Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

Swiss Government PKI Registrierrichtlinien Klasse B

Registrierrichtlinien der Swiss Government PKI für die LRA

V6.0, 01.11.2019

Klassifizierung *	Nicht klassifiziert
Status **	Freigegeben
Projektname	
Projektabkürzung	
Projektnummer	
Projektleiter	
Auftraggeber	Swiss Government PKI
Autor	Daniel Stich
Initiale	
Bearbeitende	Daniel Stich, Jürgen Weber, Beatrice Metaj
Prüfende	Michael von Niederhäusern
Genehmigende	PKI Management Board
Verteiler	LRA-Officer, Auditoren
Doc_ID	0002-RV-Swiss Government PKI B Registrierrichtlinien LRA
Kurzbeschreibung	
Ablageort	Certified PKI

* Nicht klassifiziert, Intern, Vertraulich
** In Arbeit, In Prüfung, Abgeschlossen

Änderungskontrolle, Prüfung, Genehmigung

Version	Datum	Beschreibung, Bemerkung	Name oder Rolle
2.91	23.07.2010	Ersetzt Versionen 2.x, bei der Klasse A und B in einem Dokument abgehandelt werden	Andreas Zürcher
2.92		Straffung und Sicherung der Konsistenz mit CP/CPS, Checklisten mit Links zu den Richtlinien	Daniel Stich
2.93		Einarbeitung Ergebnisse Review mit A. Zürcher	Daniel Stich
2.94		Einarbeitung Feedback LZPPS	Daniel Stich
3.00	23.02.2012	Final	Daniel Stich
3.01	23.04.2012	Anpassung der PIN Regeln	Daniel Stich
3.02	30.01.2013	PDF in RIO Prozessen und Zertifikaterstellung, signierte elektronische Dokumentübermittlung bei RIO Prozess, Anpassungen an 2-Faktor-Login auf Bundesclients	Daniel Stich
3.03	22.04.2013	Einbezug von Funktionszertifikaten Anpassung AdminPKI-> Swiss Government PKI Anpassung Organisationseinheit nach ON BIT	Tomaso Vasella
3.04	11.09.2013	Daniel Stich	
3.05	15.01.2015	Daniel Stich	Konkretisierung Identifikation anhand von Ausweisen
4.00	24.03.2015	Daniel Stich	Anwendung neues Template, Einfügen in Dokumentverwaltungssystem
4.1	22.09.2016	Daniel Stich	Anpassung an neue Wizards, Prozesse und Prestaged Smartcards
4.2	24.05.2017	Daniel Stich	Integration der neuen Formulare und Checklisten
4.3	29.08.2017	Daniel Stich	Gesamtregelung der elektronischen Archivierung von Journal und Belegen.
5.0	08.11.2017	Daniel Stich	Bereinigte und freigegebene neue Version
5.1	15.05.2019	Daniel Stich	Anpassung PSP-Anforderung Identifizierung Antragsteller gemäss Ausnahmeregelung ‘Ausweis F’
5.2	03.09.2019	Beatrice Metaj	Div. Anpassungen aufgrund interne Auditfindings
5.2	20.09.2019	Beatrice Metaj	Anpassungen Anhang B Formulare und Benutzervereinbarungen, sowie Guidelines eingefügt
5.3	14.10.2019	Cornelia Enke/ Daniel Stich, Beatrice Metaj	Input In&Out / jährlicher Review
6.0	01.11.2019	PKI Management Board	Freigabe der neuen Version

Definitionen, Akronyme und Abkürzungen

Begriff / Abkürzung	Bedeutung
Admin-Directory	Das Admin-Directory ist ein Verzeichnis der Bundesverwaltung, in welchem unter anderem die Verschlüsselungs-Zertifikate und die Revokationslisten aufbewahrt werden, so dass die End-Benutzer darauf zugreifen können. Es handelt sich um ein Verzeichnis gemäss der Empfehlung X.500 [18]

Begriff / Abkürzung	Bedeutung
Aktivierungsdaten	sind Daten, welche ein Benutzer eingeben muss, um ein kryptographisches Modul (z.B. Smartcard) zu aktivieren. Die privaten Schlüssel gehören nicht zu Aktivierungsdaten.
AdminPKI	Frühere Bezeichnung der Swiss Government PKI. Wird oft noch synonym verwendet.
Antragssteller	Ein Antragssteller ist eine Person, welche einen Antrag für ein Zertifikat stellt. Nach erfolgter Ausstellung wird diese Person als Zertifikatsinhaber bezeichnet.
Ausweis F	Ausweis für vorläufig aufgenommene Ausländer. Vorläufig Aufgenommene sind Personen, die aus der Schweiz weggewiesen wurden, wobei sich aber der Vollzug der Wegweisung als unzulässig (Verstoss gegen Völkerrecht), unzumutbar (konkrete Gefährdung des Ausländers) oder unmöglich (vollzugstechnische Gründe) erwiesen hat.
BAB-Client	Bundesabeitsplatz (Arbeitsstation vom BIT)
Crosszertifikat	Ein Crosszertifikat baut eine Vertrauensbeziehung zwischen zwei Zertifizierungsstellen auf. Dies wird auch als Kreuzzertifizierung bezeichnet.
Certificate Policy / Certificate Practice Statement (CP/CPS)	Certificate Policy (Zertifizierungsrichtlinien)/ Certificate Practice Statement (Ausführungsbestimmungen der SG-PKI): Dokument, welches die Prozesse zur Ausstellung und Verwaltung der Zertifikate, die durch die beschriebene CA ausgestellt werden, beschreibt.
Certificate Service Provider (CSP)	Certificate Service Provider (Zertifizierungsdienstanbieter): Organisation, die eine PKI-Infrastruktur betreibt, z.B. die Swiss Government PKI.
Digitale Signatur	Ergebnis einer kryptographischen Funktion, welche Schlüssel so benützt, dass der Empfänger dieser Meldung feststellen kann 1. ob der zur Codierung verwendete Schlüssel dem Signierer (Unterzeichner) gehört 2. ob die Meldung seit dem Zeitpunkt der Codierung verändert wurde.
Erneuerung eines Zertifikates	Ein Zertifikat wird auf Anforderung eines Zertifikatsinhabers ausgestellt. Die zugrundeliegenden Schlüsselpaare werden neu erstellt. Dadurch wird dem Zertifikatsinhaber ein neues Zertifikat ausgestellt. Die Neuzertifizierung nach einer Revokation ist keine Erneuerung.
Funktionszertifikat der Klasse B	Voraussetzung für den Bezug eines Funktionszertifikates ist ein gültiger Admin- oder Testaccount. Der Antragsteller muss sich persönlich bei einer lokalen Registrierstelle melden und sich mit einem gültigen Reisedokument ausweisen. Beim Zertifikat für einen A-Account wird im Unterschied zum Standardzertifikat der Klasse B und dem Zertifikat für einen T-Account nur ein Authentisierungszertifikat ausgegeben (Trägermedium Smartcard oder USB-Key).
Hashwert, Fingerprint	Ein Hashwert ist ein numerischer Wert, der aus einem gegebenen Dateninput durch die Anwendung eines sog. Hash-Algorithmus gebildet wird. Da bei einem guten Algorithmus der Hashwert für verschiede Daten auch verschieden ausfällt, dient er unter anderem als "Fingerprint" zur Sicherung der unverfälschten Übertragung von Dokumenten. Im Falle einer Verfälschung würde der vom Empfänger errechnete Hashwert nicht mehr mit dem vom Absender mit gesandten übereinstimmen. Mit dem geheimen Schlüssel des Absenders verschlüsselter Hashwert wird als digitale Signatur bezeichnet.
Key Recovery Agent (KRA)	Benutzer mit einer speziellen Berechtigung, den Key Recovery Wizard auszuführen. Die KRA Berechtigung ist im Funktionsumfang der LRA-Officer enthalten. Auf speziellen Antrag kann die KRA-Berechtigung auch anderen Mitarbeitenden erteilt werden.
Authority Revocation List (ARL)	In der ARL sind die Ausstellerzertifikate enthalten, die gesperrt worden sind.
Certificate Revocation List (CRL)	Die CRL ist eine Liste, welche die Seriennummern der Zertifikate enthält, welche vor ihrem Ablauf revoziert wurden. Diese Liste wird durch die Zertifizierungsstelle aktuell gehalten und publiziert.
Local Registration Authority (LRA)	Unter LRA verstehen wir die Organisationseinheit, die von der Swiss Government PKI beauftragt ist, in ihrem Namen die Identifikation der Antragsteller und die Beantragung und Bearbeitung der Zertifikate durchzuführen. Die Aufgaben der LRA werden von LRA-Officern wahrgenommen. Neben der Hardware (Laptop) und Software (LRA-Client), die für das Bearbeiten der Zertifikate verwendet werden, gehören insbesondere auch die Räumlichkeiten dazu, in denen die Kunden identifiziert, Zertifikate ausgestellt, Kundendossiers aufbewahrt und die Computer der LRA (LRA-Client) betrieben werden.

Begriff / Abkürzung	Bedeutung
LRA-Officer (LRAO)	Unter LRA-Officer verstehen wir eine Person, die im Auftrag der Swiss Government PKI die Funktionen der LRA (beispielsweise Identifikation des Kunden, Erstellen oder Revozieren eines Zertifikates) wahrnimmt.
LRA-Client	Unter dem LRA-Client, früher auch LRA-Station genannt, wird die Hardware (Laptop oder Desktop PC, Scanner, Drucker) mit der dazugehörenden Software (Registrieranwendung, Firewall, Diskverschlüsselung, etc.) verstanden, welche zum Ausstellen und Revozieren der Zertifikate durch die LRAO benützt wird.
Non-prestaged Smartcards	Smartcards, die den Prestaged Smartcard Prozess der SG-PKI nicht durchlaufen. Diese Karten müssen vorgängig zur Ausstellung eines Zertifikats initialisiert werden. Zudem wird das Schlüsselmaterial für die Signatur und die Authentisierung bei diesen Karten direkt auf dem Chip generiert.
Object Identifier (OID)	Der OID ist eine eindeutige numerische Identifikation eines Objektes oder einer Klasse von Objekten; die Registrierung erfolgt gemäss internationalen Normen.
Personal Identification Number (PIN)	Mit der PIN authentisiert sich der Benutzer gegenüber seiner Smartcard und kann so die auf der Smartcard gespeicherten Daten benutzen
PIN Reset User (PRU)	Benutzer, der für eine andere Person den PIN-Reset Wizard auf seiner Arbeitsstation ausführen kann. Jeder Benutzer kann PRU sein, vorausgesetzt, seine Arbeitsstation besitzt zwei Smartcard Reader.
Prestaged Smartcards	Smartcards, die vor ihrem Einsatz den Prestaged Smartcards Prozess der SG-PKI durchlaufen. Beim Prestaging werden die Smartcards initialisiert, mit 3 Sätzen von je 3 Schlüsselpaaren versehen und mit einem PUK und einer PIN gesichert. Die Seriennummer der Smartcard wird mit den Identifiern der Schüssel, dem Verschlüsselungsschlüssel, sowie dem PUK und der PIN der Smartcard zentral abgespeichert.
Public Key Infrastruktur (PKI)	Eine PKI ist die Gesamtheit der Richtlinien, Prozesse, Server, Programme und Arbeitsstationen, welche zur Verwaltung der Schlüssel und der zugehörigen Zertifikate dienen.
Publikation (eines Zertifikates)	Das Zertifikat wird für Dritte zur Verfügung gestellt, um die Chiffrierung von Informationen zu ermöglichen.
Personal Unblock Key (PUK)	Der PUK wird gebraucht, um eine Karte, die wegen zu vieler Fehleingaben der PIN, oder PIN-Verlustblockiert ist zu deblockieren und mit einer neuen PIN zu versehen.
Registration Identification Officer (RIO)	Der RIO nimmt eine persönliche Identifikation des Antragsstellers anhand dessen gültigen Reisedokuments und dessen ausgefüllten Antrages (RIO Antrag Klasse B) vor. Er übergibt dem Antragsteller eine vorbereitete Smartcard, kopiert den Ausweis auf den Antrag und übermittelt das unterschriebene Dokument zusammen mit der Checkliste RIO sowie der unterschriebenen *Benutzervereinbarung und Nutzungsbedingungen Klasse B* dem Auftrag gebenden LRA-Officer per Post, Kurier oder als eingescannte und signierte Dateien mittels verschlüsselter Mail. Der RIO arbeitet immer im Auftrag eines bestimmten LRA-Officers.
Registrieranwendung (RA)	(Siehe LRA-Client)
Sicherheitspolitik (SP)	Eine Sicherheitspolitik besteht aus der Gesamtheit von Richtlinien und Vorschriften, welche aufgrund einer Risikoanalyse ausgearbeitet wurden. Ihr Zweck ist die Reduktion von möglichem Schaden durch vorbeugende Massnahmen und Korrektur von Unregelmässigkeiten durch entsprechende Massnahmen. Die Sicherheitspolitik dient zum Schutz der Integrität, Verfügbarkeit und zum Schutz der Daten des Zertifizierungs-Dienst-Anbieters. Die Spezifikation der Sicherheitspolitik definiert das Sicherheitsniveau, welches für ein Informations-System und für jede Komponente der Sicherheitsarchitektur angestrebt wird.
Standardzertifikat der Klasse B	Standardprodukt der SG-PKI - Siehe Produktdefinition. Die Zertifikate werden auf einer Non-Prestaged Smartcard oder einem USB Key ausgestellt.
Swiss Government Enhanced CA 01	Auf dieser CA werden alle Standardzertifikate Klasse B, sowie die prestaged Zertifikate Klasse B der Kantone und Ämter, die nicht im Kreis 1 und 2 der BV sind, ausgestellt.
Swiss Government Enhanced CA 02	Auf der Swiss Government Enhanced CA 02 werden ausschliesslich Zertifikate der Bundesverwaltung für Prestaged Smartcards ausgestellt.
Swiss Government PKI (SG-PKI)	Unter Swiss Government PKI (früher AdminPKI) wird die Infrastruktur des BIT für die als Standarddienst (ehemals Querschnittsleistung) angebotenen Zertifikatsklassen verstanden.

