



Pass06 Zertifizierungsrichtlinien und -bestimmungen

Certificate Practice Statement (CPS) der Country
Signing CA Switzerland

| | | | |
|---------------------|--------------------------|--------------------------|-------------------------------------|
| Autor | Jürg Porro | | |
| Ausgabedatum | 08.09.2006 | | |
| Version | 1.0 | | |
| Status | in Arbeit | in Prüfung | genehmigt zur Nutzung |
| | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Beteiligter Personenkreis

| | |
|---------------------------|--|
| PL, TPLs | - |
| Prüfung | Hr. Markus Waldner; Hr. Roman Vanek |
| Genehmigung | Hr. Markus Waldner; Hr. Roman Vanek |
| zur Information, Kenntnis | Publiziert auf www.pki.admin.ch (http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_52_1.pdf) |

Genehmigung

Ort, Datum: Bern, 04.09.06

Unterschrift: sig. Waldner

sig. Vanek

Änderungskontrolle, Prüfung, Genehmigung

| Datum | Version | Name / Rolle | Beschreibung |
|-----------------------|----------------|---------------------|--|
| 21.06.2006 | 0.82 | J. Porro | Erste Version zum internen Review |
| 22.06.- 26.06.2006 | 0.84 | J. Porro | Bestimmungen CSCA und S3 eingefügt, geringere Überarbeitungen, rechtliche Inhalte. |
| 13.07.2006 | 0.86 | J. Porro | Geringere Überarbeitungen |
| 25.07.2006 | 0.99 | J. Porro | Projektbeschreibung & Offene Punkte |
| 31.08.2006 | 0.99-1/2 | J. Porro | Einarbeitung Review-Kommentare von Herrn Waldner und Herrn Vanek |
| 08.09.2006 | 1.0 | J. Porro | Freigegebene Version |

Inhaltsverzeichnis

| | |
|---|-----------|
| Inhaltsverzeichnis | 3 |
| 1 Allgemeines | 5 |
| 1.1 Zweck des Dokumentes | 5 |
| 1.2 Hintergrundinformationen | 5 |
| 1.2.1 Anwendungsbereich | 5 |
| 1.2.2 Pilotprojekt „Biometrischer Pass“ | 5 |
| 1.2.3 Ausblick | 5 |
| 1.2.4 Einführung biometrischer Daten in der EU | 6 |
| 1.2.5 Nationale Regelungen | 6 |
| 1.3 Verantwortliche Stellen für dieses Dokument | 7 |
| 1.3.1 Kontakt & Freigabe für dieses Dokument | 7 |
| 1.3.2 Genehmigungsverfahren für dieses Dokument | 7 |
| 1.4 Eskalationsstellen | 7 |
| 1.5 Abkürzungen | 8 |
| 2 Ausführungsbestimmungen | 10 |
| 2.1 Bestimmungen für die CSCA | 10 |
| 2.1.1 Erzeugung des CA-Schlüssels & Zertifikates | 10 |
| 2.1.2 Aufteilung oder Hinterlegung des CA-Schlüssels | 10 |
| 2.1.3 Backup des CA-Schlüssels | 10 |
| 2.1.4 Restore des CA-Schlüssels | 10 |
| 2.1.5 Verwendung des CA-Schlüssels | 11 |
| 2.1.6 Archivierung des CA-Schlüssels | 11 |
| 2.1.7 Löschung des CA-Schlüssels | 11 |
| 2.1.8 Suspendierung oder Revokation des CSCA Zertifikates | 11 |
| 2.1.9 Kompromittierung des CA-Schlüssels | 11 |
| 2.1.10 Erzeugung privater Document Signer Schlüssel & Zertifikate | 11 |
| 2.1.11 Suspendierung oder Revokation eines Document Signer Zertifikates | 11 |
| 2.2 Bestimmungen für einen Secure Signatur Server (S3) | 12 |
| 2.2.1 Verwendung der DS-Schlüssel | 12 |
| 2.2.2 Kompromittierung eines DS-Schlüssels | 12 |
| 2.2.3 Backup & Restore der DS-Schlüssel | 12 |
| 2.2.4 Archivierung der DS-Schlüssel | 12 |
| 2.2.5 Löschung der DS-Schlüssel | 12 |
| 3 CSCA Zertifikate | 13 |
| 3.1 Zertifikathierarchie | 13 |
| 3.2 Zertifikatstypen | 13 |
| 3.2.1 Allgemeine Informationen | 13 |
| 3.2.2 CA-Zertifikat | 13 |
| 3.2.3 Document Signer Zertifikate | 15 |
| 4 CA Infrastruktur | 17 |
| 4.1 Physische Sicherheit | 17 |
| 4.1.1 Lokalitäten | 17 |
| 4.2 Personelle Sicherheit | 18 |
| 4.2.1 Sicherheitsprüfung des Personals | 18 |

