



Peter Brügger

25. März 2013

# Ausführungsbestimmungen der Zertifizierungsrichtlinien (Certification Practice Statement (CPS))

## AdminPKI KlasseCC-Enterprise

**Projektname:** AdminPKI-KlasseCC-Enterprise

**Projektnummer:**

**Version:** V1.00

Status                      in Arbeit                      in Prüfung                      genehmigt zur Nutzung  
       

Beteiligter Personenkreis	
Autoren:	Peter Brügger
Prüfung:	BPSR, BSDAM, BZOD
Genehmigung:	FFB
Benützer/Anwender:	Benutzer der Klasse CC-Enterprise PKI
zur Information/Kennntnis:	-

Änderungskontrolle, Prüfung, Genehmigung			
Wann	Version	Wer	Beschreibung
12.06.2012	X 0.8	Peter Brügger	Neues Dokument (Anpassung des Dokumentes AdminPKI_KlasseC-Enterprise_CPS
09.07.2012	X0.9	Peter Brügger	Feedback von BZOD (Mario Muster),und BSDAM (Markus Von Arburg, Nicolai Brignoli , Jacques Morand) eingearbeitet
20.09.2012	X0.97	Peter Brügger	Feedback von Roger Solioz eingearbeitet
10.12.2012	X0.99	Peter Brügger	Feedback Marc Scherler u. Mario Muster eingearbeitet
04.02.2013	X1.00	Peter Bruegger	Review FFB:Kapitel 5.4: Zertifizierungen präzisiert
25.03.2013	V1.00	Markus Vonarburg	Freigabe durch FFB

## Inhaltsverzeichnis

<b>1</b>	<b>Allgemeines</b> .....	<b>5</b>
1.1	Zweck des Dokumentes .....	5
1.2	Abgrenzung.....	5
1.3	Anwendungsbereich .....	5
1.4	Sprachregelung .....	5
<b>2</b>	<b>Allgemeine Massnahmen</b> .....	<b>6</b>
2.1	Pflichten des Betreibers.....	6
2.2	Pflichten des Zertifikatnehmers.....	6
2.3	Rechtliche Grundlagen .....	7
2.4	Haftung.....	7
2.5	Kosten .....	7
2.6	Veröffentlichung.....	7
2.7	Audits .....	8
<b>3</b>	<b>Einführung</b> .....	<b>9</b>
3.1	Übersicht .....	9
3.2	Teilnehmer der PKI.....	10
3.2.1	Zertifizierungshierarchie.....	10
3.2.2	Root Certification Authority (RootCA).....	10
3.2.3	Issuing Certification Authority (IssuingCA) .....	10
3.2.4	Registrierstellen .....	11
3.1.1	Informationsdienst.....	11
3.2.5	Zertifikatsanwender.....	11
3.2.6	Zertifikatsinhaber .....	11
3.2.7	Key Archiving.....	11
3.2.8	Kunden der AdminPKI KlasseCC-Enterprise.....	11
3.3	Zertifikatsverwendung.....	12
3.3.1	Freigegebene Zertifikatsverwendung .....	12
3.3.2	Untersagte Zertifikatsverwendung.....	12
3.4	Verwaltung der Policy .....	12
3.4.1	Organisation der Dokumentenverwaltung .....	12
3.4.2	Kontaktperson.....	12
3.4.3	Genehmigungsverfahren.....	12
<b>4</b>	<b>Publikation und Verzeichnisdienst</b> .....	<b>13</b>
4.1	Verzeichnisdienste.....	13
4.2	Publikation der CPS.....	13
4.3	Publikation der CRL.....	13
4.4	Ausbreiten von Zertifikaten .....	13
<b>5</b>	<b>Identifikation und Authentifikation</b> .....	<b>14</b>
5.1	Namensgebung .....	14
5.2	Überprüfung der Identität für Maschinenzertifikate.....	14
5.3	Überprüfung der Identität für Webserver und ConfigMgr Zertifikaten .....	14
5.4	Zertifizierungen.....	14
<b>6</b>	<b>Organisatorische Anforderungen</b> .....	<b>15</b>
6.1	Zertifikatsantrag.....	15
6.2	Zertifikatsausstellung (Issue) .....	15
6.3	Erneuerung (Renew) .....	15
6.4	Sperrung (Revoke) .....	15
6.5	Beendigung für die Bezugberechtigung .....	16
6.6	Antrag und Ausstellung von Webserver und ConfigMgr Zertifikaten .....	16

## Ausführungsbestimmungen der Zertifizierungsrichtlinien für die AdminPKI-KlasseCC-Enterprise

<b>7</b>	<b>Physische Sicherheit, Sicherheit der Abläufe und des Personals .....</b>	<b>17</b>
7.1	Kontrolle der physischen Sicherheit.....	17
7.1.1	Lokalität .....	17
7.1.2	Zugangskontrolle .....	17
7.1.3	Stromversorgung und Klimatisierung .....	17
7.1.4	Wasserschaden .....	17
7.1.5	Vorbeugung und Schutz vor Feuer.....	17
7.1.6	Ablage der Datenträger.....	17
7.1.7	Entsorgung .....	18
7.1.8	Ablage ausserhalb der Gebäudes.....	18
7.2	Kontrolle der Arbeitsabläufe.....	18
7.2.1	Vertrauensfunktionen (Rollen).....	18
7.2.2	Anwendungsverantwortlicher (AV) .....	18
7.2.3	Serviceverantwortlicher (SV).....	18
7.2.4	Betriebsverantwortlicher (BV).....	18
7.2.5	Sicherheitsverantwortlicher .....	19
7.3	Personelle Sicherheit.....	19
7.3.1	Sicherheitsprüfung des Personals.....	19
7.3.2	Notwendige Anzahl Personen zur Erfüllung der Aufgaben .....	19
7.4	Audit .....	19
<b>8</b>	<b>Technische Sicherheit .....</b>	<b>20</b>
8.1.1	Schlüsselerzeugung.....	20
8.2	Publikation der Zertifikate und CRL .....	20
8.3	Schutz der privaten Schlüssel.....	20
8.3.1	HSM für Schlüsselmaterial der Root CA der KlasseCC-Enterprise.....	20
8.3.2	HSM für Schlüsselmaterial der Subordinate CA's der KlasseCC-Enterprise.	20
8.4	Berechtigungen auf der CA.....	20
8.5	Datenschutz und Datensicherheit .....	21
<b>9</b>	<b>Profile der Zertifikate und der CRL .....</b>	<b>22</b>
9.1	Zertifikate.....	22
9.2	Suspendierungs- und Revokationslisten CRL.....	22
9.2.1	Basis-Felder der CRL.....	22
9.2.2	Erweiterungen der CRL und der CRL-Einträge .....	22