Begriff / Abkürzung	Bedeutung
Wurzelzertifizierungsstelle (Root-CA)	Sie ist die Oberste Zertifizierungsstelle der schweizerischen Bundesverwaltung für Zertifikate, die gemäss ZertES ausgestellt werden sowie für Zertifikate der Klasse B. Ihr „Common Name“ lautet Swiss Government Root CA I.
Zertifikat	Ein Zertifikat enthält den öffentlichen Schlüssel eines Zertifikatsinhabers, sowie weitere Angaben über diesen. Die vollständige Information wird mit dem privaten Schlüssel der Zertifizierungsstelle, welche das Zertifikat ausstellt, digital signiert. Das Format erfüllt die Empfehlung X.509 [19]19191919
Zertifikatsanwender	Ein Zertifikatsanwender ist eine Person, die ein Zertifikat eines Zertifikatsinhabers verwendet. Ein Zertifikatsanwender kann auch eine Organisationseinheit der Bundesverwaltung, ein Informatiksystem, ein Informatikanwendung oder ein Zertifikatsinhaber einer anderen PKI oder auch Kunden oder Lieferanten sein.
Zertifikatsinhaber	Zertifikatsinhaber der Swiss Government PKI Klasse B sind Mitarbeiter oder administrative Einheiten der schweizerischen Bundesverwaltung, der kantonalen oder kommunalen Verwaltung. Im Zertifikat - nach X.509 - wird sie als subject bezeichnet.
Zertifikatsklassen	Die Swiss Government PKI gibt Zertifikate der Klassen A, B C und D auf unterschiedlichen CAs aus [16]
Zertifizierungsstelle (CA)	Eine Zertifizierungsstelle ist eine vertrauenswürdige Stelle, welche Zertifikate, sowie Revokationslisten gemäss den Empfehlungen X.509 [19] ausstellt und verwaltet. Die Common Names der Klasse B ausstellenden CAs lauten *Swiss Government Enhanced CA 01* und *Swiss Government Enhanced CA 02.*

Referenzen

Erkennungszeichen	Titel, Quelle
[1]	**Swiss Government PKI - Root CA I CP/CPS** Certificate Policy and Certification Practice Statement of the Swiss Government Root CA I Version V2.8 vom 15.05.2019 Quelle: Swiss Government PKI (http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf)
[2]	**Benutzervereinbarung und Nutzungsbedingungen Klasse B** Für persönliche, fortgeschrittene Zertifikate der Swiss Government PKI der Bundesbehörden der Schweizerischen Eidgenossenschaft Version 1.1 vom 31.03.2017 Quelle: Swiss Government PKI
[3]	**Guidelines zu Klasse B Zertifikaten der Swiss Government PKI** Erläuterungen zum Bezug und Einsatz von Klasse B Zertifikate der Swiss Government PKI Version 1.0 vom 09.03.2017 Quelle: Swiss Government PKI
[4]	**Überprüfung Identität Antragsteller Klasse B** Verbindliche, detaillierte Vorgaben zur Überprüfung der Identität von Antragstellern für Zertifikate der Klasse B der Swiss Government PKI inklusive Ausnahmeregelungen Version 1.2 vom 14.11.2017 Quelle: Swiss Government PKI
[5]	**Ergänzendes Formular für Antragsteller mit Ausweis F** Zusätzlich zum Antragsformular auszufüllendes Dokument, wenn der Antragsteller kein gültiges Reisedokument, sondern lediglich einen Ausweis F vorlegen kann. Version 1.0 vom 20.09.2019 Quelle: Swiss Government PKI
[6]	**Quickguide WALK-IN SYNCHRON** Quickguide zur Ausstellung von Zertifikaten Klasse B (Standard und Prestaged Version 1.1 vom Januar 2017 Quelle: Swiss Government PKI

Erkennungszeichen	Titel, Quelle
[7]	**Quickguide PIN Reset** Quickguide zur Rücksetzung der Smartcard PIN für Zertifikate Klasse B (Standard und Prestaged) Version 1.1 vom Januar 2017 Quelle: Swiss Government PKI
[8]	**Quickguide Rekeying (Renewal)** Quickguide zur Erneuerung von Zertifikaten Klasse B (Standard und Prestaged) Version 1.1 vom Januar 2017 Quelle: Swiss Government PKI
[9]	**Quickguide Key Recovery** Quickguide zur Wiederherstellung von Verschlüsselungszertifikaten Klasse B (Standard und Prestaged) Version 1.1 vom Januar 2017 Quelle: Swiss Government PKI
[10]	**Quickguide Revoke** Quickguide zur Revokation von Klasse B prestaged Zertifikaten Version 1.0 vom 03.06.2016 Quelle: Swiss Government PKI
[11]	**Quickguide Register Smartcard** Quickguide zur Registrierung von Smartcards Version 1.0 vom 28.12.2016 Quelle: Swiss Government PKI
[12]	**Quickguide Sprachumschaltung Wizards** Kurzbeschreibung um die Sprache in den Wizards zu ändern Version 1.0 vom 26.01.2017 Quelle: Swiss Government PKI
[13]	**Richtlinien für den Registration Identification Officer (RIO)** Version V2.0 vom 01.02.2014 Quelle: Swiss Government PKI
[14]	**Quickguide WALK-IN ASYNCHRON** Quickguide zur Ausstellung von Zertifikaten Klasse B (Standard und Prestaged) mit RIO Version 1.1 vom Januar 2017 Quelle: Swiss Government PKI
[15]	**Quickguide Token Unseal** Quickguide zur Entsiegelung von prestaged Karten (Ausstellung via RIO, Anleitung für den Endkunden) Version 1.0 vom 06.06.2016 Quelle: Swiss Government PKI
[16]	Public Key Infrastruktur (PKI) in der Bundesverwaltung: Positions- und Strategiepapier, Version 1.1, vom 7. April 2004
[17]	Verordnung vom 4. März 2011 über die Personensicherheitsprüfungen (PSPV)
[18]	ITU-T X.500, Verzeichnis-Standard: Übersicht für Konzept, Modell und Dienste
[19]	ITU-T X.509, Standard: Regelwerk für Authentifizierung
[20]	RFC 5280, Internet X.509Public Key Infrastruktur , Zertifikats- und CRL-Profile; September 2005
[21]	RFC 3647, Public Key Infrastruktur X.509 Internet, Protokolle für das Zertifikats-Management, November 2003

Erkennungszeichen	Titel, Quelle
[22]	Technische Weisung no. 20 (DT20), Struktur des Admin-Directory, Bundesamt für Informatik und Telekommunikation, 1. Juni 1999
[23]	RFC 2526, Public Key Infrastructure Certificate Policy and Certificate Practices Framework, march 1999
[24]	W002 - Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung (WIsB)
[25]	ISB Standard A006 - Smartcard. Version 2.1 und Anhang (mit den bewilligten Komponenten)
[26]	Enoncé des pratiques de certification de l'autorité de certification Admin-CA3, 30.03.2005
[27]	Whitepaper betreffend Komplexitätsanforderungen an PIN-Codes von Smartcards https://intranet.isb.admin.ch/dam/isb_kp/de/dokumente/themen/sicherheit/technologiebetrachtungen/
[28]	172.010.442 Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen vom 22. Februar 2012 (Stand am 1. April 2012) Inkrafttreten: 1. April 2012 Quelle: https://www.admin.ch/opc/de/official-compilation/2012/947.pdf
[29]	235.1 Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG) vom 19. Juni 1992 (Stand am 1. März 2019) Inkrafttreten: 1. Juli 1993 Quelle: https://www.admin.ch/opc/de/classified-compilation/19920153/201903010000/235.1.pdf
[30]	510.411 Verordnung vom 4. Juli 2007 über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV) vom 4. Juli 2007 (Stand am 1. Januar 2018) Inkrafttreten: 1. August 2007 Quelle: https://www.admin.ch/opc/de/official-compilation/2007/3401.pdf
[31]	V001 - Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (BinfV) (Bundesinformatik Verordnung BinfV) vom 9. Dezember 2011 (Stand am 1. April 2018) Inkrafttreten: 1. Januar 2012 Quelle: https://www.admin.ch/opc/de/official-compilation/2011/6093.pdf

Inhaltsverzeichnis

Tabellenverzeichnis

1 Allgemeines

Inhalt des vorliegenden Dokumentes

Das vorliegende Dokument beinhaltet und beschreibt die Richtlinien und Vorschriften, die bei der Ausstellung und der Administration der Klasse B Zertifikate der Swiss Government PKI zur Anwendung gelangen.

Zielgruppe

Das Dokument richtet sich primär an die ausgebildeten Klasse B LRA-Officer der Ämter und Kantone. Es dient der externen Auditierungsstelle als Rahmen für die Auditierung der LRA in den Organisationen.

Verwendete Begriffe und Abkürzungen

Spezielle Begriffe und Abkürzungen, welche in diesem Dokument verwendet werden, sind in der Tabelle «Definitionen, Akronyme und Abkürzungen» auf der vorangehenden Seite 2 zusammengefasst und werden in kurzer Form erläutert.

Referenzierte Dokumente

Hinweise auf referenzierte Dokumente werden in eckigen Klammern mit einem entsprechenden Erkennungszeichen angegeben – zum Beispiel [1]. In der Tabelle «Referenzen» auf der vorangehenden Seite 5 sind die referenzierten Dokumente mit allfällig zusätzlichen Informationen zum Dokument aufgelistet.

Hinweis auf weibliche und männliche Schreibweise

Aus Gründen der einfacheren Lesbarkeit wird in diesem Dokument bei personenbezogenen Bezeichnungen in der Regel nur die männliche Schreibweise verwendet. Im Sinne einer Gleichbehandlung bezieht die männliche Form jeweils die weibliche Form mit ein.

1.1 Zweck des Dokumentes

Die «Certificate Policy and Certification Practice Statement of the Swiss Government Root CA I» (im Folgenden abgekürzt mit „CP/CPS“) [1] ist das massgebende Regelwerk für die Zertifikate der Klasse B. Das Ziel dieses Dokumentes ist es, die Anforderungen der CP/CPS betreffend der LRA zu konkretisieren.

1.2 Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiter, die im Bereich der LRA (Local Registration Authority) Klasse B tätig sind. Die Swiss Government PKI kann die Aufgaben der LRA Klasse B an andere Organisationseinheiten delegieren. Diese bestimmen ihrerseits die ausführenden Mitarbeiter.

1.3 Swiss Government PKI – Zertifikate der Klasse B

Zertifikate der Klasse B sind auf einem Security-Token (einer Smartcard oder einem USB Token mit dem entsprechenden Kryptochip) gespeichert und werden nur nach einer persönlichen Registrierung des Antragsstellers abgeben.

Der Inhaber eines Klasse B Zertifikates ist eine natürliche Person (keine Organisationen, Gruppen, Funktionen) und besitzt in der Regel drei oder ein Schlüsselpaar mit den entsprechenden Zertifikaten. Je nach Zertifikatstyp (Klasse B Standardzertifikat oder Klasse B Funktionszertifikat) eines für Signatur, eines für Authentifizierung und eines für die Schlüssel- und Datenverschlüsselung oder nur eines für die Authentifizierung. Für Zertifikate der Klasse B Prestaged werden die Smartcards von Beginn weg mit drei Sätzen zu jeweils drei Schlüsselpaaren ausgerüstet, wobei jeweils nur ein Satz gleichzeitig mit aktiven Zertifikaten versehen wird.

Die Initialisierung des Security Tokens für Organisationen mit eigener PUK-Verwaltung wird mit dem Tool des Karten-Lieferanten vorgenommen und ist nicht Bestandteil der Registrieranwendung. Smartcards, welche die PUK-Verwaltung der SG-PKI benutzen, werden entweder im Staging Prozess (Prestaged Smartcards), direkt bei der Ausstellung mit dem Walk-In-Wizard oder durch den Wizard „Register Smartcard“ (Non-Prestaged Smartcards) initialisiert.

Bei der Erneuerung wird bei den Prestaged Smartcards das nächstfolgenden Schlüsseltriplet von der CA signiert. Für Non-prestaged Smartcards generiert die Applikation einen neuen Satz Schlüsselpaare und lässt sie von der CA signieren. Anschliessend werden nur die alten Schlüssel und Zertifikate für Signatur und Authentifizierung von der Karte gelöscht. Das alte Schlüsselpaar für die Schlüssel- und Datenverschlüsselung wird für spätere Entschlüsselung auf der Karte belassen.

Ein Inhaber kann sowohl ein Klasse A, ein Klasse B Standard/Prestaged und eines oder mehrere Klasse B Funktionszertifikate besitzen. Klasse A, Klasse B und Funktionszertifikate dürfen **nicht** auf demselben Security-Token abgelegt sein, aber ein Security-Token darf mehrere Funktionszertifikate beinhalten. Der/die Vor- und Nachname(n) der Person sind im Zertifikat eindeutig erkennbar und ersichtlich.

1.4 Security-Token

Eine Liste der unterstützten Security-Token und detaillierte Vorgaben dazu der unterstützten Security-Token finden sich im vom Informatikratsteuerungsorgan des Bundes (ISB) genehmigten Standard „A006 - Smartcard“ [25] und dessen Anhang.

2 Aufgaben des LRA-Officers und des RIOs

2.1 Anforderungsprofil LRA-Officer

- Hohe persönliche Integrität
- Genaues Arbeiten nach den Vorschriften der Swiss Government PKI
- Zuverlässigkeit
- Freude am Umgang mit Kunden
- Bereitschaft, eine Tätigkeit unter Berücksichtigung der Nachvollziehbarkeit, auszuüben
- Bereitschaft, eine Vertrauenswürdigkeitsprüfung durch die eigene Behörde, z.B. einer Personensicherheitsprüfung gemäss Artikel 10 der Verordnung über die Personensicherheitsprüfungen (PSPV, SR 120.4) oder Ähnliches (vgl. Kap. 3.12), durchführen zu lassen.
- Ein LRAO darf nicht für die Erfassung oder Mutation von AdminDir-Einträgen berechtigt sein

2.2 Aufgaben des LRA-Officers Klasse B

Der LRA-Officer hat folgende Aufgaben:

- Antrag und benötigte Zusatzformulare und –unterlagen prüfen (s. 5.2.3.2 - Antragsformular überprüfen)
- Antragsteller identifizieren (s.5.2.3.5 - Identität des Antragstellers überprüfen)
- Angaben im Admin-Directory verifizieren
- Zertifikat ausstellen
- Zertifikat revozieren
- Antragsteller instruieren betreffend:
  - Aktivierungsdaten
  - Schutz der Aktivierungsdaten
  - seinen Rechten und Pflichten
  - «*Benutzervereinbarung und Nutzungsbedingungen Klasse B*» [2]
  - «*Guidelines zu Klasse B Zertifikaten der Swiss Government PKI*» [3]
- Ggf. Checklisten ausfüllen und ablegen
- Journal führen über alle Aktivitäten, welche die Zertifikate betreffen
- Dossiers der Zertifikatsinhaber führen und aufbewahren
- Smartcards verwalten, eventuell beschaffen und gegebenenfalls initialisieren
- Schulung und Qualifikation der RIOs sicherstellen
- Dem RIO Kopien der Formulare „RIO Antrag Klasse B“, „Benutzervereinbarung und Nutzungsbedingungen Klasse B“, „Guidelines zu Klasse B Zertifikaten der Swiss Government PKI“ und die „Checkliste RIO“ zur Verfügung stellen
- Liste der RIOs verwalten
- Zertifikatsanträge im Rahmen des RIO Prozesses freigeben
- Kenntnisse über Vorschriften, Prozesse und technische Mittel im Zusammenhang mit Zertifikaten der Klasse B proaktiv aktuell halten

2.3 Anforderungsprofil RIO

- Genaues Arbeiten nach den Vorschriften der Swiss Government PKI und des Auftrag gebenden LRA-Officers
- Grundverständnis des Begriffs „Nachvollziehbarkeit“ und Einsicht in die Notwendigkeit dessen Umsetzung in den Tätigkeiten als RIO

2.4 Aufgaben des RIOs

Der RIO behandelt Anträge für Klasse B Zertifikate gemäss den „Richtlinien für den Registration Identification Officer (RIO)“. Er hat folgende Aufgaben:

- Antragsteller identifizieren
- Antragsteller instruieren betreffend:
  - Aktivierungsdaten
  - Schutz der Aktivierungsdaten
  - seinen Rechten und Pflichten
- Antrag und benötigte Zusatzformulare und –unterlagen prüfen (s. 5.2.3.2 - Antragsformular überprüfen)
- Ausweisdokument und Antrag kopieren
- Checkliste ausfüllen
- Ausgefüllte Checkliste, allfällige Zusatzformulare, unterschriebene Kopie des Antrags enthaltend eine Kopie des gültigen Reisedokuments sowie die unterschriebene *Benutzervereinbarung und Nutzungsbedingungen Klasse B* [2] sicher dem Auftrag gebenden LRA-Officer per Post, Kurier oder elektronisch zustellen. Falls die elektronische Übermittlung gewählt wird: Einscannen der obigen Dokumente als PDF-Files, digitales Signieren der Files mit seinem persönlichen Klasse B Zertifikat und Versand an den LRA-Officer mittels verschlüsseltem Mail.

Ein LRA-Officer (LRAO) kann die Rolle eines RIO einnehmen, aber nicht umgekehrt.

3 Allgemeine betriebliche Aspekte

3.1 Bedienzeiten der LRA

Die Servicezeiten der LRA werden von den jeweils verantwortlichen Organisationseinheiten festgelegt.

3.2 Unterstützung der LRA

Zur Unterstützung der LRA ist das Betriebsteam der Swiss Government PKI gemäss den Angaben im Service- und Produktkatalog respektive dem geltenden Service Level Agreement erreichbar.

Bei Störungen erfolgt der Kontakt zum Betriebsteam über das Service Desk BIT
(+41 (0)58 465 88 88).

Bei dringenden sicherheitsrelevanten Mitteilungen und Fragen erfolgt der Kontakt zu einem Swiss Government PKI Security Officer ebenfalls über das Service Desk BIT (+41 (0)58 465 88 88).

Für weniger zeitkritische Mitteilungen und Fragen im Bereich Sicherheit steht die Mailbox pki-secoff@bit.admin.ch zur Verfügung. Bestellungen und allgemeine Fragen können als MAC (Move/Add/Change) dem BIT-MAC-Manger-Team direkt oder als Service Request dem Service Desk BIT (+41 (0)58 465 88 88) gemeldet werden. Die Mailbox pki-info@bit.admin.ch steht nach wie vor für unterstützende Beratungen zur Verfügung.