| | | |
|-------------|---|-----------|
| 4.2.2 | Identifikation und Authentifizierung jeder Person | 18 |
| 4.2.3 | Notwendige Anzahl Personen zur Erfüllung der Aufgaben | 18 |
| 4.3 | Sicherheitsbestimmungen für die eingesetzten Systeme | 18 |
| 4.3.1 | Spezielle Sicherheitsanforderungen | 18 |
| 4.3.2 | Softwareentwicklung | 18 |
| 4.3.3 | Datenschutz und Datensicherheit | 19 |
| 4.3.4 | Netzwerksicherheit | 19 |
| 4.3.5 | Fehlerfall / Wartung | 19 |
| 4.4 | Verzeichnisdienste | 19 |
| 4.4.1 | Admin Directory | 19 |
| 5 | Weitere geschäftsbezogene und rechtliche Aspekte | 20 |
| 5.1 | Einstellung der Tätigkeit | 20 |
| 5.2 | Zertifizierungen und Auditing | 20 |
| 5.3 | Gebühren | 20 |
| 5.4 | Versicherungsschutz | 20 |
| 5.5 | Vertraulichkeit von Geschäftsinformationen | 20 |
| 5.6 | Editionspflicht | 20 |
| 5.7 | Nutzungsrecht | 21 |
| 5.8 | Vertraulichkeit von Personendaten | 21 |
| 5.9 | Garantierausschluss | 21 |
| 5.10 | Haftungsbeschränkung & Schadenersatz | 21 |
| 5.11 | Gerichtsstand | 21 |
| 5.12 | Gremien für die Vermittlung zwischen den Parteien | 21 |
| 5.13 | Inkrafttreten und Ausserkraftsetzen | 21 |
| 5.14 | Geltungsbereich | 21 |
| 5.15 | Sprache | 21 |

1 Allgemeines

1.1 Zweck des Dokumentes

Das vorliegende Dokument enthält die Zertifizierungsrichtlinien der Swiss Country Signing CA (CSCA) und beschreibt die Ausführungsbestimmungen (Verfahren) zu diesen Zertifizierungsrichtlinien.

Zertifizierungsrichtlinien enthalten ein Regelwerk, das den Einsatzbereich von Zertifikaten für eine bestimmte Benutzergruppe und/oder Anwendungsklasse mit gemeinsamen Sicherheitsanforderungen definiert.

Die Ausführungsbestimmungen der Zertifizierungsrichtlinien geben Auskunft, wie dieses Sicherheitsniveau sichergestellt wird.

1.2 Hintergrundinformationen

1.2.1 Anwendungsbereich

Diese Zertifizierungsrichtlinien gelten ausschliesslich für Zertifikate, welche von der CSCA für die Signatur von Daten im Pass06 ausgestellt werden.

Die Zertifikate können nicht für elektronische Signaturen gemäss Signaturgesetz verwendet werden.

1.2.2 Pilotprojekt „Biometrischer Pass“

Anlässlich seiner Sitzungen vom 15. September 2004 und 13. April 2005 beauftragte der Bundesrat das Eidgenössische Justiz- und Polizeidepartement (EJPD) mit der Einführung von biometrischen Pässen im Rahmen eines zeitlich und mengenmässig befristeten Pilotprojektes.

Das EJPD hat in der Folge Mitte 2005 das Bundesamt für Informatik und Telekommunikation BIT als Lieferant im Bereich PKI angefragt und die daraufhin eingereichte Offerte des BIT gutgeheissen.

Im Rahmen dieser Offerte ist die entsprechende PKI Infrastruktur für die Datensignatur der biometrischen Pässe (CSCA sowie Signaturserver) durch das BIT erfolgreich aufgebaut worden.

1.2.3 Ausblick

Mit der Annahme der Abkommen über die Assoziierung der Schweiz an Schengen am 5. Juni 2005 durch das Schweizer Volk ergibt sich unter anderem auch im Hinblick auf die definitive Einführung des biometrischen Passes in der Schweiz eine veränderte Situation.

Der Rat der EU hat am 13. Dezember 2004 die EU-Ausweisverordnung verabschiedet (siehe Ziffer 1.2.4 unten). Diese Verordnung stellt für die Schweiz eine Weiterentwicklung des Schengen-Besitzstandes dar.

Die Umsetzung dieser Weiterentwicklung hat so früh wie möglich, spätestens jedoch innert zwei Jahren nach Inkrafttreten der Abkommen zu erfolgen. Unter Berücksichtigung des Gesetzgebungsprozesses muss die definitive Einführung von biometrischen Pässen und Reisedokumenten somit aus heutiger Sicht voraussichtlich bis Herbst/Anfang Winter 2008 erfolgen, im Falle eines Referendums spätestens Anfang 2009.

1.2.4 Einführung biometrischer Daten in der EU

Am 13. Dezember 2004 hat die EU die Verordnung (EG) Nr. 2252/2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten (EU-Ausweisverordnung) verabschiedet und so die Grundlage für die Einführung biometrischer Daten in den Pässen und Reisedokumenten der Mitgliedstaaten der Europäischen Union (EU) bzw. den Schengenstaaten geschaffen. Zentrales Element dieser Verordnung ist, dass in einem ersten Schritt ein Gesichtsbild und in einem zweiten Schritt zwei Fingerabdrücke elektronisch im Pass gespeichert werden müssen. Es gelten die folgenden Einführungstermine:

- 28. August 2006: elektronisch gespeichertes Gesichtsbild;
- 28. Juni 2009: zwei elektronisch gespeicherte Fingerabdrücke.

Die Pflicht zur Aufnahme von biometrischen Daten gilt nur für Pässe und Reisedokumente mit einer Gültigkeitsdauer von mehr als 12 Monaten. Im Gegensatz zur ICAO und den USA hat die EU verschiedene verbindliche Bestimmungen zum Schutz der im Chip gespeicherten Daten vor nicht autorisiertem Auslesen festgelegt. Insbesondere zu erwähnen ist der Schutz der im Chip gespeicherten Daten vor dem unberechtigten Auslesen aus der Ferne durch das so genannte Basic Access Control Verfahren (BAC) und die Zugangs- bzw. Lesebeschränkung auf die in Zukunft im Chip gespeicherten Fingerabdrücke durch das so genannte Extended Access Control Verfahren (EAC).