## Abkürzungsverzeichnis

BIT	Bundesamt für Informatik und Telekommunikation
CA	Certificate Authority, Zertifizierungsstelle
CPS	Certification Practice Statement, Ausführungsbestimmungen der Zertifizierungsrichtlinien
CP	Certificate Policy, Zertifizierungsrichtlinien
FFB	Gremium Führung Forest Bund im Auftrag des IRB
IRB	Informatikrat Bund
LE	Leistungserbringer
MAC	Move-Add-Change Prozess des LE BIT
PXE	Preboot eXecution Environment
SCCM	Microsoft System Center Configuration Manager
HSM	Hardware Storage Module

## Referenzierte Dokumente

P018, Security Massnahmen Forest Bund, IRB

# **1 Allgemeines**

## **1.1 Zweck des Dokumentes**

Das vorliegende Dokument stellt die Ausführungsbestimmungen der Zertifizierungsrichtlinien (auch CPS genannt) der AdminPKI Klasse CC-Enterprise des Bundesamtes für Informatik und Telekommunikation (BIT) dar. Es beschreibt die Verfahren<sup>1</sup>, welche die Zertifizierungsstelle AdminPKI KlasseC-Enterprise verwendet, um Klasse CC-Enterprise Zertifikate auszugeben.

Diese Richtlinien gelten für Zertifikate, welche von der AdminPKI Klasse CC-Enterprise ausgestellt werden und definiert die Ausgabe und Verwaltung der zertifikatbasierten Public Key Infrastructure (PKI). Ebenfalls werden die an die Ausgabe und Verwaltung gebundenen Prozesse bezüglich der Registrierung von Daten von Zertifikatnehmern, der Verwendungszweck der Zertifikate, die Sperrung und Erneuerung im Detail beschrieben.

Diese Ausführungsbestimmungen wurden erstellt für den AdminPKI Klasse CC-Enterprise Serviceverantwortlichen, für die Mitarbeiter der AdminPKI KlasseCC-Enterprise, für die Zertifikatsinhaber, welche ein Zertifikat besitzen, sowie für die Zertifikatsanwender, welche sich auf ein Zertifikat verlassen.

## **1.2 Abgrenzung**

Vorliegendes Dokument ist keine Einführung in die PKI-Technologie, CAs oder Zertifikate. Es wird vorausgesetzt, dass der Leser bereits über entsprechende PKI-Kenntnisse verfügt.

## **1.3 Anwendungsbereich**

Diese Zertifikatsrichtlinien gelten ausschliesslich für Zertifikate, welche von der AdminPKI Klasse CC-Enterprise zu ihrem bestimmten Zweck ausgestellt wurden.

Das CPS soll für sämtliche beteiligten Parteien als rechtsverbindliche Grundlage gelten.

## **1.4 Sprachregelung**

In der vorliegenden Richtlinie werden Ausdrücke wie Zertifikatsanwender, Zertifikatsnutzer, Besitzer, Manager und Administrator für männliche, weibliche und juristische Personen verwendet. Allgemeine Massnahmen

---

<sup>1</sup> Die Ausführungsbestimmungen der Zertifizierungsrichtlinien [CPS] sind eine ausführliche Beschreibung der Implementation der angebotenen Dienste und der geltenden Prozesse für die Verwaltung der Zertifikate. Die CPS ist ausführlicher als die von der Zertifizierungsstelle [CA] angewendeten Zertifizierungsrichtlinien [CP]. Eine Zertifizierungsrichtlinie stellt für die unter dieser CP verwalteten Zertifikate ein bestimmtes Sicherheitsniveau dar. Die Ausführungsbestimmungen der Zertifizierungsrichtlinien geben Auskunft wie die Zertifizierungsstelle dieses Sicherheitsniveau sicherstellt.

## 2 Allgemeine Massnahmen

### 2.1 Pflichten des Betreibers

Der Betreiber der AdminPKI Klasse CC-Enterprise ist für die nachfolgend beschriebenen Punkte verpflichtet:

- Veröffentlichung und Verwalten der CRL (Certificate Revocation List), des CPS (Certificate Practice Statement) und der CP (Certificate Policies).
- Nur Daten von Personen und Organisationen zu verwalten, zu verarbeiten und zu nutzen, die zum Betreiben der CA erforderlich sind.
- Alle Personen- und Organisationsdaten, die nicht veröffentlicht werden, vor unbefugtem Zugriff zu schützen und sicher zu verwahren.
- Den Antragssteller zu informieren, wenn ein Zertifikat ausgestellt oder zurückgezogen wurde.
- Dritte über den Widerruf von Zertifikaten zu informieren.