3.3 Zutrittskontrolle

An die Räumlichkeiten der LRA werden keine besonderen Anforderungen gestellt. Die Einrichtungen der LRA können sich in einem normalen Büro befinden. Nicht zulässig sind jedoch z. B. Sitzungszimmer, Sanitätszimmer oder ähnliche Räume, zu welchen unautorisierte Personen Zutritt haben. Die Räumlichkeiten sollten für die Antragsteller leicht erreichbar sein und genug Privatsphäre für die Eingabe der Persönlichen PINs/PUKs, sowie der Revokationspassphrase gewähren. Werden Grossraumbüros mit Mitarbeitern die keine LRA-Funktionen geteilt, muss sich im Raum ein geschützter/getrennter Teil für die LRA-Aufgaben befinden. Der Raum muss genug Möglichkeiten für das Wegsperren von LRA-Material wie Formulare und Kundendaten aufweisen und genug Privatsphäre bei der Ausstellung von Zertifikaten bieten können.

3.4 Zugangskontrolle

Der Zugang zum Bundesclient (Bundesarbeitsplatz - BAB) mit LRA-Client-Funktionen ist durch die 2-Faktor Authentisierung (Klasse B Zertifikat) geschützt. Der LRA-Client ist mit einer Diskverschlüsselung ausgerüstet. Die LRA-Applikationen sind nur mit LRAO-Berechtigungen auf einer separaten LRAO-Karte oder auf dem «normalen» Klasse B Zertifikat für die 2-Faktor Authentisierung zugelassen. Der Zugriff von anderen Personen, auch von anderen LRAOs, auf persönliche Smartcards mit LRAO-Berechtigungen ist untersagt. Entweder ist die Karte immer mitzuführen oder sie muss für sich alleine weggeschlossen werden. Arbeitet der LRA-Officer nicht am BAB, so muss die Smartcard immer aus dem Kartenleser entfernt und sicher aufbewahrt, bzw. mitgeführt werden. Die für die Smartcard erforderliche PIN darf nur aufgeschrieben werden, wenn sie verschlossen und getrennt von der Smartcard aufbewahrt wird. Falls der Verdacht besteht, dass eine andere Person die PIN kennt, ist diese umgehend zu ändern. Bei Verlust der Smartcard ist dies ohne Verzug dem Service Desk BIT und der Swiss Government PKI zu melden, welche die Smartcard unverzüglich sperren.

3.5 Policy betreffend den LRA-Clients

Für die BAB-Clients mit LRA-Funktion und deren Benutzer gelten strenge Sicherheitsvorschriften sowie auch die WIsB [24] und die BinfV 31. Es ist strikt untersagt:

- Software eigenständig zu installieren
- nicht vom BIT gelieferte Hardware anzuschliessen
- Konfigurationsänderungen an Hardware und Software vorzunehmen
- die LRA-Clients für andere Aufgaben als für die ausdrücklich vorgesehenen zu verwenden

3.6 Formulare und Kundendaten

Die von der Swiss Government PKI ausgegebenen und in dieser Richtlinie aufgeführten Formulare sind zwingend zu verwenden, ausser es wird ausdrücklich auf erlaubte Alternativen (auf Papier oder in elektronischer Form) hingewiesen. Andere Formulare oder elektronische Lösungen sind aufgrund der Nachvollziehbarkeit nicht zulässig.

Kundendossiers (Antragsformulare, Informationsblätter, Revokationsanträge, etc.) sind verschlossen aufzubewahren (Cleardesk Prinzip). Entweder ist der Raum abgeschlossen und nur für die LRAO zugänglich, oder die Dokumente sind in einem Schrank wegzuschliessen, welcher ebenfalls nur von LRAOs aufschliessbar ist.

Bei der Führung von elektronischen Kundendossiers müssen die Daten in einer Ablage gespeichert werden, auf die nur autorisierte Personen, also LRA-Officer und Auditoren, Zugriff haben. Zudem ist sicherzustellen, dass die unter 3.8 - Aufbewahrungsfristen definierten Bedingungen eingehalten werden. Sämtliche abgelegten Belege müssen als PDF/A Dokument vorhanden und mit dem Zertifikat der Klasse B des zuständigen LRA-Officers bzw. des beantragenden RIOs gültig signiert sein.

3.7 Journal

Im Journal werden alle Aktivitäten der LRA bezüglich der Ausstellung und Revokation von Zertifikaten oder andere wichtige Ereignisse festgehalten. Wichtige LRA-Aktivitäten sind z.B.:

- Ausstellung von Zertifikaten
- Revokation von Zertifikaten
- Ersatz/Reparatur/temporäre Verschiebung der LRA-Client
- Erhalt neuer Smartcard-Rohlinge
- Erhalt neuer LRA-Officer Smartcard
- PIN-Reset Anfragen (falls nicht das PIN-Reset System der SG-PKI verwendet wird)
- Ggf. interne Auftragsnummer (z.B. Ticketnummer Auftragserfassungssystem)

LRA-Officer Journale können entweder handgeschrieben (s. *Journal der Swiss Government PKI Klasse B*) oder elektronisch geführt werden. Bei der elektronischen Führung müssen die jeweiligen Tages-Journale jeweils am Abend ausgedruckt, vom ausführenden LRA-Officer unterschrieben und abgelegt werden. Alternativ können die elektronischen Journale täglich in eine PDF/A-Datei exportiert und mit dem Zertifikat der Klasse B des LRA-Officer signiert und mit dem Zeitstempel des Swiss Government PKI TSA (Time Stamping Authority der SG-PKI) versehen werden. Es ist grundsätzlich erlaubt, mehrere Journale pro LRA zu führen (z.B. pro LRAO, pro Amt, pro Monat, etc…) sofern die Chronologie und die Lückenlosigkeit gewährleistet bleibt. Die Journaldaten dürfen nur temporär lokal auf dem LRA-Client gespeichert werden. Sie müssen anschliessend auf ein Medium/Laufwerk transferiert werden, wo die Archivierung gemäss 3.8 - Aufbewahrungsfristen und den Bestimmungen des DSG sichergestellt und vor dem Zugriff durch Unberechtigte geschützt ist.

Die minimalen Informationen, die ein Journaleintrag enthalten muss, sind:

1. Fortlaufende Nummer des Eintrags
2. Datum
3. Ausführender LRA-Officer
4. Kunde (Antragsteller / Zertifikatsinhaber)
5. Tätigkeit (Präfix: SZ: Standardzertifikat, FZA: Adminzertifikat, FZT: Testzertifikat, E: Erstellen, R: Revozieren, K: Key Recovery, PR: PIN-Reset)

3.8 Aufbewahrungsfristen

Formulare, Kundendaten und Journale gemäss den Kapiteln ‚3.6 - Formulare und Kundendaten' und ‚3.7 - Journal' müssen in jedem Fall während mindestens 11 Jahre nach Ablauf des Zertifikates archiviert werden. Das Archiv muss während dieser Zeit für die Auditoren zugänglich sein. Der Zugriffsschutz auf diese Daten muss auch bei elektronisch geführten Kundendossiers gewährleistet sein (kein Zugriff auf die Daten für nicht LRAOs).

3.9 Aufbewahrung leerer Smartcards

Leere, Registered und Prestaged Smartcards und andere sensible Datenträger sind sicher aufzubewahren. Entweder ist der Raum abzuschliessen und nur für LRAOs zugänglich, oder die Smartcards sind in einem Schrank, dessen Schlüssel wiederum nur die LRAOs besitzen, weggeschlossen.

3.10 Verwendung und Schutz der Zertifikate mit LRA-Officer Berechtigungen

Die Zertifikate mit LRAO-Berechtigungen dürfen nur für die vorgesehenen Zwecke verwendet und nicht weitergegeben werden. Die LRA-Officer sind verpflichtet, ihre privaten Schlüssel/Zertifikate auf der Smartcard mit Aktivierungsdaten gemäss Kapitel 3.4 zu schützen.

3.11 Entsorgung

Nicht mehr benötigte Papierdokumente betreffend der LRA (Richtlinien, Checklisten, Notizen, etc.) oder der Kunden (Teilnehmeranträge, Listen, etc.) sind mit einem Shredder oder einer Sicherheitsbox zu entsorgen. Nicht mehr benötigte Smartcards sind mit einem Locher vor der Entsorgung zu zerstören oder zu shreddern.

Bei Störungen mit dem BAB-Client melden Sie sich beim Service Desk BIT.

3.12 Vertrauenswürdigkeitsprüfung

Vorgängig zur Anmeldung als LRA-Officer ergreift die Behörde die im gesetzlichen Rahmen erlaubten sowie ihr zumutbaren Massnahmen, um die Vertrauenswürdigkeit und Integrität des Kandidaten/der Kandidatin zu überprüfen. Die SG-PKI empfiehlt der Behörde die Durchführung folgender Massnahmen:

- Personensicherheitsprüfung gemäss Artikel 10 der Verordnung über die Personensicherheitsprüfungen (PSPV, SR 120.4) bei der Fachstelle PSP des VBS [17]

und/oder

- Vornahme eigener Massnahmen zur Überprüfung der Vertrauenswürdigkeit, wie beispielsweise:
    - Kontrolle der Identität des Kandidaten/ der Kandidatin (Pass oder Identitätskarte);
    - Überprüfung von geschäftlichen und/oder privaten Referenzen des Kandidaten/ der Kandidatin;
    - Verifizierung der Vollständigkeit und Schlüssigkeit des Lebenslaufs des Kandidaten/ der Kandidatin;
    - Kontrolle der referenzierten akademischen und beruflichen Qualifikationen;
    - Überprüfung von Betreibungs- und Strafregisterauszügen.

Die unterschriftsberechtigte Person der Behörde bestätigt anschliessend gegenüber der SG-PKI, die Vertrauenswürdigkeit des Kandidaten/ der Kandidatin gemäss obenstehender Empfehlung oder auf vergleichbare Art und Weise überprüft zu haben. Sie stuft den Kandidaten/ die Kandidatin als vertrauenswürdig und integer ein und bestätigt zudem, dass er/ sie über die notwendigen Kompetenzen zur Ausübung der sicherheitsempfindlichen Tätigkeit als LRA-Officer verfügt.

3.13 Vertraulichkeit, Datenschutz

Der LRA-Officer hat eine Vertraulichkeitserklärung zu unterschreiben. Diese ist im Anmeldeformular integriert.

Die Gesetze und Verordnungen des Datenschutzes (DSG) 29292929 und die Informationsschutzverordnung (ISchV) 30 sind einzuhalten.

Insbesondere ist darauf zu achten, dass Informationen betreffend Kundendaten oder wichtige Daten der LRA oder CA verschlüsselt übermittelt und unbefugten Dritten nicht zugänglich gemacht werden.

3.14 Ausbildung des Personals

Alle LRA-Officer müssen eine Schulung durchlaufen. Am Ende der Schulung entscheidet ein schriftlicher Test, ob der Teilnehmer genügend Kenntnisse und Fähigkeiten hat, um als LRA-Officer der Klasse B tätig zu sein.

Besteht der angehende LRA-Officer den Test nicht, erhält er die LRAO Berechtigungen vorerst nicht. Er kann bei einem erneuten Kursbesuch und Test zeigen, dass er über die erforderliche Eignung und die Kompetenzen verfügt. Stellt ein LRA-Officer Mängel in seinem Wissen, Fähigkeiten oder Unklarheiten fest und kann er diese selbst nicht beheben, ist er verpflichtet, dies bei der Swiss Government PKI zu melden. Die Swiss Government PKI wird zusammen mit dem LRA-Officer eine Lösung suchen.

Bei Zuwiderhandlungen gegen die Registrierrichtlinien kann die Swiss Government PKI die LRA-Officer Berechtigungen entziehen und somit das weitere Ausstellen von Endbenutzerzertifikaten unterbinden.

Die RIO müssen ebenfalls eine Schulung absolvieren, aber mit reduziertem Umfang. Die Schulung erfolgt grundsätzlich durch den sie beauftragenden LRA-Officer. Die Schulung kann auch durch die Swiss Government PKI erfolgen. In der Schulung müssen zumindest die referenzierten Dokumente «*Überprüfung Identität Antragsteller Klasse B*» [13] «*Richtlinien für den Registration Identification Officer (RIO)*» und die «*Benutzervereinbarung*»[2] sowie die «*Guidelines*»[3] behandelt werden.

3.15 Auffrischung der Ausbildung

Der LRA-Officer ist verpflichtet, sein Wissen, besonders in Bezug auf die Registrierrichtlinien, auf dem aktuellen Stand zu halten. Zu diesem Zweck stellt die Swiss Government PKI die aktuellen Dokumente und Informationen im Kundenbereich des Internetauftritts http://www.pki.admin.ch zur Verfügung. Die Swiss Government PKI verpflichtet sich, wichtige Änderungen per Email anzuzeigen. Der LRA-Officer seinerseits ist verpflichtet, bei Erhalt eines entsprechenden Emails der Swiss Government PKI die entsprechenden Informationen im Kundenbereich des Internetauftritts der Swiss Government PKI zu lesen.

Weiter ist jeder LRA-Officer verpflichtet, innerhalb einer Beobachtungsperiode von 18 Monaten insgesamt 20 Weiterbildungspunkte zu sammeln. Mit welchen Aktivitäten wie viele solcher Punkte gesammelt werden können, ist in der nachfolgenden Aufstellung beschrieben:

Aktivität	Punktzahl
Basisschulung	10
Test Basisschulung	10
LRAO-Summit (1/2 Tag)	10
LRAO-Workshop (1/2 Tag)	5 - 10 (je nach Inhalt)
LRAO-Workshop personalisiert (min. 4 Teilnehmer, vor Ort)	5 - 10 (je nach Inhalt)
Vorbereitetes Meeting / Telekonferenz (Themenbezogen)	5

Tabelle 1: Anzahl Punkte pro LRAO-Anlass

Die Swiss Government PKI bietet regelmässig Weiterbildungs- und Wiederholungskurse für die LRA-Officer an (LRAO-Workshops oder LRAO-Summit). Die LRA-Officer können bei zu geringer Punktzahl zur Teilnahme verpflichtet werden oder die LRAO Berechtigung kann entzogen werden. Der persönliche aktuelle Punktestand

kann bei der SG-PKI via pki-info@bit.admin.ch angefragt werden. Es werden von der SG-PKI keine Punktelisten publiziert.

3.16 Regeln für PINs

Die Zertifikatsinhaber verwenden PINs (Passwörter) zur Aktivierung ihrer Chip-Karten bzw. zur Aktivierung ihrer privaten Schlüssel. Die PIN unterscheidet sich grundsätzlich vom Passwort, welches z.B. für die Anmeldung bei Applikationen verwendet wird [27]. Jeder Zertifikatsinhaber wählt seine eigene PIN aus. Die Regelung in Bezug auf die Smartcard-PIN lautet:

- *Länge:* Die PIN muss mindestens 6 Stellen lang sein.
- *Anzahl Versuche:* Die Karte muss sich selbst nach spätestens 5 Fehlversuchen sperren.
- *Komplexität:* Die Zusammensetzung der PIN ist frei wählbar (auch ein rein numerischer Code ist gestattet). Triviale PIN-Codes (beispielsweise User-ID oder 123456) dürfen nicht verwendet werden.
- *Gültigkeit:* Die PIN muss geändert werden, sobald der Verdacht besteht, dass eine andere Person Kenntnis davon erhalten hat. Läuft der LifeCycle der Smartcard aus, muss für die neue Karte eine neue PIN gewählt werden.
- *Einmaligkeit:* Eine PIN sollte nur für genau eine Smartcard verwendet werden.

Von der Verwendung von Spezialzeichen ist wegen den sprachabhängigen Tastaturlayouts abzusehen.

3.17 Revokationspassphrase

Die Revokationspassphrase dient dazu, den Benutzer im telefonischen Verkehr mit dem LRA-Officer, z.B. bei der Beantragung der Revokation seiner Zertifikate, oder im PIN-Reset Prozess gegenüber dem zuständigen Service Desk zu identifizieren. Die Revokationspassphrase besteht aus einer Frage mit der dazugehörigen Antwort.

Die Informationen der Passphrase sollten so gewählt werden, dass sie einerseits von Drittpersonen nicht abgeleitet oder leicht erraten werden können. Andererseits müssen Sie dem Antragsteller so vertraut sein, dass er die Frage immer ohne Probleme und zweifelsfrei beantworten kann.