Für das Lesen der Fingerabdrücke müssen daher besondere Zugriffsrechte gewährt werden. So kann ein Land bestimmen, welches andere Land die im Chip gespeicherten Fingerabdrücke lesen darf. Hierzu werden digitale Zertifikate erstellt und an die berechtigten Länder weitergegeben. Mittels dieser Zertifikate werden dann wiederum die einzelnen autorisierten Lesegeräte zertifiziert. Fingerabdrücke können nur von einem entsprechend zertifiziertem Lesegerät gelesen werden. Für diese Funktionalität ist der Aufbau einer weiteren PKI notwendig (Stichwort EAC).

1.2.5 Nationale Regelungen

In der Schweiz hat die Einführung des biometrischen Passes Auswirkungen auf die Gesetzgebung. Für das Pilotprojekt muss die Ausweisverordnung VAwG (SR 143.11) angepasst werden.

Für die definitive Einführung ist eine Revision des Ausweisgesetzes AwG (SR 143.1), des ANAG (SR 142.2) bzw. AuG (BBl 2005 7365) und der RDV (SR 143.5) notwendig. Im Zusammenhang mit der Übernahme der EU Gesetzgebung (Schengen) sind zudem entsprechende Staatsverträge zu schliessen.

1.3 Verantwortliche Stellen für dieses Dokument

1.3.1 Kontakt & Freigabe für dieses Dokument

Bundesamt für Informatik und Telekommunikation BIT
Abteilung eGovernment, Monbijoustrasse 74, CH-3003 Bern (Auftragnehmer)

| | |
|-------------------------------|--------------------------|
| Andreas Zürcher | Jürg Porro |
| Security Officer PKI | PL PKI Pass06 |
| andreas.zuercher@bit.admin.ch | juerg.porro@bit.admin.ch |
| +41 (0) 31 323 87 63 | +41 (0) 31 325 87 60 |

1.3.2 Genehmigungsverfahren für dieses Dokument

Bundesamt für Polizei fedpol
Sektion Ausweisschriften, Nussbaumstrasse 29, CH-3003 Bern (Auftraggeber)

| | |
|--------------------------------|-------------------------------|
| Markus Waldner | Roman Vanek |
| GPL Biometrischer Pass | Chef Sektion Ausweisschriften |
| markus.waldner@fedpol.admin.ch | roman.vanek@fedpol.admin.ch |
| +41 (0) 31 325 74 41 | +41 (0) 31 323 20 77 |

1.4 Eskalationsstellen

Auftraggeber (Bundesamt für Polizei fedpol)

Sektion Ausweisschriften; Roman Vanek; 031 323 20 77

Gesamtinformatik (Informatik Service Center EJPD ISC-EJPD)

Sektion Administrativanwendungen; Fritz Grossenbacher, 031 323 79 05

Passproduktion (Bundesamt für Bauten und Logistik BBL)

Ressort Ausweisschriften; Stephan Horisberger, 031 325 50 07

PKI-Betreiber (Bundesamt für Informatik und Telekommunikation BIT)

Abteilung eGovernment; Peter Balsiger, 031 325 40 43

1.5 Abkürzungen

In diesem Dokument werden folgende Abkürzungen verwendet:

| Abkürzung | Beschreibung |
|-----------|--|
| CA | Certification Authority (Zertifizierungsstelle) |
| CP | Certificate Policy (Zertifizierungsrichtlinie) |
| CPS | Certificate Practice Statement (Ausführungsbestimmungen zu der Zertifizierungsrichtlinie) |
| CRL | Certificate Revocation List (Sperrliste) |
| DN | Distinguished Name (Name des Zertifikatinhabers (Subject DN) bzw. des Zertifikatausgebers (Issuer DN)) |
| DSA | Digital Signature Algorithm. Ein Signatur-Algorithmus. |
| EAC | Extended Access Control. |
| EC | Elliptic Curve. Elliptische Kurve. Mathematisches Objekt, auf welchem verschiedene kryptographische Verfahren beruhen. |
| ECDSA | Variante des Signaturverfahren DSA, welche auf EC basiert. Definiert in [X9.62-1998]. |
| FIPS | Federal Information Processing Standards (publication). Durch das NIST publizierte Standards. |
| ICAO | International Civil Aviation Organization. |
| NIST | U.S. Department of Commerce / National Institute of Standards and Technology. Setzt Standards unter Anderem im Bereich von elliptischen Kurven. |
| PKD-CH | Public-Key Directory CH. Hier werden alle im Rahmen des Einsatzes biometrischer Pässe benötigten Informationen aller teilnehmenden Länder zugänglich sein. |
| PKI | Public Key Infrastruktur. |
| RDN | Relative Distinguished Name (O=Organisation, OU=Organisational Unit, L=Locality, ST=State / Province, CN=Common Name, C=Country) |
| RSA | Name des von Rivest, Shamir und Adleman entwickelten Public-Key Systems. |

Referenzen

| Abkürzung | Quelle |
|------------|---|
| FIPS 186-2 | Digital Signature Standard (DSS), NIST, 27. Januar 2000 |
| X9.62-1998 | The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute, 20. September 1998 |
| PKI Spez | Anforderungen an die PKI, fedpol (ID: DK000229) |
| ISDS | Informationssicherheits- und Datenschutzkonzept, BIT |
| | Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten (ABl. L 385 vom 29.12.2004, S. 1 – 6). |
| | Entscheidung K(2005) 409 vom 28. Februar 2005 (Gesichtsbild) und Entscheidung K(2006) 2909 vom 28. Juni 2006 (Ergänzung; Fingerabdrücke) über die technischen Spezifikationen zu Normen und Sicherheitsmerkmalen und biometrischen Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten. |

2 Ausführungsbestimmungen

Für die Tätigkeiten an der CSCA oder den S3 Servern ist ein Journal zu führen.