### 2.2 Pflichten des Zertifikatnehmers

Die ausgestellten Zertifikate sind lediglich für den dafür vorgesehenen Zweck einzusetzen.

Die Zertifikatnehmer sind für die Sicherheit der privaten Schlüsselkomponenten in ihrem Besitz verantwortlich. Um die Sicherheit zu gewährleisten, hat der Zertifikatnehmer insbesondere auf folgendes zu achten:

- Sicheres Aufbewahren des Schlüssels nach Erhalt.
- Liefern von korrekten und vollständigen Angaben bei der Antragsstellung.
- Unverzüglich anzeigen, falls die Angaben in seinem Zertifikat nicht mehr den Tatsachen entsprechen.
- Das ausgestellte Zertifikat ausschliesslich für den dafür vorgegebenen Verwendungszweck einzusetzen.
- Geeignete Massnahmen zu treffen um das System, auf welchem die Zertifikate genutzt und eingesetzt werden zu schützen (Virenschutz, Zugangsbeschränkungen usw.).
- Bei Kompromittierung des Zertifikates oder Verlust des Schlüssels unverzüglich Kontakt mit der ausstellenden Instanz aufnehmen, um das Schlüsselpaar sperren zu lassen.

Zusätzlich sind alle Zertifikatnehmer dazu verpflichtet, ihren privaten Schlüssel und die zugehörigen persönlichen Informationen geheim zu halten und nicht an unbefugte Dritte weiterzugeben.

## **2.3 Rechtliche Grundlagen**

Die vorliegenden Vereinbarungen der AdminPKI CC-Enterprise mit ihrem Personal, den RAO (Registration Authority Operator), den Zertifikatnehmern und Dritten CAs oder PKIs basieren auf folgenden rechtlichen Grundlagen:

- Verordnung über Dienste der elektronischen Zertifizierung vom 12. April 2000
- Regierungs- und Verwaltungsorganisationsgesetz (RVOG) vom 21. März 1997
- Bundesinformatikverordnung BInfV vom 23. Feb. 2000 (Stand 2012)
- Bundesgesetz über Datenschutz (Stand 3. Oktober 2000)
- Allgemeine Geschäftsbedingungen des Bundes (AGB)
- Bundesratsbeschluss vom 4. Juni 2010  
betreffend Einführung von *Zwei-Faktor Authentifikation der Benutzer bis Ende 2013*

## **2.4 Haftung**

Das Bundesamt für Informatik und Telekommunikation (BIT) lehnt ausdrücklich jede Haftung bei der Verwendung der AdminPKI CC-Enterprise Zertifikate oder der dazugehörigen Schlüssel für andere Zwecke als die in diesem Dokument genannt sind ab.

Zusätzliche Haftungsbestimmungen sind in den Allgemeinen Geschäftsbedingungen des Bundes beschrieben und geregelt. Die AGB des Bundes stützen sich in wesentlichen Fragen auf das Obligationenrecht.

## **2.5 Kosten**

Für die Nutzung der Dienste der AdminPKI KlasseCC-Enterprise entstehen für die Nutzer derzeit keine Kosten.

## **2.6 Veröffentlichung**

Alle Veröffentlichungen hinsichtlich des Betriebs der AdminPKI KlasseCC-Enterprise erfolgen im Intranet und Internet unter <http://www.pki.admin.ch/>.

In Ausnahmefällen kann eine direkte Nachricht an die beteiligten Personen mittels E-Mail übermittelt werden. Die E-Mail Nachrichten werden in diesem Fall digital signiert.

Das BIT veröffentlicht das CPS und CRLs (Certificate Revocation List) in regelmässigen Abständen, eine neue CRL wird nach jedem Zertifikatswiderruf neu veröffentlicht. Die aktuellen Ablageorte und Pfade können aus den Zertifikateinformationen entnommen werden.

## **2.7 Audits**

Interne Prüfungen des technischen Aufbaus der Infrastruktur sowie das Einhalten der Sicherheitsvorschriften, werden in unregelmässigen Abständen durch eine BIT interne Prüfstelle nach festgelegten Regeln durchgeführt. Die Ergebnisse eines solchen Audits werden nicht veröffentlicht.

## 3 Einführung

### 3.1 Übersicht

Die AdminPKI KlasseCC-Enterprise ist die Nachfolgerin der AdminPKI KlasseC-Enterprise, unterstützt aber nur noch Maschinenzertifikate. Personenzertifikate werden nicht mehr ausgegeben.

Für Personenzertifikate stehen folgende alternative Varianten zur Verfügung

- Klasse B Zertifikate auf Smart Card
- Zertifikate der Klasse C Trustcenter
- Windows integrierte Authentifikation
- Authentifikation mit Namen und Password,

Aktuell werden folgende Zertifizierungsrichtlinien unterstützt:

1. Die Richtlinie *AdminPKI KlasseCC-Enterprise* „Kerberos Authentication“ ersetzt das Template „Domain Controller Authentication“ und regelt die Verwaltung und Anwendung von Zertifikaten für die Authentifizierung mit Domain Controllern.
2. Die Richtlinie *AdminPKI KlasseCC-Enterprise* „Web Server SSL“ regelt die Verwaltung und Anwendung von Zertifikaten für die Verschlüsselung von Netzwerkverbindungen zu Servern mittels SSL.
3. Die Richtlinie *AdminPKI KlasseCC-Enterprise* „Workstation Authentication“ regelt die Verwaltung und Anwendung von Zertifikaten für die Authentifizierung interner Client-Computersysteme (Workstation, Notebook, mobile Geräte) am Netzwerk der Bundesverwaltung.
4. Die Richtlinie *AdminPKI-KlasseCC-Enterprise* „ConfigMgr Site Server Signing“ regelt die Verwaltung und Anwendung von Zertifikaten für die Signierung von Client Policies durch Microsoft SCCM Server.
5. Die Richtlinie *AdminPKI KlasseCC-Enterprise* „ConfigMgr OS Deployment“ regelt die Verwaltung und Anwendung von Zertifikaten für die Authentifizierung von neuen Client- und Server-Computersystemen, welche sich zwecks der Installation eines neuen Betriebssystems mittels PXE gestartet werden, gegenüber den Microsoft SCCM Servern.
6. Die Richtlinie *AdminPKI KlasseCC-Enterprise* „NPS“ ermöglicht eine gegenseitige Authentifizierung zwischen dem ACS ( Access Control Server) und dem NPS (Network Policy Server) des WLAN „direct“. t