3.18 PIN-Reset und PUK-Handling

Prinzipiell muss für jede gesperrte Smartcard eine Entsperrungsprozedur mittels PUK vorhanden sein. Die Verwaltung des PUKs liegt jedoch, sofern nicht die prestaged-Karte der SG-PKI verwendet wird, in der Hoheit der Behörde. Die SG-PKI hat für Ihre prestaged-Karten ein elektronisches, zentralisiertes System mit PUK-Verwaltung entwickelt, bei welchem der PUK verschlüsselt auf einem der SG-PKI Server liegt und während des Entsperrungsprozesses im Hintergrund der Karte für die Entsperrung bereitgestellt wird. Der PUK wird zu keinem Zeitpunkt einer Person angezeigt.

Wird für die PUK-Verwaltung von non-prestaged Karten ein alternatives System benutzt (Scamiad, PrivacyPUK, oder andere), muss das Amt dafür Sorge tragen, dass:

- Die PUKs nur berechtigten Personen (Mitarbeiter Service Desks, LRAOs) zur Verfügung stehen, sei es in elektronischer oder schriftlicher Form (auf Papier, Couvert etc…)
- Die PUKs nur nach ausdrücklichem Einverständnis des Kartenbesitzers (aufgrund der gesperrten Karte z.B.) von den LRAOs oder dem zuständigem Service Desk Personal abgerufen werden können
- Der Abruf eines PUKs nachvollziehbar dokumentiert wird (z.B. mittels Auftragserfassungssystem/ Ticket/ Journaleintrag…)
- Nicht derselbe PUK für mehrere Karten benutzt wird
- Die PUKs nicht «ermittelbar» sind (z.B. Personalnummer, Kartennummer, etc.)

- Eine Beschreibung des verwendeten Systems mit Abläufen, Aktivitäten, Rollen, Ablageorten etc. vorhanden und durch das Amt genehmigt ist

Wird die prestaged Karte der SG-PKI eingesetzt, so gelten für das Support Personal oder der LRAO folgende Grundsätze:

- Es bedarf eines PIN-Reset Superusers, um einen PIN-Reset durchführen zu können. Der PIN-Reset Superuser kann mittels einer Webapplikation ein internes Ticket für diejenige Karte eröffnen, wenn er den Inhaber erfolgreich identifizieren kann. Die Identifikation darf auch telefonisch unter Verwendung der Revokationspassphrase erfolgen. Erst dann kann der Inhaber seine PIN bei einem sog. PRU zurücksetzen.
- Es bedarf eines PIN-Reset Users (PRU), um die Karte zu entsperren. Der PRU hat lediglich die Funktion, dem Inhaber seinen PC zu «leihen» und den PIN-Reset-Wizard für Ihn zu starten (da der Inhaber zu diesem Zeitpunkt keine 2-Faktor Authentisierung am PC durchführen kann aufgrund seiner gesperrten Karte). Der betroffene Benutzer muss dazu beim PRU vor Ort sein und seine Karte in einen zweiten Kartenleser am PC des PRU stecken.
- Die Funktionen PIN-Reset Superuser und PRU dürfen nicht von einer Person gleichzeitig übernommen werden. Die Berechtigungen schliessen sich gegenseitig aus um das Mehraugenprinzip der PIN-Reset Prozedur einzuhalten.

Der PIN-Reset Vorgang für prestaged Karten ist in der «Quickguide: PIN-Reset»[7] im Detail dokumentiert.

4 Konformitätsprüfung

Die SG-PKI ist verpflichtet, alle 18 Monate die Durchsetzung der CPS zu überprüfen. Dazu gehört besonders die Überprüfung der Einhaltung dieser Registrierrichtlinien durch die LRA-Officer. Die Konformitätsprüfung kann durch die SG-PKI selbst oder durch eine von der SG-PKI beauftragten externen Stelle durchgeführt werden. Die LRA-Officer sind verpflichtet bei diesen Kontrollen mitzuwirken und Einsicht in die Prozesse und Dokumente zu gewähren.

Bei nicht bestehen dieser Konformitätsprüfung kann dem betroffenen LRA-Officer seine Berechtigung entzogen werden. Bei besonders gravierenden Mängeln kann der PKI Verantwortliche oder der PKI Security Verantwortliche veranlassen, dass sämtliche von diesem fehlbaren LRA-Officer ausgestellten Benutzerzertifikate ebenfalls revoziert werden.

5 Prozesse der Swiss Government PKI Klasse B

5.1 Übersicht

Für die Klasse B gibt es Zertifikate in verschiedenen Ausprägungen. Die nachstehenden Tabellen geben eine Übersicht, welche Prozesse für welche Zertifikatstypen anwendbar sind:

Klasse B Prestaged
Initialisierung der Smartcard erfolgt während dem Prestaging Prozess bei der SG-PKI
Beim Prestaging werden drei Sätze zu drei Schlüsselpaaren (Signatur, Authentifizierung, Verschlüsselung) extern generiert und auf die Karte geschrieben
KeyRecovery auf einer Drittkarte (Bevollmächtigung) ist nicht möglich
Key Recovery des privaten Verschlüsselungsschlüssels ist möglich
RIO Prozess möglich
Rekeying (Renewal) max. zwei Mal möglich

Tabelle 2: Prozess Klasse B Prestaged

Klasse B Non-prestaged
Initialisierung der Smartcard erfolgt: • Beim Ausstellen der Zertifikate mit dem Walk-In Wizard oder • Bei der Registrierung der Smartcard mit dem Register Smartcard Wizard oder • ausserhalb des Prozesses mit Hilfe eines organisationsspezifischen PUK-Verwaltungssystems durch den LRA-Officer
Es werden bei der Ausstellung der Zertifikate drei Schlüsselpaare (Signatur, Authentifizierung, Verschlüsselung) auf der Karte generiert.
KeyRecovery auf einer Drittkarte (Bevollmächtigung) ist nicht möglich
Key Recovery des privaten Verschlüsselungsschlüssels ist möglich
RIO Prozess möglich
Rekeying (Renewal) max. zwei Mal pro Smartcard erlaubt

Tabelle 3: Prozess Klasse B Non-prestaged

Klasse B Funktionszertifikat für A-Accounts
Initialisierung der Smartcard erfolgt durch den LRA-Officer bei der Ausstellung des Zertifikats mit dem Walk-in-Wizard
Es wird bei der Ausstellung lediglich das Schlüsselpaar für die Authentisierung auf der Karte generiert.
KeyRecovery auf einer Drittkarte (Bevollmächtigung) ist nicht möglich
Key Recovery des privaten Authentisierungsschlüssels ist nicht möglich
Kein RIO Prozess vorgesehen
Renewal nicht erlaubt

Tabelle 4: Prozess A-Accounts

Klasse B Funktionszertifikat für T-Accounts
Initialisierung der Smartcard erfolgt durch den LRA-Officer bei der Ausstellung des Zertifikats mit dem Walk-In-Wizard
Es wird in der Regel bei der Ausstellung ein Schlüsselpaar (Authentifizierung) auf der Karte generiert. Nach Bedarf sind auch Signatur- und Verschlüsselungsschlüssel erlaubt.
KeyRecovery auf einer Drittkarte (Bevollmächtigung) ist nicht möglich
Key Recovery des privaten Verschlüsselungsschlüssels ist möglich
RIO Prozess möglich
Renewal nicht erlaubt

Tabelle 5: Prozess T-Accounts

Für die Prozesse mit und ohne RIO existieren verschiedene Wizards für den LRA-Officer und den Teilnehmer. Siehe dazu auch die Referenzen [6], [7], [8], [9], [10], [11], [12], [14] und [15].

5.2 Prozess Zertifikat ausstellen

Es ist zwischen zwei Ausprägungen des Ausstellungsprozesses zu unterscheiden:

- Ausstellungsprozess ohne RIO (Registration Identification Officer)
- Ausstellungsprozess mit RIO

Im Folgenden wird der Prozess ohne RIO „Ausstellen ohne RIO“ und der Prozess mit RIO „Ausstellen mit RIO“ genannt.

Die Unterschiede der Prozesse mit und ohne RIO sind in der folgenden Tabelle dargestellt:

Prozess ohne RIO	Prozess mit RIO
Persönliche Identifikation des Antragstellers direkt durch den LRA-Officer. Als Beweis scannt der LRA-Officer das gültige Reisedokument des Antragstellers. Für Antragsteller unter einer Ausnahmeregelung sind die Ausweise und Dokumente, die für die jeweilige Ausnahme definiert sind, zu kontrollieren und einzuscannen. Die pro Ausnahmefall verlangten Ausweise und Zusatzdokumente sind im Kapitel ‘5.2.3.5 - Identität des Antragstellers überprüfen’ beschrieben.	Persönliche Identifikation des Antragstellers durch den RIO. Als Beweis kopiert der RIO das gültige Reisedokument und das korrekt ausgefüllte Antragsformular. Für Antragsteller unter einer Ausnahmeregelung sind die Ausweise und Dokumente, die für die jeweilige Ausnahme definiert sind, zu kontrollieren und einzuscannen. Die pro Ausnahmefall verlangten Ausweise und Zusatzdokumente sind im Kapitel ‘5.2.3.5 - Identität des Antragstellers überprüfen’ beschrieben. Der RIO füllt die Checkliste aus und übermittelt diese Unterlagen und die unterschriebenen „Benutzervereinbarung und Nutzungsbedingungen Klasse B“ [2] dem LRA-Officer, in dessen Auftrag er handelt.
Überprüfen des Antragsstellers im Admin-Directory durch LRA-Officer	Überprüfen des Antragsstellers im Admin-Directory durch RIO
Teilnehmerinstruktion betreffend Aktivierungsdaten und deren Schutz durch LRA-Officer	Teilnehmerinstruktion betreffend Aktivierungsdaten und deren Schutz durch RIO
LRA-Officer erzeugt Antrag für den Teilnehmer. Im letzten Schritt des Walk-In-Wizards erfasst der Teilnehmer seine persönliche PIN und die Daten zur telefonischen Revokation (Revocation Passphrase).	Freigabe des Antrags durch den LRA-Officer
	Teilnehmer erfasst persönliche PIN und Daten zur telefonischen Revokation (Revocation Passphrase) bei der Entsiegelung der Smartcard mit dem Unseal-Wizard

Tabelle 6: Unterschied mit/ohne RIO

5.2.1 Wer kann ein Zertifikat beantragen?

Im Antrag für die Berechtigung als LRA-Officer wird von der Linie festgelegt, für welche Organisationseinheiten und Mitarbeiter Zertifikate ausgestellt werden dürfen. Die organisatorische Zugehörigkeit des Antragstellers muss mit der Berechtigung des LRA-Officers übereinstimmen. Konkret heisst dies, dass der Eintrag des Antragstellers im Admin Directory im gleichen Directory Pfad liegen muss, der für den LRA-Officer freigegeben wurde bzw. die berechtigten Directory-Pfade müssen im Account des LRA-Officers hinterlegt sein.

5.2.2 Wie kann ein Zertifikat beantragt werden

Der LRA-Officer, respektive PKI-Verantwortliche bestimmt, auf welchem Wege ein Zertifikat beantragt werden kann (schriftlich mit Formular, Remedy-MAC, etc.) Grundsätzlich muss jedoch der Bestellvorgang nachvollziehbar sein (Auditfähig, auch 11 Jahre nach dem Ablauf des Zertifikats!). Die SG-PKI stellt ein Formular zur Verfügung, welches alle für die Anmeldung benötigten Daten enthält (s. Formular im Anhang B).

Werden Zertifikate für Ausnahmefälle beantragt, z.B. wenn der Antragsteller lediglich einen ‘Ausweis F’ vorweisen kann, müssen ausnahmslos die für die jeweilige Ausnahme vorgesehenen Zusatzformulare der SG-PKI ausgefüllt und der Anmeldung beigelegt werden.

5.2.3 Ausstellen ohne RIO

Für die Bedienung der LRA gelten die Schulungsunterlagen LRAO sowie die Quickguides zu den einzelnen Wizards [6], [7], [8], [9], [10], [11], [12], [14] und [15]. Bei widersprüchlichen Anweisungen gilt die vorliegende Richtlinie.

Der LRA-Officer geht anhand der Checkliste «C*heckliste: Ausstellen von Klasse B Zertifikaten*" (RR Kapitel 5.2.3)‘“ vor.

5.2.3.1 Eintrag im Admin-Directory überprüfen

Der Antragsteller muss zwingend im AdminDir erfasst sein, damit ein Zertifikat ausgestellt werden kann.

Dabei müssen folgende Bedingungen erfüllt sein:

1. Ist eine vollständige, plausible E-Mail Adresse im Feld ‚Mail‘ spezifiziert?
   Bei Funktionszertifikaten für A-Accounts: E-Mail Adresse des Account-Inhabers
   Bei Funktionszertifikaten für T-Accounts: E-Mail Adresse des T-Accounts. Die E-Mail-Adresse muss mit dem Zusatz „test“, „TST“ oder ähnlich gekennzeichnet sein.
2. Falls mehr als 1 Eintrag vorhanden ist: Kann der Eintrag, auf den das Zertifikat ausgestellt wird, eindeutig durch das Namens-Suffix identifiziert werden?

Ist der Antragsteller nicht oder nicht korrekt im Admin-Directory eingetragen, ist der Eintrag oder die Änderung durch den Admin-Directory Administrator des Amtes zu veranlassen. Das Verfahren kann erst dann fortgesetzt werden, wenn der Antragsteller korrekt im Admin-Directory eingetragen ist (In der Regel dauert die Replikation der Daten min. über Nacht). Der LRA-Officer kann die Überprüfung z.B. im Walk-In Wizard vornehmen.

5.2.3.2 Antragsformular überprüfen

Antragsformular auf Vollständigkeit und Korrektheit überprüfen.

1. Ist der Antragsteller gemäss 5.2.1 berechtigt, bei diesem LRA-Officer einen Antrag zu stellen?
2. Stimmen die Angaben des Antragstellers auf dem Formular mit dem Eintrag im Admin-Directory überein?
3. Ist das Formular korrekt datiert und unterschrieben?

Seit der Einführung des 2-Faktor-Logins für Bundesclients kann anstelle von Einzelanträgen vom jeweiligen HR auch eine Liste der neu eintretenden Mitarbeitenden an den zuständigen LRA-Officer geschickt werden. Die Liste muss dieselben Daten pro Mitarbeiter enthalten wie das Antragsformular. BIT-intern steht im Remedy ein MAC für die Bestellung von Zertifikate der Klasse B zur Verfügung.

5.2.3.3 Terminvereinbarung

Mit dem Antragsteller muss ein Termin für die Ausstellung des Zertifikats vereinbart werden. Dazu wird eine Mail an die auf dem Antrag aufgeführte Mailadresse geschickt. Diese Mail sollte folgenden Inhalt haben:

1. Terminvorschlag/-vorschläge für die Zertifikatserstellung
2. Aufforderung an den Antragssteller, ein gültiges Reisedokument mitzubringen. Das Reisedokument darf zum Zeitpunkt der Registrierung nicht abgelaufen sein. Für Ausnahmeregelungen sind die für die jeweilige Ausnahme definierten Zusatzformulare und –Dokumente mitzubringen (s. Kapitel '5.2.3.5 - Identität des Antragstellers überprüfen')
3. Aufforderung an den Antragsteller, sich eine PIN zurecht zu legen. Die geltenden Regeln für die PIN gemäss ‚3.17 - Regeln für PINs' werden nochmals in Erinnerung gerufen.
4. Aufforderung an den Antragsteller, eine Revokationspassphrase vorzubereiten.
5. Kontaktdetails des LRA-Officers für Fragen und die Lösung von Terminkollisionen

Bei Neueintritten kann die Terminvereinbarung auch durch das zuständige HR koordiniert werden. Dem Antragsteller sind dabei die oben aufgeführten Informationen auf jeden Fall zu kommunizieren.

5.2.3.4 Ausstellungsprozess starten

Nach Eintreffen des Antragstellers startet der LRA-Officer auf dem LRA-Client den Walk-In Wizard und wählt die geeignete Policy aus (für Funktionszertifikate von A-Accounts muss die Policy zur Erstellung eines einzelnen Authentisierungszertifikats angewählt werden). Danach wird der Benutzer mit Name oder E-Mail-Adresse in der Ausstellapplikation gesucht und der korrekte Eintrag ausgewählt. Das AdminDir fungiert hier als Datenquelle.