2.1 Bestimmungen für die CSCA

2.1.1 Erzeugung des CA-Schlüssels & Zertifikates

Die Erzeugung der CA Schlüsselpaare hat im Rahmen einer so genannten Root-Key Zeremonie in einer kontrollierten Umgebung unter Aufsicht eines Revisors zu erfolgen. Der private Schlüssel der CSCA (CA-Schlüssel) ist dabei in einem mindestens nach FIPS 140-2 Level 3 zertifizierten Hardware Security Modul (HSM) zu speichern.

Die Algorithmen der Schlüsselerzeugung sind auf Antrag des Auftraggebers offen zu legen. Als Quelle/Input für den Algorithmus sind Zufalls-Bits aus einem mindestens nach FIPS 140-2 Level 3 zertifizierten HSM zu verwenden.

Das CSCA Zertifikat ist direkt im Anschluss an die Zeremonie zu erzeugen, mit dem CA-Schlüssel zu signieren und im Verzeichnisdienst Admin-Directory des Bundes zu veröffentlichen.

Zusätzlich ist das CSCA Zertifikat durch das BIT dem Auftraggeber zu übergeben und durch diesen an die weiteren Empfänger zu verteilen.

2.1.2 Aufteilung oder Hinterlegung des CA-Schlüssels

Der CA-Schlüssel ist nicht auf mehrere Personen (m aus n) aufzuteilen und ist nicht zu hinterlegen.

2.1.3 Backup des CA-Schlüssels

Das private Schlüsselmaterial der CSCA ist nach der Root Key Zeremonie einmalig mit dem Standard Backup-Verfahren des HSM auf drei mindestens nach FIPS-140-2 Level 3 zertifizierte Backup-Token zu sichern.

Es ist organisatorisch sicherzustellen, dass für die Durchführung eines Backups mehr als eine Partei mit ihren entsprechenden Credentials anwesend ist. Keine Partei darf die für diesen Prozess notwendigen Credentials vollständig besitzen.

Diese Backup-Token sind an räumlich getrennten Orten sicher aufzubewahren.

2.1.4 Restore des CA-Schlüssels

Das private Schlüsselmaterial der CSCA ist - im Notfall und auf schriftliche Anweisung des Auftraggebers - mit dem Standard Restore-Verfahren des HSM von einem der oben erwähnten Backup-Token wieder herzustellen.

Es ist organisatorisch sicherzustellen, dass für die Durchführung eines Restore mehr als eine Partei mit ihren entsprechenden Credentials anwesend ist. Keine Partei darf die für diesen Prozess notwendigen Credentials vollständig besitzen.

2.1.5 Verwendung des CA-Schlüssels

Der Zugriff auf den CA-Schlüssel ist durch die Authentisierungs- und Autorisierungsverfahren des HSM sowie physischen Zutrittskontrollen zu schützen.

Die CSCA darf ihren privaten Signaturschlüssel nur zum Signieren ihres eigenen Zertifikates sowie von Document Signer Zertifikaten und von CRLs verwenden.

2.1.6 Archivierung des CA-Schlüssels

Der CA-Schlüssel ist - ausser mittels des oben erwähnten Backups - nicht zu archivieren.

2.1.7 Löschung des CA-Schlüssels

Der CA-Schlüssel ist nach Ablauf der Benutzungsperiode zu löschen bzw. das HSM und die Backup-Token sind zu initialisieren. Ein neuer Schlüssel ist im Rahmen einer erneuten Zeremonie zu erzeugen.

2.1.8 Suspendierung oder Revokation des CSCA Zertifikates

Eine Suspendierung oder Revokation des CSCA Zertifikates ist nicht geplant. Falls dieser Fall eintreten sollte, ist das Vorgehen durch den Auftragnehmer innerhalb eines Arbeitstages nach Kenntnis des Vorfalles mit dem Auftraggeber abzustimmen.

2.1.9 Kompromittierung des CA-Schlüssels

Wurde der CA-Schlüssel kompromittiert oder besteht ein begründeter Verdacht auf eine Kompromittierung, so wird umgehend der Auftraggeber informiert. Das weitere Vorgehen wird vom Auftraggeber bestimmt. Der Auftraggeber und der Auftragnehmer stellen in ihrem Verantwortungsbereich sicher, dass die Fristen und Vorgaben eingehalten werden.

2.1.10 Erzeugung privater Document Signer Schlüssel & Zertifikate

Die privaten Document Signer Schlüssel (DS-Schlüssel) sind nach ihrer Erzeugung direkt auf den Secure Signature Server (S3) zu übermitteln und auf der CSCA zu löschen.

Die entsprechenden Zertifikate sind direkt nach der Erzeugung im Verzeichnisdienst Admin-Directory des Bundes zu veröffentlichen, welches gleichzeitig als Archiv dient.

2.1.11 Suspendierung oder Revokation eines Document Signer Zertifikates

Sofort nach Eingang des Auftrages für die Revokation eines Zertifikates ist das Zertifikat durch die CSCA zu revozieren. Danach ist eine neue Liste der revozierten Zertifikate (CRL) zu generieren und im Admin-Directory des Bundes zu veröffentlichen.

