Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Büroautomation und Support

Martin Egger

26. Februar 2009

Ausführungsbestimmungen der Zertifizierungsrichtlinien (Certification Practice Statement (CPS))

AdminPKI KlasseC-Enterprise

Projektname: **PKI-KlasseC-Enterprise**

Projektnummer:

Version: **V1.3**

Status	in Arbeit	in Prüfung	genehmigt zur Nutzung
	☐	☐	☒

Beteiligter Personenkreis	
Autoren:	Johann Wiss, Martin Egger
Prüfung:	Peter Brügger
Genehmigung:	FFB
Benützer/Anwender:	Benutzer der Klasse C Enterprise PKI
zur Information/Kenntnis:	-

Änderungskontrolle, Prüfung, Genehmigung			
Wann	**Version**	**Wer**	**Beschreibung**
19.04.2006	X0.1	Johann Wiss	Neues Dokument
29.06.2006	V1.0	Martin Egger	Freigabe durch FFB
05.04.2007	V1.1	Martin Egger	Web Server SSL Zertifikat, Workstation Authentication Zertifikat, Neuformulierung Genehmigungsverfahren, div. Neuformulierungen Freigabe durch FFB
15.08.2007	V1.1.1	Martin Egger	Name der CA im Forest EVD angepasst
03.07.2008	V1.2	Martin Egger	Config Manager OS Deployment Zertifikat, Config Manager Site Server Signing Zertifikat Neuformulierung Key Recovery Freigabe durch FFB
26.02.2009	V1.3	Martin Egger	Neue Kapitel ‚Allgemeines' und ‚Allgemeine Massnah-

			men' eingefügt Freigabe durch FFB

Inhaltsverzeichnis

Abkürzungsverzeichnis

BIT	Bundesamt für Informatik und Telekommunikation
CA	Certificate Authority, Zertifizierungsstelle
CPS	Certification Practice Statement, Ausführungsbestimmungen der Zertifizierungs-richtlinien
CP	Certificate Policy, Zertifizierungsrichtlinien
FFB	Gremium Frührung 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

Referenzierte Dokumente

1 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 KlasseC-Enterprise des Bundesamtes für Informatik und Telekommunikation (BIT) dar. Es beschreibt die Verfahren[1], welche die Zertifizierungsstelle AdminPKI KlasseC-Enterprise verwendet, um KlasseC-Enterprise Zertifikate auszugeben.

Diese Richtlinien gelten für Zertifikate, welche von der AdminPKI KlasseC-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 KlasseC-Enterprise Serviceverantwortlichen, für die Mitarbeiter der AdminPKI-KlasseC-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 KlasseC-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.

[1] Die Ausführungsbestimmungen der Zertifizierungsrichtlininen [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-KlasseC-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-KlasseC-Enterprise mit ihrem Personal, den RAO (Registration Authoritie 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 16. Mai 2000)
- Bundesgesetz über Datenschutz (Stand 3.Oktober 2000)
- Allgemeine Geschäftsbedingungen des Bundes (AGB)

2.4 Haftung

Das Bundesamt für Informatik und Telekommunikation (BIT) lehnt ausdrücklich jede Haftung bei der Verwendung der AdminPKI-KlasseC-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-KlasseC-Enterprise entstehen für die Nutzer derzeit keine Kosten.

2.6 Veröffentlichung

Alle Veröffentlichungen hinsichtlich des Betriebs der AdminPKI-KlasseC-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 KlasseC-Enterprise unterstützt aktuell folgende Zertifizierungsrichtlinien (Certificate Policy (CP)):

1. Die Richtlinie *AdminPKI-KlasseC-Enterprise - S/MIME* regelt die Verwaltung und Anwendung von Zertifikaten einerseits für die Verifikation und Integrität (Signatur) und andererseits zur Generierung von Chiffrierschlüsseln und deren Übermittlung (Chiffrierung) für EMail. Da beide Zertifikate für den Einsatz im Produkt SecureMessaging (Mail-Client) erstellt wurden und sich die Zertifikate im Wesentlichen nur in der Key Usage unterscheiden, wurde auf separate CPs verzichtet.

2. Die Richtlinie *AdminPKI-KlasseC-Enterprise - Domain Controller Authentication* regelt die Verwaltung und Anwendung von Zertifikaten für die Authentifizierung mit Domain Controllern.

3. Die Richtlinie *AdminPKI-KlasseC-Enterprise - IPSEC* regelt die Verwaltung und Anwendung von Zertifikaten für Authentifizierung mittels IPSec.