5.2.3.5 Identität des Antragstellers überprüfen

Für die Überprüfung der Identität muss der Antragssteller persönlich beim LRA-Officer anwesend sein. Die Identifizierung muss mittels eines gültigen Reisepasses oder einer für die Einreise in die Schweiz gültigen Identitätskarte vorgenommen werden. Ein (Firmen-)Personalausweis genügt zur Identifizierung nicht. Die Überprüfung der Identität des Antragsstellers beinhaltet drei Elemente:

1. Überprüfung der Echtheit des vorgelegten Reisedokuments ID/Pass. Zum Beispiel genügt ein (Firmen-) Personalausweis oder ein Führerausweis nicht zur Identifizierung. Das Dokument ist auf folgende Punkte zu überprüfen:
    a. Ist das Reisedokument noch gültig (Zum Zeitpunkt der Registrierung nicht abgelaufen)
    b. Sind die bekannten Sicherheitsmerkmale vorhanden. (Es müssen mindestens vier der offiziellen Sicherheitsmerkmale des Ausweises verifiziert werden)
    c. Entsprechen die Angaben im Dokument denjenigen des Antrags.
    d. Stimmt die Unterschrift im Reisedokument mit derjenigen auf dem Antragsformular überein?

2. Persönliche Identifikation des Antragsstellers durch Vergleich der Person mit der Fotografie auf der Ausweisschrift.
    a. Stimmt die Person mit der Fotografie auf dem Reisedokument überein
    b. Stimmen Alter und Grösse mit den Angaben auf dem Dokument überein

3. Überprüfen, ob die Angaben im Dokument mit denjenigen des Antrags und dem Eintrag im Admin Directory übereinstimmen. Insbesondere muss die Übereinstimmung von Name und Vorname im Dokument mit demjenigen des Admin Directories nach folgenden Kriterien festgestellt werden:

Seit dem 1. Januar 2014 werden in der Bundesverwaltung für Neueintritte vom zuständigen HR zusätzlich zu den Namensfeldern «Name» und «Vorname» die Felder «Name gem. Ausweis» und «Vorname gem. Ausweis» erfasst. Der Inhalt dieser Felder wird im Walk-In-Wizard angezeigt. Je nach Inhalt dieser vier Namensfelder muss die Prüfung nach den nachstehenden Regeln ausgeführt werden. Die dabei angewendete Regel muss auf der entsprechenden Bildschirmseite des Walk-In-Wizards angekreuzt werden. Die anwendbaren Regeln lauten:

- **Regel 1:** Beide Felder «Name gem. Ausweis» und «Vorname gem. Ausweis» sind ausgefüllt und sind identisch mit Name(n) und Vorname(n) auf dem vorgewiesenen Reisedokument Auf dem Bildschirm wird die Option 'Identifiziert mit <Name gem. Ausweis> / <Vorname gem. Ausweis> gemäss Ausweis' angeklickt.

- **Regel 2:** Felder «Name gem. Ausweis» und «Vorname gem. Ausweis» sind ausgefüllt jedoch **nicht** identisch mit dem vorgewiesenen Reisedokument. Auf dem Bildschirm wird die Option 'Feld <Name gem. Ausweis> / <Vorname gem. Ausweis> ungültig' angeklickt. Es wird kein Zertifikat ausgestellt.

- **Regel 3:** Die Felder «Name gem. Ausweis» und «Vorname gem. Ausweis» sind nicht ausgefüllt. «Name» und «Vorname» stimmen jedoch mit dem vorgewiesenen Reisedokument unter Berücksichtigung der Bedingungen im Dokument „Überprüfung Identität Antragsteller Klasse B" [4] überein. Auf dem Bildschirm wird die Option 'Identifiziert mit <Name> / <Vorname>' angeklickt.

- **Regel 4:** Die Felder «Name gem. Ausweis» und «Vorname gem. Ausweis» sind nicht ausgefüllt. «Name» und «Vorname» stimmen auch unter Berücksichtigung der Bedingungen im Dokument „Überprüfung Identität Antragsteller Klasse B" [4] nicht mit dem Reisedokument überein, sind jedoch plausibel. Der Antragsteller hat bereits ein Zertifikat mit diesem Namen/Vornamen besessen, also bei einem Kartenersatz oder dem Ausstellen einer Folgekarte. Dann muss beim zuständigen HR ein Auftrag zur Erfassung der Daten in den Feldern «Name gem. Ausweis» und «Vorname gem. Ausweis» ausgelöst werden. Der Antragsteller muss auf einer Liste mit provisorisch ausgestellten Zertifikaten erfasst werden. Das Zertifikat darf ausgestellt werden. Auf dem Bildschirm wird die Option 'Provisorische Ausstellung mit «Name» / «Vorname»' angeklickt. Die Mutation durch das HR im IPDM (ehemals BV+) muss vom LRA-Officer getrackt werden.

- **Regel 5:** Die Felder «Name gem. Ausweis» und «Vorname gem. Ausweis» sind nicht ausgefüllt. «Name» und «Vorname» stimmen auch unter Berücksichtigung der Bedingungen im Dokument „Überprüfung Identität Antragsteller Klasse B" [4] nicht mit dem Reisedokument überein. Es existiert kein früheres Zertifikat des Antragstellers.
  Es darf kein neues Zertifikat ausgestellt werden. Beim zuständigen HR muss ein Auftrag zur Erfassung der Daten in den Feldern «Name gem. Ausweis» und «Vorname gem. Ausweis» ausgelöst werden. Auf dem Bildschirm wird die Option ' <Name> / <Vorname> ungültig' angeklickt.

Ausnahme 'Ausweis F'

In Ausnahmefällen kann eine Identifizierung auch anhand eines gültigen 'Ausweis F' erfolgen. Die Überprüfung des Ausweises muss den oben beschriebenen Regeln zur Überprüfung eines Reisedokuments entsprechen. Bei Anträgen mit 'Ausweis F' als Grundlage müssen die nachstehend aufgeführten zusätzlichen Formulare und Dokumente vorgewiesen werden:

- Vollständig ausgefülltes und vom zuständigen ISBO unterschriebenes 'Ergänzendes Formular für Antragsteller mit Ausweis F' [5]. Auf diesem Formular anerkennt der ISBO, dass der Antragsteller aufgrund der vorgelegten Ausweisschriften nicht eindeutig identifiziert werden kann, und akzeptiert das damit verbundene Risiko für seine Organisation.
- Die Bewilligung der zuständigen kantonalen oder Bundesbehörde zur Erwerbstätigkeit.

5.2.3.6 Karte vorbereiten

In der Bundessverwaltung wird strategisch das Produkt Prestaged Smartcard eingesetzt. Diese Smartcards werden zentral für den Einsatz bei der SG-PKI vorbereitet und müssen deshalb nicht separat initialisiert werden. Nicht formatierte Non-prestaged Smartcards, die die PUK-Verwaltung der SG-PKI verwenden, werden während des Ausstellprozesses durch den Walk-in Wizard oder durch den Register Smartcard-Wizard initialisiert.

Wird das PUK-Management anderer Hersteller (wie z.B. Privacy PUK oder SCAMIAD) verwendet, so ist nach den internen Vorgaben der Organisationseinheit vorzugehen und die Smartcard vorgängig mit dem Drittprodukt unter Berücksichtigung der Regelungen in Kap.3.18 dieser Richtlinien zu initialisieren.

5.2.3.7 Dokumente digitalisieren

Die für die Identifikation verwendeten Dokumente, insbesondere Ausweise, müssen während des Ausstellungsprozess digitalisiert und im System (Background Server) gespeichert werden. Dazu steht im Walk-In-Wizard ein integrierter Scanprozess zur Verfügung.

Um beim Scanvorgang qualitativ gute Resultate zu erzielen, verwenden Sie folgende Einstellungen:

Farben: TrueColor
Auflösung: **200 x 200** oder 300 x 300 (je nach Einstellmöglichkeiten des Scanners)
File Format: **JPEG** (File Extension: .jpg)
PDF (File Extension: .pdf) für doppelseitigen Scan beider Seiten der ID

Normalerweise hat das Resultat des Scanvorgangs eine Grösse von A4. Schneiden Sie vor dem Speichern das Reisedokument aus, so dass nur noch das eigentliche Reisedokument gespeichert wird.
Speichern Sie das Dokument in ein privates Verzeichnis Ihres Clients. Nach der Ausstellung des Zertifikates sind Sie verpflichtet diese Dateien und allfällige E-Mails zu löschen, und anschliessend den Papierkorb des Clients sowie des Outlooks zu leeren!

Wichtig: IDs müssen **beidseitig** eingescannt werden, da die Gültigkeitsdauer nur auf der Rückseite ersichtlich ist.

5.2.3.8 Information Antragsteller über PIN und Revokationspassphrase

Der Antragsteller wird nochmals über Sinn und Zweck der Revokationspassphrase orientiert und, falls er sich noch keine Passphrase zurechtgelegt hat, aufgefordert, sich eine solche gemäss den Vorgaben in Kapitel 3.178 zu überlegen. Ebenfalls werden nochmals die Regeln für die PIN-Bildung gemäss Kapitel 3.16 in Erinnerung gerufen.

5.2.3.9 Zertifikate beantragen und auf Karte speichern

Die Smartcard des Antragstellers wird in den zweiten Kartenleser eingesteckt. Standardzertifikate dürfen nicht mit Klasse A Zertifikaten oder Klasse B Funktionszertifikaten auf derselben Karte erstellt werden. Mehrere Klasse B Funktionszertifikate (z.B. ein Administrator-Zertifikat und mehrere Test-Zertifikate) dürfen jedoch auf der gleichen Karte gespeichert werden.

Im nächsten Schritt werden alle benötigten und vorgängig digitalisierten Dokumente im System gespeichert. Minimal handelt es sich dabei um die Kopie des gültigen Reisedokuments. Alle Dokumente, die für die eindeutige Identifizierung und Registrierung benötigt wurden, z.B. Heiratsurkunden, Bürgschaftsschreiben, weitere Ausweise etc., müssen eingebunden werden. Der Prozess dazu ist im Kap. 5.2.3.7 - Dokumente digitalisieren beschrieben.

Der Wizard erstellt anschliessend den Antrag und sendet ihn an das zentrale System, wo die Zertifikate erstellt werden.

Der Benutzer wird aufgefordert, seine persönliche PIN und die Revokationspassphrase einzugeben. Danach werden die Zertifikate auf die Benutzer-Smartcard geschrieben und die Karte mit der persönlichen PIN des Users gesichert.

5.2.3.10 Erhalt quittieren lassen/Unterzeichnung der Benutzervereinbarung

Im Anschluss an die Zertifikatsausstellung wird ein Blatt mit den «Fingerprints» (eindeutige Erkennungszahl für ein Zertifikat) der Zertifikate ausgedruckt. Der Antragsteller muss mündlich anhand der Dokumente *«Benutzervereinbarung und Nutzungsbedingungen Klasse B»* [2] und *«Guidelines zu Zertifikate der Klasse B Zertifikaten der Swiss Government PKI»* [3] auf seine Rechte und Pflichten aufmerksam gemacht werden (Zweck der Zertifikate, Inhalt der Smartcard, Revozieren der Zertifikate, Sorgfaltspflicht für PIN, Revokationspassphrase).

Eine Kopie der *«Benutzervereinbarung und Nutzungsbedingungen Klasse B*» [2] muss zum Schluss vom Antragsteller unterschrieben werden. Damit bezeugt er, die Informationen gelesen und zur Kenntnis genommen und die Smartcard mit den Zertifikaten erhalten zu haben. Der LRA-Officer vergleicht die Unterschrift auf diesem Formular mit derjenigen auf dem Antragsformular. Die Kopie der Fingerprints wird an das unterschriebene

Exemplar der *«Benutzervereinbarung»* angeheftet. Alternativ zur Papierkopie ist dem LRAO frei gestellt die «*Benutzervereinbarung*» dem Antragsteller elektronisch zur Verfügung zu stellen. Er muss jedoch dafür besorgt sein, die mit dem Klasse B Zertifikat signierte Version des Dokuments innerhalb von 5 Arbeitstagen zu erhalten und diese gem. den Vorgaben im Kap. 3.8 elektronisch zu archivieren. Erhält der LRAO die signierte Benutzervereinbarung nicht zurück, müssen die entsprechenden Zertifikate revoziert werden.

5.2.3.11 Abschluss Ausstellung

Zum Schluss werden dem Antragsteller

- die neue Smartcard
- die nicht unterschriebenen Kopien der «*Benutzervereinbarung»* [2] sowie der *«Guidelines»* [3]
- seine Reisedokumente sowie die weiteren benötigten Unterlagen

ausgehändigt.

5.2.3.12 Journal führen

Die durchgeführten Aktivitäten müssen vom LRA-Officer im LRA Journal festgehalten werden. Dabei gelten die unter ‚3.7 - Journal' aufgeführten Regeln.

5.2.3.13 Gespeicherte Dateien von lokalen Systemen löschen

Falls Scans der Reisedokumente ausserhalb des Walk-In-Wizards gemacht und lokal gespeichert wurden, müssen diese nach erfolgter Ausstellung der Zertifikate wieder gelöscht werden. Insbesondere ist hier auch zu achten, dass nichts auf persönlichen oder firmeneigenen Mail Accounts gespeichert bleibt (Siehe auch ‚5.2.3.7 – Dokumente digitalisieren')

Bemerkung: Dies muss gemacht werden, weil es sich sonst um eine nicht angemeldete Datensammlung i.S. des Datenschutzgesetzes handeln würde. Die Dateien werden jedoch während des Ausstellungsprozesses in der Datenbank der Swiss Government PKI abgelegt (welche nach DSG29 gemeldet ist).

5.2.3.14 Ablage Kundendossier

Der ausgeführte Antrag, die unterschriebene Kopie des Formulars und die *«Benutzervereinbarung und Nutzungsbedingungen Klasse B»* [2] werden im Kundendossier abgelegt.

Wird das Kundendossier elektronisch geführt, müssen die vorgängig erwähnten Dokumente gescannt, im PDF/A gespeichert, mit dem persönlichen Klasse B Zertifikat des LRAO unterschrieben und dann so abgelegt werden, dass:

- Eine Chronologie erkennbar ist
- Der Auftrag jederzeit gefunden werden kann
- Allfällige Informationen von Umsystemen, (wie z.B. Ticketnummer, etc.) vorhanden sind (dazugehörige Tickets etc. müssen min. 11 Jahre nach Ablauf des Zertifikates auffindbar sein)

5.2.4 Ausstellen mit RIO

Im Prozess «Ausstellen mit RIO» delegiert der LRA-Officer die Identifikation des Antragstellers und weitere Aufgaben an den RIO (Registration Identification Officer). Der Antragssteller und der RIO befinden sich dabei an einem vom LRA-Officer entfernten Ort. Der Prozess wird auch asynchroner Ausstellprozess genannt. Administrations-Funktionszertifikate dürfen nicht über diesen Prozess ausgestellt werden.

Weitere zu befolgende Dokumente zu diesem Prozess sind die «*Richtlinien für den Registration Identification Officer (RIO)*» [13] und die «*Quickguide Walk-In-Wizard asynchron*» [14]. Bei widersprüchlichen Anweisungen gilt diese Richtlinie.

Im Interesse der Vollständigkeit wird hier der gesamte Prozess beschrieben, also einschliesslich der Schritte, die der Antragssteller zur Aktivierung der Smartcard zum Schluss selbst ausführt.

5.2.4.1 Antragserstellung

Der Antragsteller füllt auf dem Formular «*Klasse B: RIO Antrag zur Ausstellung von Klasse B*» den Abschnitt 1 mit den Angaben zu seiner Person und seinen Organisations- und Kommunikationsdaten. Er datiert und unterschreibt diesen Abschnitt.