Der Auftraggeber ist gleichzeitig ebenfalls in Kenntnis der neuen CRL zu setzen und wird die weiteren notwendigen Prozesse entsprechend einleiten. Der Auftraggeber und der Auftragnehmer stellen in ihrem jeweiligen Verantwortungsbereich sicher, dass die Fristen und Vorgaben eingehalten werden.

2.2 Bestimmungen für einen Secure Signatur Server (S3)

2.2.1 Verwendung der DS-Schlüssel

Ein Document Signer Schlüssel (DS-Schlüssel) ist bei Erhalt sofort in einem FIPS-140-2 Level 3 zertifizierten HSM zu speichern.

Der Zugriff auf einen DS-Schlüssel ist durch die Authentisierungs- und Autorisierungsverfahren des HSM sowie physischen Zutrittskontrollen zu schützen.

Der S3 hat vor der Benutzung eines DS-Schlüssels die Vertraulichkeit der Datenquelle (Herkunft des Request) zu überprüfen. Der S3 hat den zu signierenden Dateninhalt weder zu interpretieren noch zu überprüfen.

Ein DS-Schlüssel ist ausschliesslich für die Signatur der Daten biometrischer Pässe zu verwenden.

2.2.2 Kompromittierung eines DS-Schlüssels

Wurde ein DS-Schlüssel kompromittiert oder besteht ein begründeter Verdacht auf eine Kompromittierung, so wird umgehend der Auftraggeber informiert. Das weitere Vorgehen wird vom Auftraggeber bestimmt. Der Auftraggeber und der Auftragnehmer stellen in ihrem jeweiligen Verantwortungsbereich sicher, dass die Fristen und Vorgaben eingehalten werden.

2.2.3 Backup & Restore der DS-Schlüssel

Für DS-Schlüssel ist kein Backup und kein Restore durchzuführen.

2.2.4 Archivierung der DS-Schlüssel

DS-Schlüssel sind nicht zu archivieren.

2.2.5 Löschung der DS-Schlüssel

Die DS-Schlüssel sind nach der festgelegten Benutzungsdauer (Anzahl Signaturen bzw. Gültigkeitszeitraum) auf dem HSM des S3 zu löschen.

3 CSCA Zertifikate

3.1 Zertifikatshierarchie

Die Zertifikatshierarchie besteht aus einer self-signed Root-CA, welche direkt die Document Signing Zertifikate ausstellt. Diese Document Signing Zertifikate haben alle den gleichen Verwendungszweck und gehören derselben Klasse an (Ausstellungsprozess, Sicherheitsmerkmale).

3.2 Zertifikatstypen

3.2.1 Allgemeine Informationen

Alle von der CSCA ausgestellten Zertifikate beruhen auf dem X.509v3 Standard. Es werden ausschliesslich Zertifikate beruhend auf kryptographischen Verfahren für elliptische Kurven über Primkörpern ausgestellt.

Als Hash-Algorithmus wird SHA-1 verwendet.

3.2.2 CA-Zertifikat

Das CA-Zertifikat ist mit dem korrespondierenden privaten Schlüssel (CA-Schlüssel) signiert (self-signed). Die Überprüfung des CA-Zertifikates erfolgt durch Vergleich des Hash-Wertes (Fingerprint) des CA-Zertifikates mit dem durch das Bundesamt für Informatik und Telekommunikation BIT unter anderem in diesem Dokument publizierten Wert (siehe 3.2.2.6 unten).

3.2.2.1 Namensgebung

Das CA-Zertifikat hat folgenden Subject- und Issuer-DN:

| RDN | Beschreibung |
|-----|---------------------------|
| C | CH |
| O | Admin |
| OU | Services |
| OU | Certification Authorities |
| CN | csca-switzerland-1 |

3.2.2.2 Gültigkeitsperiode (Validity)

Die Gültigkeitsperiode des CA-Zertifikates setzt sich zusammen aus dem maximalen Vorlauf plus der maximalen Benutzungsdauer eines CSCA-Schlüssels plus der Gültigkeitsperiode eines Document Signer Zertifikates.

Die Gültigkeitsperiode eines CA-Zertifikates wird mit 4'082 Tagen festgelegt.

3.2.2.3 Benutzungsperiode des CSCA-Schlüssels (Private Key Usage Period)

Die empfohlene Benutzungsperiode des CA-Schlüssels beträgt 1'461 Tage. Beginn und Ende der Benutzungsperiode werden im CA-Zertifikat in der Zertifikats-erweiterung Private Key Usage Period festgehalten.

Die Benutzungsperiode des CA-Schlüssels wird mit 1'827 Tagen festgelegt.

3.2.2.4 Vorlauf des CA-Schlüssels

Als Vorlauf des CA-Schlüssels wird der Zeitraum zwischen dem Beginn der Gültigkeitsperiode und dem Beginn der Benutzungsperiode bezeichnet. Der Vorlauf beträgt mindestens 0 Tage und höchstens 31 Tage.

Die Vorlaufdauer des CA-Schlüssels wird mit 0 Tagen festgelegt.

3.2.2.5 Anzahl ausgestellte biometrische Ausweise

Es wird festgelegt, dass die mit dem gleichen CA-Schlüssel signierten Document Signer Schlüssel gemeinsam maximal 5'000'000 biometrische Ausweise signieren.