4. Die Richtlinie *AdminPKI-KlasseC-Enterprise – Web Server SSL* regelt die Verwaltung und Anwendung von Zertifikaten für die Verschlüsselung von Netzwerkverbindungen zu Servern mittels SSL.

5. Die Richtlinie *AdminPKI-KlasseC-Enterprise – Workstation Authentication* regelt die Verwaltung und Anwendung von Zertifikaten für die Authentifizierung interner Client-Computersyssteme (Workstation, Notebook, mobile Geräte) am Netzwerk der Bundesverwaltung.

6. Die Richtlinie *AdminPKI-KlasseC-Enterprise – ConfigMgr Site Server Signing* regelt die Verwaltung und Anwendung von Zertifikaten für die Signierung von Client Policies durch Microsoft SCCM Server.

7. Die Richtlinie *AdminPKI-KlasseC-Enterprise – ConfigMgr OS Deployment* regelt die Verwaltung und Anwendung von Zertifikaten für die Authentifizierung von neuen Client- und Server-Computersysstemen, welche sich zwecks der Installation eines neuen Betriebssystems mittels PXE gestartet werden, gegenüber den Microsoft SCCM Servern.

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

Die Kunden der AdminPKI KlasseC-Enterprise sind interne und externe Mitarbeiter der Bundesverwaltung, die über einen Windows Active Directory Domain Account verfügen, sowie interne Computersysteme, welche in das Active Directory der Bundesverwaltung integriert sind.

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

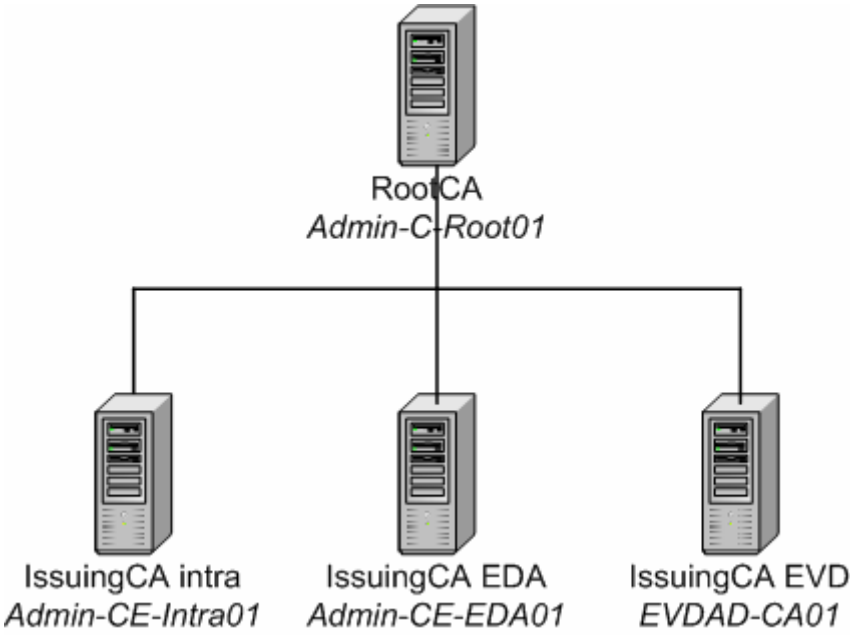
Die Zertifikatsinhaber sind in keiner Weise autorisiert, im Namen der schweizerischen Bundesverwaltung kommerzielle Transaktionen oder rechtsgültige Unterschriften gem. dem

Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) vorzunehmen.

3.2 Teilnehmer der PKI

3.2.1 Zertifizierungshierarchie

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



3.2.2 Root Certification Authority (RootCA)

Die Aufgabe der RootCA **Admin-C-Root01** auf der ersten Stufe ist die Validierung der Zertifikate der Zertifizierungsstellen der zweiten Stufe. Die RootCA stellt keine Teilnehmer-zertifikate 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-CE-Intra01** für den Forest Intra, **Admin-CE-EDA01** für den Forest EDA und **EVDAD-CA01** für den Forest EVD auf der zweiten Stufe generieren, validieren, publizieren, archivieren 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.

Dienste für KeyRecovery oder Revokation werden via MAC angeboten.

3.2.5 Verzeichnisdienst

Die Personen-Zertifikate werden im Active Directory der Bundesverwaltung publiziert. Die Personendaten und somit auch die Zertifikate der verschiedenen Forests werden synchronisiert. Die Listen der revozierten und suspendierten Zertifikate (CRL) werden im Active Directory und auf einem HTTP-Server unter http://www.pki.admin.ch/ publiziert.