Die einzelnen Zertifikatstypen werden ausschliesslich für den vorgesehenen Zweck (Key Usage) verwendet und nicht mit anderen Verwendungszwecken erweitert oder vermischt.

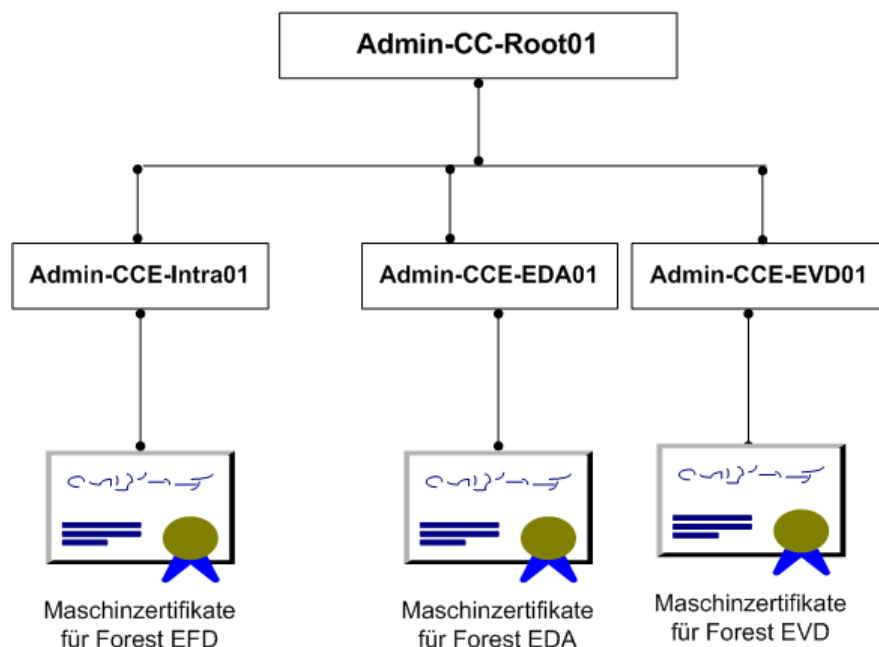
Die schweizerische Bundesverwaltung ist nicht verpflichtet, mit anderen Zertifizierungsstellen Vereinbarungen über die gegenseitige Anerkennung von Zertifikaten abzuschliessen.



## 3.2 Teilnehmer der PKI

### 3.2.1 Zertifizierungshierarchie

Die Ausgabe und Verwaltung von Zertifikaten der AdminPKI KlasseCC-Enterprise beruht auf einer zweistufigen, hierarchischen Infrastruktur:



### 3.2.2 Root Certification Authority (RootCA)

Die Aufgabe der RootCA **Admin-CC-Root01** auf der ersten Stufe ist die Validierung der Zertifikate der Zertifizierungsstellen der zweiten Stufe. Die RootCA stellt keine Teilnehmerzertifikate oder Maschinenzertifikate aus.

Die RootCA signiert ihr Zertifikat mit dem eigenen Schlüssel. Es existiert kein Zertifikat zur Verifikation der Authentizität des Zertifikates der RootCA. Die Verifikation muss auf einem andern Weg durchgeführt werden. Zum Beispiel kann der Zertifikatsanwender den Fingerprint des Zertifikats in seiner Applikation mit dem Fingerprint des publizierten Zertifikats vergleichen.

### 3.2.3 Issuing Certification Authority (IssuingCA)

Die IssuingCAs **Admin-CCE-Intra01** für den Forest Intra, **Admin-CCE-EDA01** für den Forest EDA und **Admin-CCE-EVD01** für den Forest EVD auf der zweiten Stufe generieren, validieren, publizieren, und verwalten die Zertifikate der Zertifikatsinhaber. Diese IssuingCAs unterscheiden sich nicht in den Zertifizierungsrichtlinien und in den Prozessen für die Ausgabe und Verwaltung der Zertifikate.

### **3.2.4 Registrierstellen**

In dieser PKI gibt es keine Registrierstellen im herkömmlichen Sinne. Die Ausstellung von Zertifikaten wird über die Zugehörigkeit zum Active Directory der Bundesverwaltung sowie über Gruppenmitgliedschaften und Berechtigungen auf den Zertifikatstemplates gesteuert. Siehe dazu auch die Kapitel 5 und 6.

### **3.1.1 Informationsdienst**

Der Informationsdienst dient der Publikation:

- der vorliegenden Ausführungsbestimmungen der Zertifizierungsrichtlinien
- der Zertifizierungsrichtlinien
- der CA Zertifikate
- der ‚Certificate Revocation List‘ (CRL) aller CA der AdminPKI KlasseCC-Enterprise
- der Prozessbeschreibungen
- der Formulare

Der Informationsdienst steht unter der Adresse <http://www.pki.admin.ch/> sowohl im Intranet als auch im Internet zur Verfügung.