3.2.2.6 Fingerprint

| Hash-Alg. | Fingerprint |
|-----------|---|
| SHA-1 | A2B6 D663 B233 6191 4D30 B020 0B88 6816 761B DC11 |
| MD5 | 8ee6 9e68 ba31 435c d8c9 7af1 f428 f601 |

3.2.2.7 Signaturverfahren

Das CA-Zertifikat ist mit ECDSA signiert (self-signed). Der CA Schlüssel wird ausschliesslich für ECDSA Signaturen verwendet.

3.2.2.8 EC-Parameter

Der CA-Schlüssel beruht auf der Elliptischen Kurve P-384 gemäss [FIPS 186-2]. Die EC-Parameter werden im CA-Zertifikat explizit angegeben, inklusive Cofactor.

3.2.2.9 Erweiterungen (Extensions)

Das CA-Zertifikat enthält folgende X.509v3 kompatible Erweiterungen.

| Name | Critical | Wert |
|--------------------------|----------|--|
| Private Key Usage Period | No | Siehe Abschnitt 3.2.2.3. |
| Certificate Policies | No | Policy: 2.16.756.1.17.3.52.1 CPS: http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_52_1.pdf |
| Subject Key Identifier | No | 4EC8 9D98 C9B4 E090 F52B 5B85 9750 56BF E824 EB76 |
| Key Usage | Yes | Certificate Sign, CRL Sign |
| Basic Constraints | Yes | CA:TRUE, pathlen:0 |

3.2.3 Document Signer Zertifikate

3.2.3.1 Namensgebung

Die Document Signer Zertifikate haben folgenden Subject-DN:

| RDN | Beschreibung |
|-----|------------------|
| C | CH |
| O | Admin |
| OU | Services |
| OU | Signature-Server |
| OU | Pass06 |
| CN | ds-001 |

Der Issuer-DN der Document Signer Zertifikate ist der Subject-DN des CA-Zertifikates gemäss Abschnitt 3.2.2.1.

3.2.3.2 Gültigkeitsperiode (Validity)

Die Gültigkeitsperiode des Document Signer Zertifikates setzt sich zusammen aus dem maximalen Vorlauf plus der maximalen Gültigkeitsdauer eines biometrischen Ausweises plus dem maximalen Vorlauf plus der maximalen Benutzungsdauer eines Document Signer Schlüssels.

Die Gültigkeitsperiode eines Document Signer Zertifikates wird mit 2'224 Tagen festgelegt.

3.2.3.3 Benutzungsperiode eines DS-Schlüssels (Private Key Usage Period)

Die maximale Benutzungsperiode eines DS-Schlüssels beträgt 366 Tage. Beginn und Ende der Benutzungsperiode werden im Document Signer Zertifikat in der Zertifikatserweiterung Private Key Usage Period festgehalten.

Die Benutzungsdauer eines DS-Schlüssels wird mit 93 Tagen festgelegt.

3.2.3.4 Vorlauf des DS-Schlüssels

Als Vorlauf des DS-Schlüssels wird der Zeitraum zwischen dem Beginn der Gültigkeitsperiode und dem Beginn der Benutzungsperiode bezeichnet. Der Vorlauf beträgt mindestens 0 Tage und höchstens 31 Tage.

Die Vorlaufdauer eines DS-Schlüssels wird mit 0 Tagen festgelegt.

3.2.3.5 Anzahl Signaturen eines DS-Schlüssels

Ein DS-Signer Schlüssel signiert maximal 100'000 biometrische Ausweise. Die empfohlene Anzahl beträgt 25'000.

Die Anzahl Signaturen eines DS-Schlüssels wird mit 25'000 festgelegt.

3.2.3.6 Signaturverfahren

Die Document Signer Zertifikate sind durch den CA-Schlüssel mit ECDSA signiert. Die DS-Schlüssel werden ausschliesslich für ECDSA Signaturen verwendet.

3.2.3.7 EC-Parameter

Die DS-Schlüssel beruhen auf der Elliptischen Kurve P-256 gemäss [FIPS 186-2]. Die EC-Parameter werden in den Document Signer Zertifikaten explizit angegeben, inklusive Cofactor.

3.2.3.8 Erweiterungen (Extensions)

Die Document Signer Zertifikate enthalten folgende X.509v3 kompatible Erweiterungen.

| Name | Critical | Wert |
|--------------------------|----------|--|
| Private Key Usage Period | No | Siehe Abschnitt 3.2.2.3. |
| Certificate Policies | No | Policy: 2.16.756.1.17.3.52.1 CPS: http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_52_1.pdf |
| Authority Key Identifier | No | 4EC8 9D98 C9B4 E090 F52B 5B85 9750 56BF E824 EB76 |
| Key Usage | Yes | Digital Signature |

4 CA Infrastruktur

Die CSCA ist nicht öffentlich, untersteht der Hoheit des Bundesamtes für Polizei und wird vom Bundesamt für Informatik und Telekommunikation BIT betrieben.

4.1 Physische Sicherheit

4.1.1 Lokalitäten

Die CSCA wird im PKI-Raum des Bundesamtes für Informatik und Telekommunikation BIT betrieben. Es handelt sich um eine Sicherheitszone, welche ausschliesslich für Public Key Infrastrukturen (PKI) zur Verfügung steht.

Die Secure Signature Server (S3) stehen in einem speziellen Raum im Media Center Bund (MCB) beim Bundesamt für Bauten und Logistik BBL. Es handelt sich beim MCB ebenfalls um eine Sicherheitszone mit restriktivem Zutritt.

4.1.1.1 Zugangskontrolle

Nur namentlich bekannte Personen mit einem speziellen Badge haben Zutritt zum Raum, in welchem sich das System der CSCA befindet. Übrige Personen (z.B. für Wartung) haben nur in Begleitung eines autorisierten Mitarbeiters Zutritt und dieser Zutritt wird im Journal aufgeführt.