3.2.6 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 KlasseC-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.

3.2.7 Zertifikatsinhaber

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

3.2.8 Zertifikatsanwender

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

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 3.2.6) 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 KlasseC-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 KlasseC-Enterprise Serviceverantwortlicher:

AdminPKI KlasseC-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 KlasseC-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.

Personen-Zertifikate werden im Active Directory publiziert. Die Personendaten und somit auch die Zertifikate der verschiedenen Forests werden synchronisiert.

CA-Zertifkate und CRL werden im Active Directory und auf einem Web Server 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 publizert.

4.3 Publikationsintervall der CRL

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

5 Identifikation und Authentifikation

5.1 Namensgebung

Im Zertifikat steht im Subject Name der *common name* und im Alternative Subject Name die *EMail-Adresse* resp. der *DNS-Name* aus dem Active Directory des Zertifikatsinhabers.

5.2 Überprüfung der Identität für Personenzertifikate

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

5.3 Überprüfung der Identität für Maschinenzertifikate

Die AdminPKI KlasseC-Enterprise nimmt selber keine eigene Prüfung der Identität vor. Die AdminPKI KlasseC-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 5.4.

5.4 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 vor. Es gelten hier die auf der Webseite http://www.pki.admin.ch unter dem Abschnitt ‚Maschinenzertifikate' publizierten Vorgaben.

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 gilt der Abschnitt 5.6.

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 Zertifikatstemplates, sowie von Gruppenmitgliedschaften und Group Policy Object (GPO) wird detailliert festgelegt, welche User und 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 5.6.

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 5.6).

6.4 Sperrung (Revoke)

Die Sperrung eines Zertifikates wird zurzeit zentral im Auftrage des zuständigen Adminstrators des LEs durch das BIT erbracht und direkt auf der Certification Authority (CA) vorgenommen. Das BIT garantiert eine Sperrung, wenn ein Verdacht auf Komprimitierung 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 C-Enterprise/Formulare' zu finden.

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 5.6).

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 Adminstrator des LEs durchgeführt.

6.6 Antrag und Ausstellung von Webserver und ConfigMgr Zertifikaten

Der Administrator des Serversystems erstellt via Webenrollment Seite einen Request an die AdminPKI KlasseC-Enterprise. Der CA Betrieb überprüft die Identität des Antragstellers (siehe Anschnitt 5.4), gibt den pending Request frei und stellt damit das Zertifikat aus. Die Installation des Zertifikats auf dem Serversystem erfolgt anschliessend via die Webenrollment Seite durch den Administrator.

Im Feld ‚Name' auf der Webenrollment Seite 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 der definierten Namensgebung (siehe dazu Abschnitt 5.1) im Zertifikat wird die Vertrauenswürdigkeit garantiert.

6.7 Key Recovery

Die privaten Keys der S/MIME-Userzertifikate werden mittels ‚Credential Roaming' im Active Directory gespeichert sowie auf der CA archiviert. Es wird ein eingeschränkter Dienst für KeyRecovery ausschliesslich für S/MIME-Encryption-Zertifikate angeboten. Der entsprechende Prozess ist auf der Webseite http://www.pki.admin.ch unter dem Abschnitt ‚Zertifikatstypen/Klasse C-Enterprise/Prozesse' beschrieben. Die zugehörigen Formulare sind auf derselben Seite unter ‚Zertifikatstypen/Klasse C-Enterprise/Formulare' zu finden.

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 KlasseC-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.

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 detailiertere Beschreibung befindet sich im Organisationshandbuch der AdminPKI KlasseC-Enterprise.

7.2.2 Anwendungsverantwortlicher (AV)

Der AV ist generell verantwortlich für Implementation, Koordination und Verwaltung der AdminPKI KlasseC-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) getroffen Vereinbarungen betreffend der AdminPKI KlasseC-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 KlasseC-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 KlasseC-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 KlasseC-Enterprise auf Unregelmässigkeiten sowie für die Durchführung von Securityaudits.

7.3 Personelle Sicherheit

7.3.1 Sicherheitsprüfung des Personals

Das Personal der AdminPKI KlasseC-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 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 Personen-Zertifikate werden im Active Directory der Bundesverwaltung publiziert und stehen so allen Zertifikatsanwendern zur Verfügung.

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.

Zusätzlich werden die privaten Schlüssel für S/MIME Verschlüsselung in einem Key Archive gespeichert. Für das Key Recovery sind immer zwei Rollen nötig, der CA Administrator und der Key Recovery Agent.

8.4 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 anteigende 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