https erreichbar.

---

## **Rechtliches**

### **Haftung**

Die Zertifikate dienen der sicheren Identifikation von Servern und der sicheren Kommunikation zwischen Servern. Diese Funktion wird nach dem Stand der Technik und den Voraussetzungen und Anforderungen des Portalverbundes geboten.

Die Anwendungen haben behördlichen Charakter und entsprechen den üblichen rechtlichen Gepflogenheiten einer Kommunikation zwischen Behörden.

Das BMI übernimmt die Aufgabe, die Portalverbund-CA aufzubauen, zu betreiben und zu verwalten. Es besteht jedoch keine Haftung seitens des BMI, die über die gesetzlichen Bestimmungen hinausgeht.

### **Datenschutz**

Die Vorschriften des Datenschutzes werden durch die Rechtsabteilung vorgegeben und kontrolliert, der Datenschutz entspricht den jeweils geltenden gesetzlichen Vorschriften.

### **Kosten und Gebühren**

Der Erwerb und die Verwendung der Zertifikate sind mit keinen Gebühren verbunden.

---

## **Abläufe in Kurzform**

### **Antrag**

Der Antrag auf Ausstellung eines Zertifikats erfolgt bei BMI, IV/2/e, Berggasse 43, 1090 Wien, bzw. +43 (01) 90600 39629.

Das Antragsformular ist verfügbar unter <http://portal.bmi.gv.at/ref/pki/portalCA/Antragsformular.html>

## **Registrierung**

Nur Behörden mit entsprechenden Anwendungen des Portalverbundes sind zu diesem zugelassen und können dafür benötigte Zertifikate erhalten.

## **Bestellung/Request**

Nach erfolgreicher Registrierung erhält der Antragsteller Unterlagen über den Bestellvorgang, bzw. die Erzeugung eines Requests.

Der Besteller kann zwischen PKCS#12 und Java Key Store wählen, die Keys können selbst erzeugt oder von der IT-MS generiert und mit dem Zertifikat ausgeliefert werden.

## **Zertifikatserstellung**

Die Zertifikate werden in 14tägigem Rhythmus erstellt und auf Disketten ausgeliefert.

## **Installation openssl**

Das Werkzeug der Wahl für die Handhabung von Keys und Zertifikaten ist openssl. OpenSSL wird auf allen wesentlichen Plattformen (Unix, Linux, Windows, Mac OS, VMS) unterstützt. Installation ist einfach, unter normalen Umständen werden nur wenige Funktionen benötigt (Key-Generierung, Request-Erzeugung, Prüfung von Zertifikaten, Tests, Konvertierungen)

Alternativ können verschiedene Java Tools verwendet werden, so etwa die Standard Java Security Classes und das Java Key Tool oder die IAIK Tools, die einen weit größeren Funktionsumfang haben, aber lizenziert werden müssen.

## **System Hardening, Sicherheitsmaßnahmen**

Dazu gehören Firewall, Rechteverwaltung, minimierte Installation, Intrusion Detection, Logging, Backups, Monitoring.

Wichtig ist zum Beispiel auch, dass nur die notwendigen Module des verwendeten Webservers installiert sind.

## **Installation des Zertifikats**

Je nach verwendeter Server-Software werden auf unterschiedliche Weise das benötigte Root-Certificate und das Client Certificate des Servers eingespielt und konfiguriert. Zugriffsrechte auf das Key-File minimieren!

## **Überprüfung**

Nicht nur die Gültigkeit des Zertifikats muss geprüft werden – sinnvollerweise bietet sich ein Test des Gesamtsystems an, bei dem auch die Zertifikate geprüft werden.

Beim Ablauf dieser Prüfung bietet IT-MS (BMI) ihre Unterstützung an.

## **Certificate Revocation List**

Die Certificate Revocation List wird seitens IT-MS gewartet. Die Liste wird bei jeder Veränderung erneuert, zusätzlich zu den zeitgesteuerten Erneuerungen der Liste.

## **Sperrung**

Im Falle eines Einbruchs auf dem Server, beziehungsweise anderen Missbrauchs des Zertifikates hat der Systemadministrator die IT-MS umgehend zu informieren, um die Sperrung des betroffenen Zertifikats zu veranlassen.

## **Zertifikatserneuerung**

Die Verlängerung ist ein Monat vor Ablauf des aktuellen Zertifikats zu beantragen, Formular unter <http://portal.bmi.gv.at/ref/pki/portalCA/cert-verlaengerung.html>

## **Schlüsselerneuerung**

Im Falle eines Einbruchs oder anderen Missbrauchs des Zertifikats wird nach einer Sperrung des betroffenen Zertifikats ein neues Schlüsselpaar erstellt, auf dem das neue Zertifikat basiert.

## **Deinstallation**

Wenn der betroffene Portalverbund-Server nicht mehr seine Funktion wahrnimmt, muss das Zertifikat gesperrt und deinstalliert werden.

---

## **Definitionen**

In zukünftigen Versionen dieses Dokuments wird ein Glossar enthalten sein.