Zum Raum mit den S3 haben einige wenige namentlich bekannte Personen Zutritt. Dazu existiert ein weiterer Schlüssel in einem Safe, auf welchen wenige Personen Zugriff haben. Übrige Personen haben nur in Begleitung eines autorisierten Mitarbeiters Zutritt. Der Raum mit dem S3 wird zusätzlich mit einer zertifizierten Videoanlage überwacht.

4.1.1.2 Stromversorgung und Klimatisierung

Die Räume (von CSCA und S3) sind mit einer Klimaanlage für die Regulierung von Temperatur und Feuchtigkeit ausgerüstet. Alle elektrischen Komponenten sind an eine unterbrechungsfreie Stromversorgung angeschlossen.

4.1.1.3 Wasserschaden

Die Räume (von CSCA und S3) sind mit Wassermeldern ausgerüstet, welche direkt mit dem Überwachungszentrum des Gebäudes verbunden sind. Bei einem Alarm werden die erwähnten Informatikgeräte automatisch heruntergefahren und die Stromzufuhr wird unterbrochen.

4.1.1.4 Vorbeugung und Schutz vor Feuer

Die Räume (von CSCA und S3) sind mit Rauchmeldern ausgerüstet, welche alle direkt mit dem Überwachungszentrum des Gebäudes verbunden sind. Bei einem Brandmeldealarm werden die erwähnten Informatikgeräte automatisch abgeschaltet und die Stromzufuhr wird unterbrochen.

4.1.1.5 Ablage der Datenträger

Datenträger, welche Informationen im Zusammenhang mit der CSCA enthalten, einschliesslich Sicherheitskopien, werden in einem feuersicheren Tresor im PKI-Raum aufbewahrt.

Schützenswerte Dateien der CSCA werden in mindestens zwei verschiedenen Gebäuden aufbewahrt.

4.2 Personelle Sicherheit

4.2.1 Sicherheitsprüfung des Personals

Das Personal für die CSCA besteht aus Mitarbeitenden des BIT. Sie verfügen über die notwendige Qualifikation und Erfahrung, um PKI Dienstleistungen zu erbringen und sind im Allgemeinen vollzeitlich für die PKI tätig.

Der Arbeitsvertrag jedes Mitarbeitenden enthält eine Vertraulichkeits-Klausel. Alle Mitarbeitenden der PKI BIT haben bei ihrer Einstellung eine Personensicherheitsprüfung gemäss Artikel 10 Absatz 1 Buchstabe a der Verordnung über die Personensicherheitsprüfungen (PSPV) bestanden.

4.2.2 Identifikation und Authentifizierung jeder Person

Der technische Zugang zu den einzelnen IT-Systemen wird durch Benutzerkennung und Passwort oder Smartcard und Passwort realisiert. Kryptografische Devices wie HSM und CA-Server sind besonderen Authentisierungsverfahren unterworfen.

4.2.3 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 des CA-Schlüssels,
- Backup und Recovery des CA-Schlüssels,
- Austausch der Hardware, welche den CA-Schlüssel oder DS-Schlüssel enthalten.

Die beiden Personen sind zu gleichen Teilen verantwortlich für den Schutz der Informationen und Credentials, welche bei sensiblen Transaktionen benötigt werden. Keine der beiden Personen ist allein in der Lage, solche Information zu verwenden oder darauf zuzugreifen.

Alle anderen Aufgaben, inkl. Generation der DS-Schlüssel, dürfen von einer autorisierten Person allein ausgeführt werden.

4.3 Sicherheitsbestimmungen für die eingesetzten Systeme

4.3.1 Spezielle Sicherheitsanforderungen

Die CSCA sowie die S3 werden auf einem programmierbaren Hardware Security Module (HSM) betrieben. Dieses HSM ist nach FIPS 140-2 Level 3 oder höher zertifiziert. Die Applikationen laufen auf speziell gehärteten Systemen (LINUX).

4.3.2 Softwareentwicklung

Die Softwareentwicklung für die CSCA und den S3 erfolgt durch qualifiziertes Personal. Geänderte Software wird erst nach einem definierten Test- und Abnahmeverfahren auf die produktiven Systeme übernommen.

4.3.3 Datenschutz und Datensicherheit

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

4.3.4 Netzwerksicherheit

Die CSCA sowie die S3 sind durch mehrere Firewalls vor unberechtigten Zugriffen geschützt. Der administrative Zugriff auf die CSCA und die S3 ist nur von der Admin-Workstation über gegenseitig authentifizierte SSH-Verbindungen möglich.

Der Zugriff des DPPS (Partnersystem der Passproduktion) auf den produktiven S3 ist nur über gegenseitig authentifizierte HTTPS-Verbindungen möglich.

4.3.5 Fehlerfall / Wartung

Die für die CSCA benutzte Hardware darf nur nach schriftlicher Einwilligung und unter den Auflagen des Security Officers PKI des BIT aus dem PKI-Raum entfernt werden. Insbesondere dürfen keine Teile eingesandt oder ausgetauscht werden. Der Auftraggeber ist umgehend zu informieren.

4.4 Verzeichnisdienste

4.4.1 Admin Directory

Die durch die PKI des Pass06 Schweiz (PCH06) erzeugten Zertifikate und die Liste der revozierten und suspendierten Zertifikate (CRL) werden im elektronischen Verzeichnisdienst Admin-Directory publiziert.