### **3.2.5 Zertifikatsanwender**

Ein *Zertifikatsanwender* ist eine Person, die ein Zertifikat eines Zertifikatsinhabers verwendet.

### **3.2.6 Zertifikatsinhaber**

Ein Computersystem wird *Antragsteller* genannt, wenn sie direkt oder indirekt einen Antrag für ein Zertifikat stellt. Nach erfolgter Ausstellung wird das Computersystem als *Zertifikatsinhaber* bezeichnet. Im Zertifikat - nach X.509 - wird sie als *subject* bezeichnet.

### **3.2.7 Key Archiving**

Es wird kein Key-Archiving angeboten.

### **3.2.8 Kunden der AdminPKI KlasseCC-Enterprise**

Die Kunden der AdminPKI KlasseCC-Enterprise sind interne Computersysteme, welche in das Active Directory der Bundesverwaltung (Forest intra) integriert sind.

Zertifikate an Personen werden nur noch im Ausnahmefall angeboten. Vorgängig ist der Einsatz von Klasse B Zertifikaten auf Smart Card zu Prüfen.

## **Ausführungsbestimmungen der Zertifizierungsrichtlinien für die AdminPKI-KlasseCC-Enterprise**

Sha256 wird als default Hash Algorithmus eingesetzt, darum wird der Einsatz von Windows 7 oder Windows Server 2008 Systemen oder neuer vorausgesetzt.

### **3.3 Zertifikatsverwendung**

#### **3.3.1 Freigegebene Zertifikatsverwendung**

Die Zertifizierungsrichtlinien und die Anwendungen werden durch den FFB freigegeben. Die Liste der autorisierten Anwendungen steht im Informationsdienst (siehe 3.2) zur Verfügung.

#### **3.3.2 Untersagte Zertifikatsverwendung**

Die Zertifikatsinhaber sind in keiner Weise autorisiert, im Namen der schweizerischen Bundesverwaltung kommerzielle Transaktionen oder rechtsgültige Unterschriften gem. dem Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) vorzunehmen.

### **3.4 Verwaltung der Policy**

#### **3.4.1 Organisation der Dokumentenverwaltung**

Das vorliegende CPS wird durch den AdminPKI KlasseCC-Enterprise Serviceverantwortlichen verwaltet. Unter der Adresse <http://www.pki.admin.ch> wird die gültige Version des vorliegenden CPS und die gültigen Versionen der Zertifizierungsrichtlinien (CPs) publiziert.

#### **3.4.2 Kontaktperson**

Das vorliegende CPS steht unter der Leitung des AdminPKI KlasseCC-Enterprise Serviceverantwortlichen:

AdminPKI KlasseCC-Enterprise Serviceverantwortlicher  
Bundesamt für Informatik und Telekommunikation  
Monbijoustrasse 74  
CH-3003 Bern

#### **3.4.3 Genehmigungsverfahren**

Die vorliegende CPS wird vom FFB genehmigt.

Der AdminPKI KlasseCC-Enterprise Serviceverantwortliche kann typographische Anpassungen oder Neuformulierungen von Abschnitten ohne inhaltliche Änderungen an der vorliegenden CPS vornehmen und publizieren. Der FFB wird nachträglich darüber informiert, Einsprachen sind dann möglich.

Grössere Änderungen oder neue Dokumentversionen sind in jedem Fall durch den FFB genehmigungspflichtig.

## 4 Publikation und Verzeichnisdienst

### 4.1 Verzeichnisdienste

Als Verzeichnisdienste stehen das Active Directory der verschiedenen Forests der BVerw sowie interne und externe (Internet) Web Server der BVerw zur Verfügung.

Die Maschinenzertifikate werden im Normalfall nicht in Active Directory publiziert.

Die Listen der revozierten und suspendierten Zertifikate (CRL) werden im Active Directory und auf einem HTTP-Server unter <http://www.pki.admin.ch/> publiziert.

### 4.2 Publikation der CPS

Das CPS wird sowohl auf einem internen als auch auf einem externen (Internet) Web Server der BVerw unter <http://www.pki.admin.ch> publiziert.

### 4.3 Publikation der CRL

Die CRL der IssuingCAs haben eine Gültigkeit von sieben Tagen. Die Gültigkeit der CRL der RootCA beträgt ein Jahr.

Der Publikationsintervall der der Root CA CRL beträgt 1 Jahr

Der Publikationsintervall der der Issuing CA CRL beträgt 7 Tage. Alle 2 Std wird mittels eines Scripts eine CRL generiert und auf die Publikationsserver. kopiert

### 4.4 Ausbreiten von Zertifikaten

- Schwerpunktmässig werden Zertifikate der Issuing CA's der KlasseCC-Enterprise mittels autoenrollment ausgebreitet.
- Ist autoenrollment nicht möglich kann als nächste Option das Enrollment über den Zertifikatsmanager (certreq.msc) eingesetzt werden.

Erst als dritte Möglichkeit darf das manuelle enrollment mit certreq.exe in Betracht gezogen werden.

Die CPS darf mit keiner Methode verletzt werden.

## 5 Identifikation und Authentifikation

### 5.1 Namensgebung

Im Zertifikat steht im Subject Name der *common name* und im Alternative Subject Name der *DNS-Name* aus dem Active Directory des Zertifikatsinhabers. Davon ausgenommen sind die unter Abschnitt 5.3 aufgeführten Zertifikate

### 5.2 Überprüfung der Identität für Maschinenzertifikate

Die AdminPKI KlasseCC-Enterprise nimmt selber keine eigene Prüfung der Identität vor. Die AdminPKI KlasseCC-Enterprise verlässt sich auf die Prüfung, welche im Rahmen der Aufnahme von Computersystemen im Windows Active Directory Domain der Bundesverwaltung stattfindet. Das gleiche gilt bei der Mutation von Computern und Rechten.