5.2.4.2 Identifikation Antragsteller durch den RIO

Die Identität des Antragstellers muss vom RIO eindeutig festgestellt werden. Dazu muss der Antragsteller den RIO persönlich aufsuchen. Anhand der nachfolgenden Schritte werden die nötigen Kontrollen durchgeführt und die zusätzlichen Angaben im Antragsformular ergänzt.:

1. Der Antragssteller meldet sich mit seinem Identifikationsmittel (gültiger, nicht abgelaufener Reisepass oder Identitätskarte) persönlich bei einem RIO.
2. Der RIO geht anhand der Checkliste RIO vor und füllt diese aus.
3. Der RIO kontrolliert anhand des Reisedokumentes, ob das Gesicht des Antragstellers mit dem Gesichtsbild des Reisedokumentes übereinstimmt. Bei Nichtübereinstimmung verweigert der RIO die Fortsetzung des Identifikationsprozesses und meldet den Verstoss dem zuständigen LRA-Officer. Alternative Identifikationsmittel nach Ausnahmeregelungen und die dabei anzuwendenden Prozesse sind im Kapitel '5.2.3.5 - Identität des Antragstellers überprüfen' aufgeführt. Die dortige Auflistung ist abschliessend.
4. Bei Übereinstimmung übergibt der RIO dem Antragsteller eine neue registrierte Smartcard und notiert die Seriennummer des Kryptochips auf dem dafür vorgesehenen Feld des Formulars. Wenn die Seriennummer nicht auf der Smartcard aufgedruckt ist, kann sie entweder mittels der Karten-Middleware oder dem Unseal Wizard abgefragt werden. Der RIO macht den Benutzer darauf aufmerksam, dass dieser die neue Karte ab sofort unter seiner alleinigen Kontrolle behalten muss.
5. Der RIO und der Antragsteller bestätigen mit ihrer Unterschrift in Abschnitt 2 des Antragsformulars, dass eine persönliche Begegnung und die Identifikation anhand eines gültigen Reisedokumentes stattgefunden haben und dass der Antragsteller die bezeichnete Smartcard erhalten hat.
6. Der RIO stellt sicher dass der Antragsteller den Inhalt der «*Benutzervereinbarung und Nutzungsbedingungen Klasse B*»I' [2] verstanden und eine Kopie davon erhalten hat. Eine zweite Kopie muss vom Antragsteller unterschrieben werden.
7. Der RIO legt das Antragsformular und das Reisedokument so auf das Kopiergerät, dass das Reisedokument mit sichtbarem Gesichtsbild auf der Kopie im vorgesehenen Feld der Antragsbestätigung erscheinen wird.
   IDs müssen beidseitig kopiert werden.
8. Der RIO kopiert das Antragsformular und das Reisedokument sowie sämtliche, für die Ausstellung benötigten Zusatzformulare und Dokumente. Der Antragsteller und der RIO unterzeichnen die nun vollständige Kopie des Antragsformulars. Das Antragsformular ohne das kopierte Reisedokument kann vernichtet werden.
9. Der RIO schickt die beiden unterschriebenen Dokumente (Antragsformular und unterschriebene «*Benutzervereinbarung*» [2]), die Kopien allfälliger Zusatzdokumente sowie die ausgefüllte Checkliste an den zuständigen LRA-Officer. Die Zustellung kann auf eine der beiden nachfolgend beschriebenen Arten vorgenommen werden:
   a. Die unterschriebenen Dokumente werden per Post oder Kurier an den zuständigen LRA-Officer geschickt.
   b. Der RIO scannt die Dokumente im PDF/A Format und signiert sie mit seinem gültigen Klasse B Standardzertifikat. Die so präparierten Dokumente werden dann per verschlüsselter Mail an den zuständigen LRA-Officer geschickt. Die Voraussetzungen für dieses Vorgehen sind:
      i. Der RIO ist im Besitz eines gültigen Klasse B Standardzertifikats
      ii. Der RIO hat Zugang zum öffentlichen Encryption Key des LRA-Officers
      iii. Der RIO Arbeitsplatz ist mit einer Scanmöglichkeit ausgerüstet
10. Werden die Dokumente elektronisch übermittelt, so müssen die Papierdokumente nachträglich per

Briefpost an den LRA-Officer zur Ablage im Kundendossier geschickt werden, sofern keine elektronischen Kundendossiers gemäss Spezifikationen in Kapitel „5.2.4.3 - Genehmigung Antrag durch LRA-Officer“ geführt werden.

5.2.4.3 Genehmigung Antrag durch LRA-Officer

Nach Erhalt und Kontrolle der unter ‚5.2.4.2 - Identifikation Antragsteller durch den RIO‘ ausgefertigten Dokumente kann der LRA-Officer den Antrag genehmigen und die Generierung der Zertifikate freigeben. Dazu führt er folgende Schritte der Checkliste „Ausstellen mit RIO“ aus:

1. Der LRA-Officer überprüft, ob alle Dokumente beigelegt sind und das Antragsformular von einem autorisierten RIO unterzeichnet ist. Die benötigten Dokumente sind:
   - Unterzeichnetes Antragsformular
   - Unterzeichnetes Formular «*Benutzervereinbarung- und Nutzungsbedingungen Klasse B Zertifikaten der Swiss Government PKI*» [2]
   - Unterzeichnete ‚Checkliste RIO ‘
   - Weitere, im Falle einer Ausnahmeregelung verlangte Dokumente und Ausweise

   Wurden die Dokumente via E-Mail übermittelt, überprüft der LRA-Officer, ob
   - Die Dokumente verschlüsselt übermittelt wurden
   - Die Dokumente mit der gültigen Signatur des RIO elektronisch unterschrieben sind
2. Der LRA-Officer startet auf dem LRA-Client mit seiner Smartcard den Walk-In-Wizard im RIO Modus. Er sucht den Antragssteller im System, indem er seinen Namen oder seine E-Mail-Adresse eingibt.
3. Wurden die Formulare in Papierform übermittelt, scannt der LRA-Officer die vom RIO erhaltenen, unterzeichneten Kopien des Antragsformulars und der unterzeichneten «*Checkliste RIO*» sowie weitere, im Falle einer Ausnahmeregelung verlangte Dokumente und Ausweise. Um qualitativ gute Resultate zu erzielen, sollten folgende Einstellungen verwendet werden:

Farben:	TrueColor
Auflösung:	200 x 200 oder 300 x 300 (je nach Einstellmöglichkeiten des Scanners)
File Format:	JPEG (File Extension: .jpg) oder PDF/A (File Extension .pdf)

   Elektronisch erhaltene Dokumente können direkt eingebunden werden. Die Dokumente lädt der LRA-Officer dann in den Walk-In-Wizard
4. Der LRA-Officer überprüft, ob die Angaben auf dem Antragsformular mit denjenigen der Ausweiskopie und dem Eintrag des Antragstellers im AdminDir übereinstimmen (s. Richtlinien in Punkt 3 im Kapitel „5.2.3.5 - Identität des Antragstellers überprüfen“).
5. Stimmen die nötigen Angaben überein, so gibt der LRA-Officer die Seriennummer der dem Benutzer ausgehändigten Smartcard ein und gibt den Antrag frei.
6. Der frei gegebene Antrag wird in einem Ticket angelegt und an die CA zur Zertifizierung übermittelt. Die Ticketnummer wird in einem sogenannten Unseal-Dokument (pdf-Format) festgehalten
7. Der LRA-Officer leitet das Unseal-Dokument oder den Unseal-Code («E-Ticket-Nummer») entweder direkt an den Benutzer oder an den RIO weiter.
8. Der LRA-Officer trägt den Vorgang im Journal nach
9. Der LRA-Officer legt das unterzeichnete Formular «*Benutzervereinbarung und Nutzungsbedingungen Klasse B*» [2] im Kundendossier ab.

   Wird das Dossier elektronisch geführt, muss entweder die vom RIO signierte elektronische Version abgelegt werden oder der LRA-Officer erstellt aus den Papierdokumenten eine PDF/A Version, die er vor der Ablage mit seinem Zertifikat der Klasse B unterzeichnet. Die elektronischen Kundendossiers müssen bezüglich Aufbewahrungssicherheit, Datenschutz, Aufbewahrungsdauer und Revisionsfähigkeit die Anforderungen in den Kap. 5.2.3.13 und 3.8 dieser Richtlinien erfüllen.

5.2.4.4 Installation des Zertifikats auf der Smartcard des Antragstellers

Als letzter Schritt muss das Zertifikat noch auf der Smartcard des Antragstellers installiert werden

1. Nach erfolgter Zertifikatsausstellung erhält der Antragssteller per E-Mail oder via RIO das Unseal-Dokument mit der E-Ticket-Nummer.
2. Der Antragssteller startet den Unseal Wizard auf einem am Netz angemeldeten Client und schiebt seine Smartcard ins Lesegerät. Falls der Client den 2-Faktor-Login für Windows verlangt, muss für diesen Schritt ein zweites Kartenlesegerät installiert sein. Der Benutzer gibt die erhaltene Ticketnummer ein. Der Wizard prüft, ob die im Ticket spezifizierte Smartcard mit derjenigen im zweiten Lesegerät eingesteckten Smartcard übereinstimmt.
3. Bei Übereinstimmung wird der Benutzer aufgefordert, seine persönliche PIN und die Revokationspassphrase einzugeben
4. Der Wizard speichert die Revokationspassphrase in der zentralen Datenbank ab, lädt die Zertifikate auf die Smartcard und sichert die Karte mit der neuen persönlichen PIN.

5.3 Prozess Zertifikat revozieren

5.3.1 Wer kann eine Revokation beantragen?

Die folgende, abschliessende Aufzählung listet alle Rollen auf, die eine Revokation eines Zertifikats beantragen können:

- der Zertifikatsinhaber selbst
- Mitarbeiter des zuständigen HR (Personaldienst)
- Linienvorgesetzte,
- der Swiss Government PKI Verantwortliche
- der PKI Security Officer
- der zuständige LRA-Officer
- der ISBO des Amtes

5.3.2 Wie kann eine Revokation beantragt werden?

Der Zertifikatsinhaber kann die Revokation beim LRAO persönlich, via E-Mail oder per Telefon beantragen. Der LRA-Officer plausibilisiert den Request, z.B. über die Revokationspassphrase.

HR-Stellen oder Vorgesetzte können Revokationsanträge auch als Listen (z.B. Excel-Files) an den LRA-Officer schicken. Dies ist vor allem bei Austritten oder Wechseln von Mitarbeitern der Fall. Der LRA-Officer überprüft die Zuständigkeit. Der LRAO darf Revokationsanträge von Drittpersonen nur schriftlich entgegennehmen (signierte Mail, signierte Revokationsanträge). Die telefonische Revokation ist nur für den Zertifikatsinhaber bestimmt.

Der LRA-Officer, der PKI Security Officer und der Swiss Government PKI Verantwortliche können ein Zertifikat direkt in der LRA Anwendung revozieren.

5.3.3 Welches sind Gründe für eine Revokation?

Die Gründe für eine Revokation sind insbesondere:

- Die Smartcard ist gestohlen worden oder kann nicht mehr gefunden werden.
- Die Smartcard ist defekt.
- Die Smartcard wird erneuert.
- Der Kunde hat die PIN für die Smartcard vergessen und es existiert kein PUK-Verwaltungssystem, um die PIN zurücksetzen zu können.
- Die Smartcard wurde wegen zu vielen Fehlversuchen gesperrt und es existiert kein PUK-Verwaltungssystem, um die Karte entsperren zu können.

- Beendigung des Arbeitsverhältnisses mit dem Zertifikatsinhaber.
- Änderung von Daten, die im Zertifikat enthalten sind (Name, E-Mail-Adresse, etc.).
- Verdacht auf Kompromittierung (bekannt werden) des privaten Schlüssels (andere Person konnte einen Dienst nutzen, z.B. eine E-Mail signieren).
- Der Kunde hält sich nicht an die Richtlinien (z.B. Nicht-Befolgen der CP/CPS).
- Der LRA-Officer hält eine Revokation aus anderen Gründen angezeigt.

5.3.4 Vorgehen

Ein Revokationsantrag ist **immer sofort** zu bearbeiten. Herrscht betreffend der Gültigkeit eines Revokationsantrags Unsicherheit (z.B. bei einem telefonischen Antrag), ist folgendes zu beachten: Das Ziel der Revokation ist es, den Kunden vor einem möglichen Schaden durch den Missbrauch seiner Zertifikate zu bewahren. Ein betrügerischer Revokationsantrag und nachfolgende Revokation können aber auch Schaden anrichten, indem die Dienstleistungen vom Kunden nicht mehr genutzt werden können, oder eine Amtshandlung verhindert wird. Der LRA-Officer hat also den potenziellen Schaden einer Nichtrevokation und einer betrügerischen Revokation abzuschätzen.

Der LRA-Officer geht wie folgt vor:

5.3.4.1 Plausibilisieren des Antrags

Anhaltspunkte sind:

- Kann der Antragsteller identifiziert werden? (Stimme, Telefonnummer, Revokationspassphrase)?
- Ist die HR-Stelle oder der Vorgesetzte zuständig für die Zertifikatsinhaber?

5.3.4.2 Formular für Revokation

Wird ein Revokationsantrag durch Drittpersonen (also nicht der LRAO und nicht der Zertifikatsinhaber selbst) veranlasst (vgl. hierzu Kap. 5.3.1), so muss der Revokationsantrag schriftlich, mittels «*Revokation Zertifikate der Swiss Government PKI Klasse B*» erfolgen. Wird der Antrag nicht in Papierform vorgelegt ist dabei zu achten, dass das Dokument, oder die Mail mit der Anlage vom Antragsteller signiert wurden.

Ebenso ist ein Formular für die Revokation dann notwendig, wenn die Informationen (Grund, Auftraggeber) zur Revokation nicht im Revokations-Wizard eingegeben werden, bzw. wenn nicht über den offiziellen Revokation-Wizard revoziert werden kann. Das Formular kann in diesen Fällen auch vom LRAO ausgefüllt werden. Dies gilt insbesondere bei Revokationen mit der CMC-Konsole und bei Revokationsaufträgen an die SG-PKI.

5.3.4.3 Revokation

Für die Revokation wird der Revocation-Wizard auf der LRA Station gestartet und der Zertifikatsinhaber gesucht. Danach werden die zu revozierenden Zertifikate ausgewählt. Der LRAO erhält eine Seite mit den für das Zertifikat gespeicherten Identitätsdokumenten. Er verifiziert anhand dieser Dokumente die Identität des Zertifikatsinhabers.

Nach erfolgter Identifizierung werden die gewählten Zertifikate revoziert. Der Zertifikatsinhaber erhält automatisch eine Mitteilung per Mail über die Revokation.

5.3.4.4 Administrativer Abschluss

Ist ein Revokationsformular vorhanden, wird es im Kundendossier abgelegt. Wird das Kundendossier elektronisch geführt, gelten dazu die Anforderungen in den Kap. 3.8 und 5.2.3.14. Der Revokationsvorgang wird im Journal gemäss ‚3.7 - Journal' dokumentiert.

5.4 Prozess Zertifikat erneuern

Zertifikate können innerhalb ihrer Gültigkeitsdauer bis zu zwei Mal durch die Inhaber selbstständig erneuert werden. Dieser Vorgang wird Renewal oder Rekeying genannt. Voraussetzung ist, dass die aktuellste Version

des Renewal Wizards auf dem Client des Benutzers installiert ist und dass sich auf der Smartcard noch genügend Speicherplatz befindet. Da Prestaged Smartcards bereits drei Schlüsselsätze auf der Karte haben, ist diese Bedingung für diesen Kartentyp in der Regel gegeben. Das Vorgehen ist dabei wie folgt:

- Starten des Renewal Wizards auf dem Büroautomationsclient des Benutzers mit dem noch gültigen Klasse B Zertifikat.
- Die sich im Kartenleser befindliche Smartcard wird angezeigt.
- Bestätigen, dass es sich um die korrekte Karte handelt
- Anschliessend lässt der Wizard 3 neue Zertifikate erstellen und auf die Smartcard schreiben. Das alte Signaturzertifikat und Authentifikationszertifikat werden gelöscht. Alte Verschlüsselungszertifikate bleiben auf der Smartcard erhalten.

Falls die Zertifikate schon abgelaufen sind, kann die oben beschriebene Erneuerung nicht mehr durchgeführt werden. Es muss ein neues Zertifikat durch den LRA-Officer ausgestellt werden. Das Verfahren ist das gleiche wie bei der Erstausgabe der Zertifikate.

5.5 Prozess Key Recovery eigener Schlüssel

Der Zertifikatsinhaber kann für seine eigenen Verschlüsselungsschlüssel selbstständig ein Key Recovery beantragen. Das Vorgehen ist dabei wie folgt:

Über die URL https://keyrecovery.pki.admin.ch/KeyRecoveryRequest/ kann man sich mit seinem aktuell gültigen Klasse B Zertifikat an der Anwendung anmelden und ein E-Ticket für Key Recovery initialisieren. Mit der Ticket-Nummer und seiner Smartcard begibt man sich zum nächsten zuständigen LRA-Officer oder Key Recovery Agent (KRA).