Das Admin-Directory ist ein bundesverwaltungsinterner Verzeichnisdienst gemäss der Norm X.500 der ITU-T. Der Dienst ist mittels HTTP Protokoll auf der Adresse www.verzeichnisse.admin.ch (für Personen) und mittels LDAP Protokoll unter admindir.admin.ch (port 389; für weitere Objekte wie CA- oder Server-Zertifikate) erreichbar. Der öffentliche Teil des Verzeichnisdienstes, das Admin-Directory Public, ist vom Internet aus erreichbar.

Bemerkung: Das für die operativen Prozesse der Passbenutzung relevante Verzeichnis ist das Public-Key Directory CH (PKD-CH). Die entsprechenden Informationen werden aus dem Admin Directory dorthin kopiert.

5 Weitere geschäftsbezogene und rechtliche Aspekte

5.1 Einstellung der Tätigkeit

Das Bundesamt für Informatik und Telekommunikation BIT informiert die betroffenen Stellen frühzeitig, mindestens aber 6 Monate im Voraus, falls eine Einstellung der Tätigkeiten der CA-Infrastruktur vorgesehen ist.

Die ausgestellten Zertifikate sowie die Log-Dateien der CA-Infrastruktur werden archiviert. Der Zeitraum der Aufbewahrung richtet sich nach den anwendbaren Archivierungsvorschriften des Auftraggebers.

5.2 Zertifizierungen und Auditing

Der Auftraggeber informiert den Betreiber so früh als möglich über allfällig durchzuführende Zertifizierungen oder Audits. Die anfallenden Kosten werden zwischen Auftraggeber und Auftragnehmer aufgeteilt. Der Auftraggeber trägt genau dann die Kosten zu 100%, wenn die Kosten bzw. der Nutzen nur der Applikation oder den Prozessen im Zusammenhang mit dem biometrischen Pass zugewiesen werden kann.

5.3 Gebühren

Die Gebühren für Dienstleistungen des BIT im Rahmen der CSCA sind im Angebotspaket des BIT für den Unterhalt und den Betrieb der Applikationen für die CSCA und den S3 enthalten. Details sind im entsprechenden Service Level Agreement (SLA) geregelt. Das SLA wird nach Bedarf angepasst.

5.4 Versicherungsschutz

Entfällt.

5.5 Vertraulichkeit von Geschäftsinformationen

Das BIT trägt als Betreiber der CSCA und des S3 die Verantwortung für Massnahmen zum Schutz vertraulicher Informationen. Daten dürfen nur im Rahmen der Dienstleistung bearbeitet und an Dritte nur weitergegeben werden, wenn zuvor eine Vertraulichkeitserklärung unterzeichnet wurde und die mit den Aufgaben betrauten Mitarbeiter auf Einhaltung der gesetzlichen Bestimmungen über den Datenschutz verpflichtet wurden.

Zu Auditions- oder Revisionszwecken können vertrauliche Dokumente in Gegenwart des Verantwortlichen für Operative Sicherheit des BIT eingesehen werden.

5.6 Editionsspflicht

Der Auftragnehmer stellt dem Auftraggeber auf Verlangen die Dokumente, Beschriebe und Regelungen in Zusammenhang mit der ‚Country Signing CA Switzerland‘ zur Überprüfung zur Verfügung.

5.7 Nutzungsrecht

Für eine erweiterte oder anderweitige Nutzung der im Rahmen des Pilotprojektes "Biometrischer Pass" oder allfälliger Folgeprojekte erstellten Systeme (CSCA bzw. S3) ist die schriftliche Zustimmung des Auftraggebers einzuholen.

Sollte der Auftragnehmer den Betrieb einstellen oder der Auftrag zur Führung der ‚Country Signing CA Switzerland‘ einer anderen Stelle übertragen werden, kann der Auftraggeber die erstellten Programme, Anwendungen und vom Auftraggeber finanzierten Komponenten dieser Stelle, einschliesslich der Dokumentation, zur Verfügung stellen. Den berechtigten Geheimhaltungsinteressen des Auftragnehmers ist Rechnung zu tragen.

5.8 Vertraulichkeit von Personendaten

Im Rahmen des Betriebs der CSCA und des S3 werden durch das BIT Personendaten verarbeitet. Diese Daten werden weder interpretiert noch gespeichert. Im Übrigen gelten die Regelungen des Datenschutzgesetzes.

5.9 Garantieausschluss

Entfällt.

5.10 Haftungsbeschränkung & Schadenersatz

Entfällt.

5.11 Gerichtsstand

Entfällt.

5.12 Gremien für die Vermittlung zwischen den Parteien

Die Vermittlung erfolgt auf Direktionsstufe der direkt beteiligten Ämter, welche unter Ziffer 1.4 Eskalationsstellen aufgeführt sind.

5.13 Inkrafttreten und Ausserkraftsetzen

Dieses Dokument tritt nach Freigabe am Tag der Produktionsaufnahme für die biometrischen Pässe in Kraft und ist gültig, bis es durch eine neue Version ersetzt wird. Die Ausgabe einer neuen Version ersetzt alle vorherigen Versionen.

Die Terminierung der CSCA ist nicht vorgesehen.

5.14 Geltungsbereich

Alle in diesem Dokument enthaltenen Regelungen gelten zwischen dem Betreiber der CSCA und dem S3, dem Passproduzenten und dem Auftraggeber.

5.15 Sprache

Dieses Dokument wurde in deutscher Sprache verfasst. Bei Abweichungen in Übersetzungen ist die deutsche Version massgebend.