Für die Regelung betreffend ‚Webserver SSL‘, ‚ConfigMgr OS Deployment‘ und ‚ConfigMgr Site Server Signing‘ Zertifikaten gilt der nachfolgende Abschnitt 5.3.

### 5.3 Überprüfung der Identität für Webserver und ConfigMgr Zertifikaten

Im Falle von ‚Webserver SSL‘, ‚ConfigMgr OS Deployment‘ und ‚ConfigMgr Site Server Signing‘ Zertifikaten nimmt AdminPKI KlasseC-Enterprise eine Prüfung der Identität des Antragstellers über den vorhandenen Computer-Account im Forest intra vor. Der Antragsteller muss seinen Antrag signiert dem Betrieb CA zukommen lassen.

### 5.4 Zertifizierungen

Die AdminPKI Klasse CC-Enterprise gibt keine Zertifikate mit digitaler rechtsverbindlicher Signature oder Extended-Validation-SSL-Zertifikate heraus (sichtbar an der grün-hinterlegten Adresszeile des Browsers).

## 6 Organisatorische Anforderungen

### 6.1 Zertifikatsantrag

Der Zertifikatsantrag ist implizit im Auftrag zur Erstellung oder Änderung eines Accounts resp. zur Aufnahme eines Computersystems im Windows Active Directory Domain der Bundesverwaltung enthalten.

Für die Beantragung von ‚Webserver SSL‘, ‚ConfigMgr OS Deployment‘ und ‚ConfigMgr Site Server Signing‘ Zertifikaten geben die Abschnitte 5.3 + 6.6 Auskunft.

### 6.2 Zertifikatsausstellung (Issue)

Als Basis für den Ausstellungsprozess, wird die Funktionalität der Microsoft Enterprise PKI genutzt, welche die Möglichkeit des automatischen Registrierungs- und Ausstellungsvorgangs (Autoenrollment) zur Verfügung stellt. Anhand von Berechtigungen auf den definierten Zertifikatstemplaten, sowie von Gruppenmitgliedschaften und Group Policy Object (GPO) wird detailliert festgelegt, welche Computer Systeme ein entsprechendes Zertifikat erhalten sollen.

Mit diesen definierten Kontrollmechanismen, zusammen mit dem Vorhandensein eines entsprechenden User- oder Computer-Objekts im Active Directory der Bundesverwaltung und verbunden der definierten Namensgebung (siehe dazu Abschnitt 5.1) im Zertifikat wird die Vertrauenswürdigkeit garantiert.

Für die Ausstellung von ‚Webserver SSL‘, ‚ConfigMgr OS Deployment‘ und ‚ConfigMgr Site Server Signing‘ Zertifikaten gilt der Abschnitt 6.6.

### 6.3 Erneuerung (Renew)

Die Erneuerung der Zertifikate erfolgt analog dem Ausstellungsprozess automatisch und transparent über Autoenrollment, sofern die in Abschnitt 6.2 definierten Kriterien erfüllt sind.

Zertifikate des Typs ‚Webserver SSL‘, ‚ConfigMgr OS Deployment‘ und ‚ConfigMgr Site Server Signing‘ müssen neu beantragt werden (siehe dazu Abschnitt 6.6).

### 6.4 Sperrung (Revoke)

Die Sperrung eines Zertifikates wird zurzeit zentral im Auftrage des zuständigen Administrators des LEs durch das BIT erbracht und direkt auf der Certification Authority (CA) vorgenommen. Das BIT garantiert eine Sperrung, wenn ein Verdacht auf Komprimierung des Schlüssels vorliegt. Ebenfalls behält sich das BIT vor, ausgestellte Zertifikate aufgrund von Defekten oder Störungen im Zusammenhang mit dem Public und Private Key zu sperren. Die zugehörigen Formulare sind auf der Webseite <http://www.pki.admin.ch> unter dem Abschnitt ‚Zertifikatstypen/Klasse CC-Enterprise/Formulare‘ zu finden.

## **Ausführungsbestimmungen der Zertifizierungsrichtlinien für die AdminPKI-KlasseCC-Enterprise**

Die gesperrten Zertifikate werden über eine webbasierende Certificate Revocation List (CRL) veröffentlicht. In der Regel wird ein gesperrtes Zertifikat, sofern die in Abschnitt 6.2 definierten Kriterien erfüllt sind, umgehend durch ein neues ersetzt. Zertifikate des Typs ‚Webserver SSL‘, ‚ConfigMgr OS Deployment‘ und ‚ConfigMgr Site Server Signing‘ müssen hingegen neu beantragt werden (siehe dazu Abschnitt 5.3).

### **6.5 Beendigung für die Bezugberechtigung**

Bei Austritt eines Mitarbeiters wird über die Sperrung (und späteres Löschen) des Windows Active Directory Domain Accounts auch die Nutzung der Zertifikate eingestellt. Die Sperrung/Löschung wird durch den zuständigen Administrator des LEs durchgeführt.

### **6.6 Antrag und Ausstellung von Webserver und ConfigMgr Zertifikaten**

Wie für alle ausgegebenen Maschinenzertifikate müssen die Server oder Workstation Member des Forest's sein

Der Administrator des Serversystems erstellt mit dem Zertifikatsmanager (certmgr.msc) Seite einen Request an die AdminPKI KlasseCC-Enterprise. Der CA Betrieb, gibt den pending Request frei und stellt damit das Zertifikat aus und schickt dieses dem Antragsteller per Mail zu. Die Installation des Zertifikats auf dem Serversystem erfolgt anschliessend durch den Administrator.