Dieser identifiziert den Benutzer und startet den Key Recovery Wizard. Er steckt die Smartcard des Benutzers in einen freien Kartenleser und gibt die Nummer des E-Tickets ein. Danach werden dem Benutzer seine alten Verschlüsselungsschlüssel am Bildschirm angezeigt. Nach Auswahl des gewünschten Schlüssels wird dieser zusätzlich zu den bereits vorhandenen Encryption Keys auf die Smartcard geschrieben.

5.6 Prozess Key Recovery Fremdschlüssel

Grundsätzlich dürfen Encryption Schlüssel nur auf die Smartcard des Besitzers geschrieben werden. In ausserordentlichen Fällen kann es aber dennoch nötig sein, den oder die Encryption Keys einer Person auf die Karte eines anderen Benutzers zu installieren. Gründe dafür können sein:

- Der/die MitarbeiterIn ist nicht mehr für das Amt tätig.
- Der/die MitarbeiterIn ist für längere Zeit krankheitsbedingt abwesend
- Der/die MitarbeiterIn ist verstorben.

Da damit alle verschlüsselten Mails und Dokumente des Zertifikatsinhabers gelesen werden können (sofern sich auch die verschlüsselten Daten im Besitz des Schlüsselhalters befinden), muss jeder dieser Fälle separat beurteilt werden. Zu diesem Zweck muss ein detailliert begründeter Antrag an den Verantwortlichen der PKI gestellt werden. Das weitere Vorgehen wird dann individuell und immer unter Beizug des Rechtsdienstes festgelegt.

6 Formulare und Checklisten

Für die obengenannten Prozesse wurden die nachstehenden Formulare und Checklisten ausgearbeitet. Alle Formulare und Checklisten können als separate Dokumente beim PKI-Verantwortlichen oder auf der WEB-Seite der Swiss Government PKI bezogen werden:

6.1 Formular Zertifikatsantrag

Vor der Ausgabe der Zertifikate über den Prozess «*Ausstellen ohne RIO*» (vgl. Kapitel 5.2.3) muss der Kunde den «*Klasse B: Antrag für persönliche Zertifikate der Swiss Government PKI Klasse B*» ausfüllen. Das Formular kann von der WEB-Seite der Swiss Government PKI heruntergeladen werden. Es steht den Kunden frei, für ihre Organisation ein eigenes Formular für diesen Zweck zu entwerfen. Dabei müssen mindestens folgende Daten erhoben werden:

- Name, Vorname
- Organisationseinheit
- E-Mail
- Eindeutige Personalnummer oder Suffix

Zusätzlich sollte das Formular bereits Hinweise über die Regeln zur Bildung der PIN und der persönlichen Passphrase enthalten.

Das Formular soll dem Kunden zum Voraus abgegeben werden, damit er genügend Zeit hat, sich eine PIN sowie eine Revokationspassphrase zu überlegen. Der Kunde unterschreibt das Antragsformular und bestätigt die Korrektheit der Informationen.

Alternativ können Ämter, Klasse B Zertifikate auch via Ihr internes Auftragserfassungssystem (z.B. Remedy-MAC, Gever etc.) beantragen. Dabei ist sicherzustellen, dass die Anträge den Ausstellungen eindeutig zugeordnet werden können und 11 Jahre nach Ablauf der Gültigkeit des Zertifikats archiviert und auditierbar bleiben (vgl. Kap. 5.2.3.14 und 3.8).

In der Bundesverwaltung ist die Erstausgabe des Standardzertifikats in der Regel in den HR-Prozess ‚Eintritt neue Mitarbeiter' integriert. Die neu eintretenden Mitarbeiter können vom zuständigen HR dem LRA-Officer auch auf Listen gemeldet werden. Dabei sind pro Neueintritt die oben erwähnten Daten aufzuführen.
Für den Prozess «*Ausstellen mit RIO*» (vgl. Kapitel 5.2.4) wird das Formular «*Klasse B Antrag zur Ausstellung von Klasse B Zertifikaten»* verwendet.

6.1.1 Ergänzendes Formular für Antragsteller mit Ausweis F

Wird unter der Ausnahmeregelung ein Antrag für einen Benutzer mit 'Ausweis F' gestellt, muss zusätzlich zum Antragsformular das «*Ergänzendes Formular für Antragsteller mit Ausweis F*» ausgefüllt und vom zuständigen ISBO unterzeichnet werden. Mit seiner Unterschrift bestätigt der ISBO, davon Kenntnis genommen zu haben, dass der Antragsteller mit einem 'Ausweis F' nicht eindeutig identifiziert werden kann und die SG-PKI folglich keine Garantie über die korrekte Identifizierung des Antragstellers abgeben kann. Das Formular ist Bestandteil der auditrelevanten Dokumentation der betroffenen Ausstellprozesse.

6.2 Benutzervereinbarung und Nutzungsbedingungen Klasse B

Das Formular «*Benutzervereinbarung und Nutzungsbedingungen Klasse B*» [2] enthält nur die wichtigsten Informationen; es wurde speziell für den Endbenutzer erstellt. Die vollständige Information ist in der CP/CPS [1] enthalten. Das Formular ist Bestandteil der auditrelevanten Dokumentation eines Ausstellprozesses. (Das momentan noch vorhandene Formular «*Bestätigung für Erhalt und Umgang mit der Smartcard*» enthält die Fingerprints der Zertifikate. Am Ende des Dokumentes wird die Smartcard Nummer, falls vorhanden, eingetragen.

Diese Nummer kann bei Problemen mit der Smartcard (Verlust oder Beschädigung) hilfreich sein. Das Formular ist nicht Bestandteil der Auditrelevanten Dokumentation eines Ausstellprozesses.

6.3 Formular zur Revokation

Bei der Revokation mit dem Revoke-Wizard müssen Auftraggeber und Grund im Wizard hinterlegt werden, in diesem Fall muss das Revokationsformular nicht ausgefüllt und nicht abgelegt werden. Andernfalls gehört das Formular zur auditrelevanten Dokumentation eines Revokationsprozesses - Vgl. hierzu Kap. 5.3.4.2.

6.4 Formular Key Recovery Fremdschlüssel

Zu diesem Prozess wird kein spezielles Formular erstellt. Der Antrag muss mit einer detaillierten Begründung an den Verantwortlichen PKI gestellt werden. Die dazu benötigten Unterlagen sind Bestandteil der auditrelevanten Dokumentation für das KeyRecovery.

6.5 Checkliste Zertifikat ausstellen ohne RIO

Diese Checkliste «*Ausstellen von Klasse B Zertifikaten*» dient dem LRA-Officer als Behelf bei der Ausstellung und muss nicht ausgefüllt oder pro erstelltem Zertifikat abgelegt werden.

6.6 Checkliste Zertifikat ausstellen mit RIO

Diese Checkliste «*Ausstellen mit RIO*» dient dem LRA-Officer als Behelf bei der Ausstellung und muss nicht ausgefüllt oder pro erstelltem Zertifikat abgelegt werden.

6.7 Checkliste RIO

Die «*Checkliste RIO*» ist ein erforderliches Element der Antragstellung beim Prozess mit RIO. Es muss vom RIO mit jedem Antrag ausgefüllt, an den bewilligenden LRA-Officer geschickt und von diesem im Kundendossier abgelegt werden. Diese Checkliste ist Bestandteil der auditrelevanten Dokumentation eines Ausstellprozesses.

6.8 Checkliste Zertifikat revozieren

Diese Checkliste «*Revokation von Klasse B Zertifikaten*» dient dem LRA-Officer als Behelf bei der Ausstellung und muss nicht ausgefüllt oder pro revoziertem Zertifikat abgelegt werden.

7 Eskalationsverfahren

Sollten Unklarheiten, Fragen oder Probleme mit Kunden, dem Betrieb der Swiss Government PKI oder anderen OEs auftreten, die Sie nicht selbst lösen können, wenden Sie sich bitte an den PKI-Verantwortlichen des BIT.

8 Änderungsvorschläge

Bitte senden Sie Bemerkungen oder Änderungsvorschläge zu diesem Dokument oder zu den Formularen an:

Serviceverantwortlicher Swiss Government PKI
Bundesamt für Informatik und Telekommunikation
Monbijoustrasse 74
CH-3003 Bern
E-Mail: pki-info@bit.admin.ch

ANHANG

Anhang A: Prozess Checklisten – Klasse B

Checkliste: Ausstellen von Klasse B Zertifikaten

Prozess Klasse B „Ausstellen ohne RIO“ (RR Kapitel 5.2.3)

V2.1, 20.09.2019

Nr.	Beschreibung	Referenz RR [1]
Vorarbeiten zur Zertifikatsausstellung		
1.	Antrag überprüfen:	
	a) Ist der Antragsteller im Admin-Directory vorhanden? Mit korrektem Namen inklusive Suffix und E-Mail-Adresse?	5.2.3.1
	b) Ist der Antragsteller zum Bezug eines Zertifikates der Klasse B berechtigt? Im Ast des AdminDir, in dem der LRAO zuständig ist	5.2.1
	c) Stimmt die E-Mail-Adresse im Antrag mit dem Eintrag im Admin-Directory überein?	5.2.3.2
	d) Sind die Angaben im Antrag vollständig und plausibel?	5.2.3.2
2.	Termin für die Ausstellung des Zertifikats über die vom Antragsteller angegebene E-Mail-Adresse vereinbaren. Es muss mindestens darauf hingewiesen werden, dass nur Pass oder ID als Identifikationsnachweis akzeptiert werden. Hilfreich ist auch, wenn bereits Informationen zur Wahl der PINs und der Revokationspassphrase gegeben werden.	5.2.3.3
3.	Smartcard vorbereiten: Eine separate Initialisierung ist nur dann notwendig, wenn für die PUK-Verwaltung eine Fremdsoftware eingesetzt wird. Alle anderen Karten sind entweder bereits beim Prestaging vorbereitet worden oder werden vom Walk-In-Wizard bei der Verarbeitung als Erstes formatiert.	5.2.3.6
Zertifikatsausstellung		
4.	Identität überprüfen	5.2.3.5
	a) Art des Reisedokumentes: Handelt es sich um einen Pass oder eine ID? Oder kann der Antragsteller gemäss einer Ausnahmeregelung mit einem anderen Ausweis identifiziert werden? Ist das Dokument echt (min.4 Sicherheitsmerkmale checken)?	
	b) Ist das (Reise-)Dokument noch gültig?	

[1] Swiss Government PKI_B_Registrierrichtlinien

	c) Entsprechen die Angaben im Antrag denen im (Reise-)Dokument und denen im AdminDir, insbesondere der Name und Vorname des Antragstellers.?	
	d) Gesicht des Antragsstellers mit Gesichtsbild im (Reise-)Dokument vergleichen. Kann der Antragsteller diese Person sein?	
5.	Ausweis und ggf. weitere benötigten Dokumente digitalisieren und speichern	5.2.3.7
6.	Information des Antragstellers über die Wahl des PIN und der Revokationspassphrase *(kann auch bereits im Einladungs-Mail erwähnt werden)*	5.2.3.8
7.	Smartcard mit Hilfe des Walk-In Wizards ausstellen. Der User muss dabei die PIN und die Revokationspassphrase selber setzen	5.2.3.9
8.	Antragsteller über seine Pflichten gemäss «*Benutzervereinbarung und Nutzungsbedingungen Klasse B*» und «*Guidelines für Zertifikate der Klasse B*» orientieren und mit dem Kunden besprechen.	5.2.3.10
9.	«*Bestätigung für Erhalt und Umgang mit der Smartcard*» an unterschriebene Dokumente heften (optional), eine Kopie der «*Benutzervereinbarung*» unterschreiben lassen.	5.2.3.10
10.	Stimmt die Unterschrift auf den «*Benutzervereinbarung und Nutzungsbedingungen Klasse B*» mit derjenigen im (Reise-)Dokument überein?	
11.	Die Smartcard, das Reisedokument, ggf. weitere Dokumente und die nicht unterschriebenen «*Benutzervereinbarung und Nutzungsbedingungen Klasse B* » und «*Guidelines für der Zertifikate der Klasse B*» dem Antragsteller aushändigen	5.2.3.11
12.	Journal führen	5.2.3.12
13.	Die im Schritt 5. erstellte Datei des (Reise)Dokumenten inkl. allfällige zu deren Versand benutzte Mails löschen	5.2.3.13
14.	Das unterschriebene Exemplar der «*Benutzervereinbarung und Nutzungsbedingungen Klasse B*» - und, sofern der Antrag auf Papier vorliegt, – im Kundendossier, oder im elektronischen Archiv, zusammen mit den Fingerprints der Zertifikate ablegen.	5.2.3.14

Checkliste: Ausstellen von Klasse B Zertifikaten

Prozess Klasse B „Ausstellen mit RIO“, Check-Punkte LRAO (RR Kapitel 5.2.4)

V2.1, 20.09.2019

Beschreibung	**Referenz RR 1**
Antragserstellung	
Antragsteller/HR/Linie füllt den 1. Teil des Formulars aus: «*Klasse B: RIO Antrag zur Ausstellung von Klasse B Zertifikaten*» und informiert den RIO (und den Kunden) über eine neue Ausstellung https://www.bit.admin.ch/adminpki/00240/00367/00820/00822/index.html?lang=de	5.2.4.1
Identifikation Antragsteller und Weiterleiten Antrag durch RIO	
Der RIO geht anhand der Checkliste «*Checkliste RIO*» vor, dokumentiert die einzelnen Schritte darauf und leitet die Unterlagen an den LRA-Officer weiter. Dabei ist wichtig, dass die Seriennummer der Smartcard auf das Antragsformular aufgeschrieben wird und die Kopien/Scans vollständig und lesbar sind	5.2.4.2
Genehmigung Ausstellung Zertifikate durch LRA-Officer	
Überprüfung des Antrag:	5.2.4.3
a) Sind alle benötigten Unterlagen vorhanden (Antragsformular (mit Seriennummer der Karte), Checkliste, Unterschriebene Kopie «*Benutzervereinbarung und Nutzungsbedingungen Klasse B*», ggf. weitere benötigte Kopien gemäss Ausnahmeregelung) **Bei elektronischer Übermittlung**: Wurden alle Dokumente verschlüsselt übermittelt?	
b) Ist die Antragsbestätigung von einem autorisierten RIO unterzeichnet? **Bei elektronischer Übermittlung**: Ist die elektronische Unterschrift des RIO gültig?	
c) Kopie des (Reise-)Dokuments und ggf. weiterer Dokumente einscannen und abspeichern **Bei elektronischer Übermittlung**: Abspeichern der signierten Antragsbestätigung	
d) Abgleich Daten im System mit Angaben auf dem Antragsformular: Ist der User richtig im AdminDir erfasst?	
Ausstellung der Zertifikate via Walk-In-Wizard: «RIO»-Policy benutzen	
e) Scans einfügen. Der frei gegebene Antrag wird in einem Ticket angelegt und an die CA zur Zertifizierung übermittelt. Die Ticketnummer wird in einem sogenannten Unseal-Dokument (pdf-Format) festgehalten.	