Eine Anleitung für das manuelle Enrollment ist auf [www.pki.admin.ch](http://www.pki.admin.ch) unter dem Abschnitt „Zertifikatstypen/Klasse CC-Enterprise/Anleitungen“ verfügbar.

Im Feld "Value" von „Subject der Certificate Properties“ vom Zertifikatsmanager muss zwingend der *DNS Name des Serversystems* resp. die *URL der Webseite* eingegeben werden.

Mit diesen definierten Kontrollmechanismen, zusammen mit dem Vorhandensein eines entsprechenden Computer-Objekts im Active Directory der Bundesverwaltung und verbunden mit der definierten Namensgebung (siehe dazu Abschnitt 5.1) im Zertifikat wird die Vertrauenswürdigkeit garantiert.

## **7 Physische Sicherheit, Sicherheit der Abläufe und des Personals**

### **7.1 Kontrolle der physischen Sicherheit**

Es gilt generell der Bundesstandard ‚Security Massnahmen Forest Bund (P018)‘ des IRB [1].

#### **7.1.1 Lokalität**

Die AdminPKI KlasseCC-Enterprise wird in den RZ-Räumen des BIT in der gleichen Sicherheitszone betrieben wie die Domaincontroller für das Active Directory der Bundesverwaltung. Eine zweite, identisch aufgebaute Anlage befindet sich im Rechenzentrum am KaVor Standort des BIT. Bei beiden Rechenzentren handelt es sich um Sicherheitszonen mit restriktivem Zutritt.

#### **7.1.2 Zugangskontrolle**

Es haben nur namentlich bekannte Personen mit einem persönlichem Badge Zutritt zu den RZ-Räumlichkeiten. Sämtliche Zugänge werden durch Videokameras überwacht. Generell gilt die Weisung für die Zugangskontrolle zum Rechenzentrum des BIT.

#### **7.1.3 Stromversorgung und Klimatisierung**

Die RZ-Räume des BIT sind mit einer Klimaanlage für die Regulierung von Temperatur und Feuchtigkeit ausgerüstet. Alle elektrischen Komponenten sind an eine unterbrechungsfreie Stromversorgung angeschlossen.

#### **7.1.4 Wasserschaden**

Die RZ-Räume des BIT sind mit Wassermeldern ausgerüstet, welche direkt mit dem Überwachungszentrum des Gebäudes verbunden sind. Bei einem Alarm werden die Systeme automatisch heruntergefahren und die Stromzufuhr wird unterbrochen.

#### **7.1.5 Vorbeugung und Schutz vor Feuer**

Die RZ-Räume des BIT sind mit Rauchmeldern ausgerüstet, welche alle direkt mit dem Überwachungszentrum des Gebäudes verbunden sind. Bei einem Brandmeldealarm werden die Systeme automatisch abgeschaltet und die Stromzufuhr wird unterbrochen.

#### **7.1.6 Ablage der Datenträger**

Datenträger, welche Informationen im Zusammenhang mit der PKI enthalten, einschliesslich Sicherheitskopien, werden in einem feuersicheren Tresor im Rechenzentrum des BIT aufbewahrt.



## **Ausführungsbestimmungen der Zertifizierungsrichtlinien für die AdminPKI-KlasseCC-Enterprise**

### **7.1.7 Entsorgung**

Alle Papierdokumente und Datenträger, die zu entsorgen sind, werden in einem für klassifizierte Dokumente geprüften Aktenvernichter vernichtet.

### **7.1.8 Ablage ausserhalb der Gebäudes**

Schützenswerte Dateien werden an zwei verschiedenen Standorten aufbewahrt.

## **7.2 Kontrolle der Arbeitsabläufe**

### **7.2.1 Vertrauensfunktionen (Rollen)**

Die folgenden Rollen sind allgemein beschrieben. Eine detailliertere Beschreibung befindet sich im Organisationshandbuch der AdminPKI KlasseCC-Enterprise.

### **7.2.2 Anwendungsverantwortlicher (AV)**

Der AV ist generell verantwortlich für Implementation, Koordination und Verwaltung der AdminPKI KlasseCC-Enterprise. Er entscheidet über die Eingaben des Serviceverantwortlichen und anderer Antragssteller betreffend aller Veränderungen an der Konfiguration oder den Betriebsprozessen mit domänenübergreifenden Auswirkungen und stellt sicher, dass solche Veränderungen ohne Funktionsbeeinträchtigungen oder Ausfälle der Büroautomation erfolgen.

### **7.2.3 Serviceverantwortlicher (SV)**

Der SV ist gegenüber dem AV verantwortlich für die Einhaltung der in der SLA (Service Level Agreement) getroffenen Vereinbarungen betreffend der AdminPKI KlasseCC-Enterprise. Er vertritt diese PKI in Gremien und gegenüber den Leistungserbringern. Für diese PKI trägt er die Budgetverantwortung.

Gleichzeitig ist er verantwortlich für die Weiterentwicklung, die Erweiterung und die Anpassung an der AdminPKI KlasseCC-Enterprise nach Anforderungen des Anwendungsverantwortlichen, für den Unterhalt der CPS, CP und der Zertifikatstemplates sowie für die Führung der OID Liste.

### **7.2.4 Betriebsverantwortlicher (BV)**

Der Betriebsverantwortliche ist gegenüber dem Serviceverantwortlichen verantwortlich für die Installation, den Betrieb und die Verfügbarkeit der AdminPKI KlasseCC-Enterprise gemäss OLA (Operation Level Agreement). Er koordiniert die bereichsübergreifende Problembehebung. Zudem ist er zuständig für den Unterhalt der Betriebsdokumente.

### **7.2.5 Sicherheitsverantwortlicher**

Der Sicherheitsverantwortliche ist gegenüber dem Serviceverantwortlichen verantwortlich für die regelmässige Überprüfung der Logdateien des Betriebs der AdminPKI KlasseCC-Enterprise auf Unregelmässigkeiten sowie für die Durchführung von Securityaudits.

## **7.3 Personelle Sicherheit**

### **7.3.1 Sicherheitsprüfung des Personals**

Das Personal der AdminPKI KlasseCC-Enterprise besteht aus internen Mitarbeitern des BIT. Sie verfügen über die notwendige Qualifikation und Erfahrung, um die Zertifizierungsdienstleistung zu erbringen. Jeder Mitarbeiter wird persönlich durch den Betriebsverantwortlichen über den Umfang und die Grenzen seines Verantwortlichkeitsbereiches unterrichtet. Der Arbeitsvertrag jedes Mitarbeitenden enthält eine Vertraulichkeits-Klausel. Alle Mitarbeiter haben eine Sicherheitsüberprüfung erfolgreich bestanden (erweiterte Sicherheitsprüfung gem. PSPV Art. 11 vom 19. Dezember 2001).

### **7.3.2 Notwendige Anzahl Personen zur Erfüllung der Aufgaben**

Die nachfolgenden Prozesse verlangen bei ihrer Ausführung die gleichzeitige Anwesenheit von mindestens zwei Personen mit verschiedenen Rollen:

- Generierung eines CA-Schlüssels
- Backup und Recovery eines CA-Schlüssels
- Austausch von Hardware welche CA-Schlüssel enthält

Die beiden Personen sind zu gleichen Teilen verantwortlich für den Schutz der Informationen und Credentials, welche bei sensiblen Transaktionen benötigt werden.

Alle anderen Aufgaben dürfen von einer autorisierten Person alleine ausgeführt werden.

## **7.4 Audit**

Es werden alle CA relevanten Ereignisse geloggt und während 180 Tage aufbewahrt.

## 8 Technische Sicherheit

### 8.1.1 Schlüsselerzeugung

Die Schlüssel für die CAs werden in einem mindestens nach FIPS 140-2 Level 2 zertifizierten Hardware Security Modul (HSM) generiert und gespeichert.

Die Schlüssel für die Zertifikatsinhaber werden auf dem CA Server erzeugt und dem Zertifikatsinhaber mittels Autoenrollement zugestellt. Die Zertifikate werden in der Datenbank der CA gespeichert.

### 8.2 Publikation der Zertifikate und CRL

Die Zertifikate der CAs und die CRL stehen ebenfalls im Active Directory und zusätzlich auf einem internen sowie einem externen (Internet) WebServer unter <http://www.pki.admin.ch> zur Verfügung.

### 8.3 Schutz der privaten Schlüssel

Die Schlüssel und das Zertifikat werden in einem geschützten Bereich (Encrypted Data Store) des jeweiligen Systems gespeichert. Die Schlüssel sind durch das Windows Logon geschützt.

#### 8.3.1 HSM für Schlüsselmaterial der Root CA der KlasseCC-Enterprise

Das Schlüsselmaterial (Zertifikate und private Key) der Root CA wird auf HSM erstellt und abgelegt

#### 8.3.2 HSM für Schlüsselmaterial der Subordinate CA's der KlasseCC-Enterprise

Schlüsselmaterial (Zertifikate und private Key) von Subordinate CA's des CA Typ's „Microsoft Enterprise“ wird auf HSM generiert und abgelegt.

Schlüsselmaterial (Zertifikate und private Key) von Subordinate CA's des CA Typ's, „Microsoft Standalone“ können ohne HSM betrieben werden, wenn die Sicherheitsanforderungen der eingesetzten Anwendungen dies erlauben.

### 8.4 Berechtigungen auf der CA

Die Berechtigungen „Manage CA“ und „Manage and Issue Certificates“ wird von der Betriebsorganisation der CA nicht weitergegeben

## **8.5 Datenschutz und Datensicherheit**

Datenschutz, Datensicherheit und Risikoanalysen werden im Rahmen des Informationssicherheits- und Datenschutzkonzepts (ISDS) behandelt, welches durch das BIT erstellt wurde.

## 9 Profile der Zertifikate und der CRL

### 9.1 Zertifikate

Die Definition der Zertifikate befindet sich in der entsprechenden CP.

### 9.2 Suspendierungs- und Revokationslisten CRL

#### 9.2.1 Basis-Felder der CRL

Die Suspendierungs- und Revokationslisten enthalten die folgenden Felder:

version	1 (CRL nach Version 2)
signature	OID des Algorithmus mit dem die CRL signiert wurde
issuer	Distinguished Name DN de CA, welche die CRL signiert hat
thisUpdate	Zeitpunkt der Ausgabe der CRL
nextUpdate	Gültigkeit der CRL
revokedCertificate	Liste der revozierten und suspendierten Zertifikate

#### 9.2.2 Erweiterungen der CRL und der CRL-Einträge

Die folgenden Felder werden benützt:

nextPublish	Zeitpunkt, wann die nächste CRL publiziert wird
CRLNumber	jede CRL besitzt eine eigene fortlaufend ansteigende Nummer
reasonCode	gibt den Grund für die Revokation eines Zertifikates an; Applikationen können je nach verwendetem Eintrag unterschiedlich reagieren
invalidityDate	gibt den (vermuteten) Zeitpunkt an, seit dem der private Schlüssel kompromittiert ist oder das Zertifikat aus einem anderen Grund als ungültig angesehen werden muss