[1] Swiss Government PKI_B_Registrierrichtlinien

f) Das Unseal-Dokument mit dem Aktivierungscode an die private Adresse des Kunden schicken (alternativ dazu können die Aktivierungsdaten dem RIO per verschlüsselter und signierter Mail zugestellt werden)	
g) Ablage der Dokumente unter a) (Papierform) im Kundendossier und, bei **elektronischer Übermittlung**, im elektronischen Kundendossier	
h) Nachführen Journal	5.2.4.3, 3.7
Abholen Zertifikat durch Antragsteller	
1) Token-Unseal Wizard öffnen (beim RIO oder einem Berufskollegen, der 2 Kartenleser besitzt)	
2) Karte in Lesegerät einfügen (diese wird durch das System automatisch erkannt)	
3) Wenn vom Wizard gefragt, den Aktivierungscode eingeben → Die Zertifikate werden gespeichert	
4) Danach die PIN und die Revokationspassphrase eingeben → Die Karte ist einsatzbereit	

Checkliste: Revokation von Klasse B Zertifikaten

Prozess Klasse B „Zertifikat revozieren“ (RR Kapitel 5.3)

V2.1, 20.09.2019

Nr.	Beschreibung	Referenz RR[1]
Antrag prüfen		
1.	Antrag plausibilisieren	5.3.4.1
2.	Falls nicht schon durch den Antragsteller erledigt und nötig, Revokationsformular ausfüllen	5.3.4.2
Zertifikat revozieren		
3.	Suche des entsprechenden Zertifikats im «Revoke Wizard»	5.3.4.3
4.	Identifizierung des Zertifikatsinhabers anhand der gespeicherten Identitätsdokumente	
5.	Revozieren der Zertifikate	
Abschluss		
6.	Revokationsformular ablegen (falls vorhanden aufgrund gewählter Prozess/ Applikation)	5.3.4.4
7.	Journal nachführen	5.3.4.4, 3.7

1) Swiss Government PKI_B_Registrierrichtlinien

Checkliste RIO:

V2.1, 20.09.2019

Nr.	Beschreibung der Aufgabe	Resultat (OK / NOK)	**Datum**
1	Antrag prüfen und plausibilisieren (Diese Person ist berechtigt, Zertifikate der Swiss Government PKI Klasse B zu beziehen und ist im Admin-Directory des Bundes erfasst)		
2	Identität überprüfen durch Vergleich des gültigen Reisedokumentes mit dem Antragsformular (zulässig nur gültige Identitätskarte oder gültiger Pass).		
	Name: _____		
	Art des Reisedokumentes gemäss Antragsformular (nur gültige Identitätskarte, gültiger Pass oder Ausnahme gemäss Liste in Registrierrichtlinien) Seriennummer des Dokumentes: _____ Gültigkeit des Reisedokumentes: _____	☐ ID ☐ Pass ☐ andere _____	
	Gesicht des Antragsstellers mit Gesichtsbild im Reisedokument vergleichen		
3	Preregistrierte (oder prestaged) Smartcard überreichen. Benutzer darauf aufmerksam machen, dass er die Karte ab diesem Moment immer unter seiner alleinigen Kontrolle behalten muss. Seriennummer der Smartcard: _____		
4	Teil 2 des Antragsformulars ausfüllen, inkl. Unterschriften		
5	«*Benutzervereinbarung und Nutzungsbedingungen Klasse B*» und «*Guidelines zu Klasse B Zertifikaten der Swiss Government PKI*» dem Kunden erklären		
6	«*Benutzervereinbarung und Nutzungsbedingungen Klasse B*» und «*Guidelines zu Klasse B Zertifikaten der Swiss Government PKI*» dem Kunden aushändigen, eine Kopie der Benutzervereinbarung unterschreiben lassen und wieder einziehen.		
7	Ausweisdokument auf Rückseite des Antrages Kopieren (ID beidseitig!). Alle Dokumente kopieren.		
8	Alle Seiten mit Kopien von Dokumenten unterzeichnen und vom Kunden gegenzeichnen lassen		
9	Checkliste unterschreiben		
10	Versand der Dokumente an den LRAO «*Benutzervereinbarung und Nutzungsrichtlinien Klasse B*», Ausgefülltes Antragsformular, diese Checkliste RIO) Bei elektronischer Übermittlung: Die signierten Dokumente verschlüsselt, per E-Mail an den zuständigen LRA-Officer schicken.		

RIO Name/ Vorname	Organisationseinheit:	Ort, Datum:

Unterschrift RIO: _____

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Betrieb
Betrieb Front End Services
PKI

Anhang B: Formulare für Klasse B Zertifikate

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Betrieb
Betrieb Front End Services
PKI

NICHT KLASSIFIZIERT

Klasse B: Antrag für persönliche Zertifikate der Swiss Government PKI Klasse B

Fortgeschrittene Zertifikate

V2.3, 20.09.2019

Dieses Formular dient zur Beantragung eines Klasse B Zertifikats der Swiss Government PKI. Dabei wird unterschieden zwischen den sogenannten Standardzertifikaten (mit Authentisierung, Signatur und Verschlüsselung) und den Funktionszertifikaten für Test- und Administratoren Accounts (nur Authentisierung für A-Accounts)

Zur Ihrer Identifikation bei Ihrer Registrierstelle benötigen Sie eine gültige Identitätskarte oder einen gültigen Pass.

**Diese Felder sind zwingend auszufüllen*

Name Vorname(n)*:	
Ausweispapier Nr.*:	Gültig bis*:
Organisationseinheit*:	
Zertifikatstyp*: Standard Klasse B Zertifikat	
E-Mail[1*]:	
Geschäftsadresse*:	
Heimatort:	Geburtsdatum:
Smartcard-Nr:	

Ort / Datum*:

_____

Unterschrift*:

_____

NICHT KLASSIFIZIERT

Klasse B: Ergänzendes Formular für Antragsteller mit Ausweis F

V1.1, 20.09.2019

Dieses Formular ist Bestandteil des Antrags zur Beantragung eines Klasse B Zertifikats der Swiss Government PKI, im Falle, dass der Antragsteller über keine gültigen Reisedokumente, sondern lediglich einen 'Ausweis F'. besitzt.

Dieses Formular muss zusammen mit einem vollständig ausgefüllten und gültig unterschriebenen Antrag für Zertifikate der Swiss Government PKI Klasse B eingereicht werden.

Das Formular muss vom zuständigen ISBO unterschrieben werden. Mit seiner Unterschrift bestätigt der ISBO, dass er davon Kenntnis hat, dass die Identität des Antragstellers auf der Basis eines 'Ausweis F' nicht eindeutig festgestellt werden kann und die SG-PKI in der Folge nicht dafür haftbar gemacht werden kann, wenn die wahre Identität des Antragstellers nicht gesichert festgestellt werden kann.

Name:		Vorname:
Ausweispapier Nr.:		
Organisationseinheit:		
Zertifikatstyp:	Standardzertifikat	☐
	Funktionszertifikat:	
	Administrator	☐
	Test	☐
E-Mail[1]:		
Geschäftsadresse:		
Heimatort:		Geburtsdatum:
☐ Interner Mitarbeiter	☐ Externer Mitarbeiter	

[1] Bei ‚Funktionszertifikat Administrator' Maildresse des Account-Inhabers.

ISBO: **Antragsteller:**

Name, Vorname: _____ S/N des Ausweises: _____
(in Blockbuchstaben)

Ort / Datum: _____ Ort/ Datum: _____

Unterschrift: _____ Unterschrift: _____

Klasse B: RIO Antrag zur Ausstellung von Klasse B Zertifikaten

Formular zur Übermittlung der Antragstellerinformationen an den LRAO

V1.1 20.09.2019

1 Angaben zum Antragsteller (vom Antragsteller auszufüllen und dem RIO zuzustellen)

Der Antragsteller bestellt hiermit eine vorbereitete Smartcard zur Ausstellung von Klasse B Zertifikaten der Swiss Government PKI:

Name, Vorname:

Departement/ Kanton/ Amt:

E-Mailadresse:

Telefonnummer:

Ort, Datum: Unterschrift: _____

2 Identifikation und Kartenzuteilung (von RIO zusammen mit dem Antragsteller zu komplettieren und dem LRAO zuzustellen)

Der Antragsteller erhält vom RIO eine vorbereitete Smartcard, die nach Antragsfreigabe vom LRA-Officer mit der ihm mitgeteilten/zugesendeten S-PIN entsiegelt werden kann.

Der RIO teilt dem Antragsteller die Smartcard mit
folgenden Erkennungsnummern zu: **Seriennummer** (zwingend): _____
Kartennummer oder LegicID (optional): _____

Der RIO und der Antragsteller bestätigen mit der Unterschrift, dass eine persönliche Begegnung, die Übergabe der Smartcard mit oben genannter Seriennummer und die Identifikation anhand eines gültigen Reisedokumentes stattgefunden haben:

RIO:	**Antragsteller:**
Name, Vorname: _____ (in Blockbuchstaben)	S/N des Ausweises: _____
Ort / Datum: _____	Ort/ Datum: _____
Unterschrift: _____	Unterschrift: _____

3 Benutzervereinbarung und Nutzungsbedingungen

Der RIO stellt sicher, dass der Antragsteller den Inhalt der *Benutzervereinbarung und Nutzungsbedingungen* verstanden und eine Kopie davon erhalten hat. Eine zweite Kopie muss vom Antragsteller unterschrieben und vom RIO dem LRA-Officer, zusammen mit diesem ausgefüllten Dokument, inklusive den Kopien der Reisedokumente, zugestellt werden.

4 Kopie des Reisedokumentes

Eine Kopie des gültigen Reisedokumentes des Antragstellers muss auf der Rückseite dieses Dokumentes erstellt werden. Identitätskarten müssen zwingend beidseitig kopiert werden. Passkopien bitte immer mit den Seiten des Fotos, der Unterschrift und des Gültigkeitsdatums. Rückseite, sowie zusätzlich benötigte Seiten müssen von beiden Parteien mit Ort, Datum und Unterschrift versehen werden. Die Rückseite dieses Dokumentes dient dazu als Vorlage/Unterlage für die Kopien.

[Reise-/ Identitätsdokumente zum Kopieren hier auflegen]

RIO:

Ort / Datum: _____

Unterschrift: _____

Antragsteller:

Ort/ Datum: _____

Unterschrift: _____

NICHT KLASSIFIZIERT

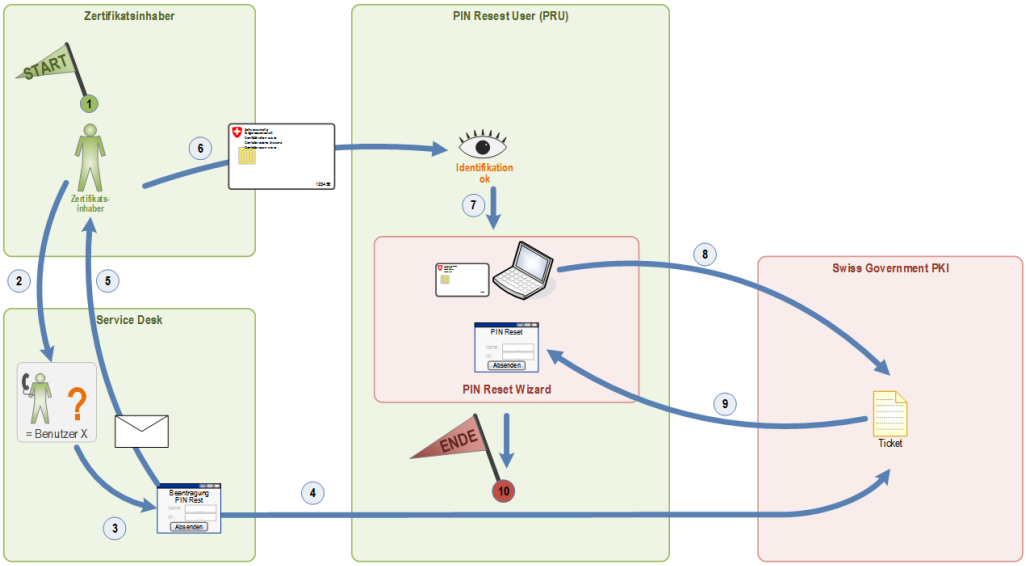
Antragsformular für PIN Reset für Superuser/ Servicedesks

Berechtigungen zur Online-Ticketerstellung

V1.1 25.10.2019

Dieses Formular dient zur Berechtigungsfreigabe zur Online Ticketerstellung für das PIN Reset von User Smartcards. Dies sollte nur für Service Desk Mitarbeiter oder Superuser ausgefüllt werden. Die Berechtigungen zur Ticketerstellung sind nur der 1. Teil für den PIN Reset von prestaged Smartcards. Der betroffene User muss in einem 2. Schritt zu einem Mitarbeiter und die Smartcard am Client des Mitarbeiters freischalten, bzw. den neuen PIN für seine Karte eingeben. (Siehe dazu auch das Merkblatt für PRUs unter):
https://www.bit.admin.ch/adminpki/00240/06271/06273/06281/index.html?lang=de

Prozess zum PIN-Reset:



Angaben zur antragstellenden Person:

Name, Vorname, Suffix:

Departement/ Kanton:

Amt:

Funktion:

E-Mailadresse:

Telefonnummer:

S/N Authentisierungszertifikat

Datum:

Digitale Signatur: _____

Bewilligung (bitte mit Timestamp):

Digitale Signatur Organisationsverantw.:

_____

Digitale Signatur Amtsvorsteher:

_____

Digitale Signatur SG-PKI SecOff:

_____

Berechtigungsentzug:

Bitte entziehen Sie der oben genannten Person (als *antragstellende Person* bezeichnet) die Berechtigungen zur Ticketerstellung von PIN Reset Anfragen ☐

NICHT KLASSIFIZIERT

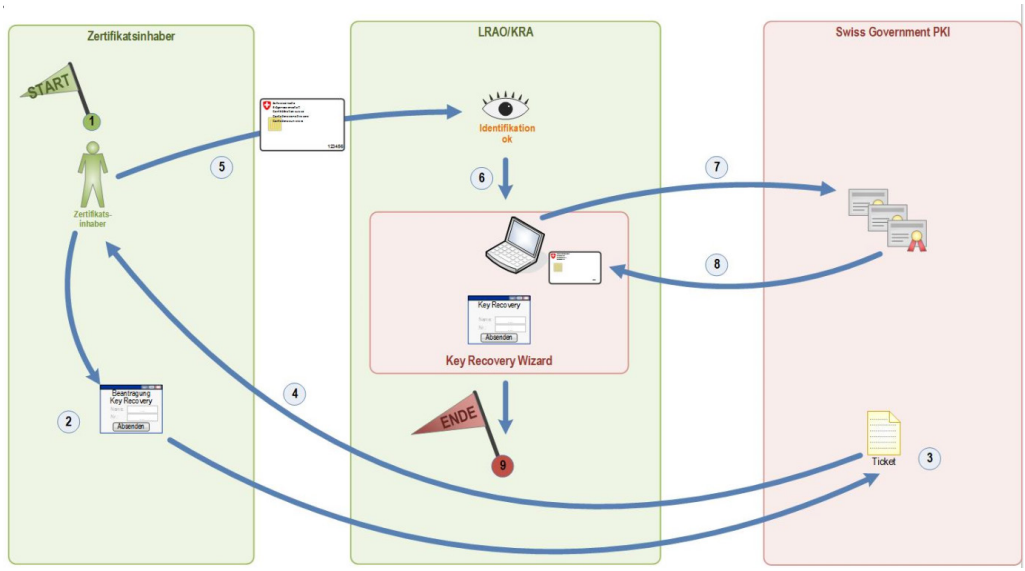
Antragsformular für ein Key Recovery Agent (KRA)

Berechtigungen für den Key Recovery Wizard

V1.1 25.10.2019

Dieses Formular dient dazu einen RIO, einen Mitarbeiter einer IT-Supportorganisation oder einen Super-User als Key Recovery Agent (KRA) zu berechtigen. Die Berechtigungen zum KRA sind für den 2. Teil des Prozesses «Key Recovery» notwendig. Der Benutzer, der ein Key Recovery benötigt, ruft in seinem Browser die Seite zum «Key Recovery» auf (https://keyrecovery.pki.admin.ch/KeyRecoveryRequest/) und erstellt dort ein **eTicket** im zentralen PKI System. Nachdem der Zertifikatsinhaber dem KRA sein eTicket angegeben hat, startet der KRA den «Key Recovery Wizard» und gibt die eTicket-Nummer ein. Der Wizard zeigt daraufhin alle für diesen Zertifikatsinhaber jemals ausgestellten Verschlüsselungs-Zertifikate an. Der Zertifikatsinhaber gibt dem KRA diejenigen Schlüssel an, die er wiederherstellen möchte. Nach Eingabe der persönlichen PIN, schreibt der Wizard die gewählten Encryption Keys auf die Smartcard des Zertifikatinhabers.

Key Recovery Prozess:



Angaben zur antragstellenden Person:

Name, Vorname, Suffix:

Departement/ Kanton:

Amt:

Funktion:

E-Mailadresse:

Telefonnummer:

S/N Authentisierungszertifikat:

Datum:

Digitale Signatur: _____

Bewilligung (bitte mit Timestamp):

Digitale Signatur Organisationsverantw.:

_____

Digitale Signatur Amtsvorsteher:

_____

Digitale Signatur SG-PKI SecOff:

_____

Berechtigungsentzug:

Bitte entziehen Sie der oben genannten Person (als *antragstellende Person* bezeichnet) die Berechtigungen als Key Recovery Agent (KRA) ☐

NICHT KLASSIFIZIERT

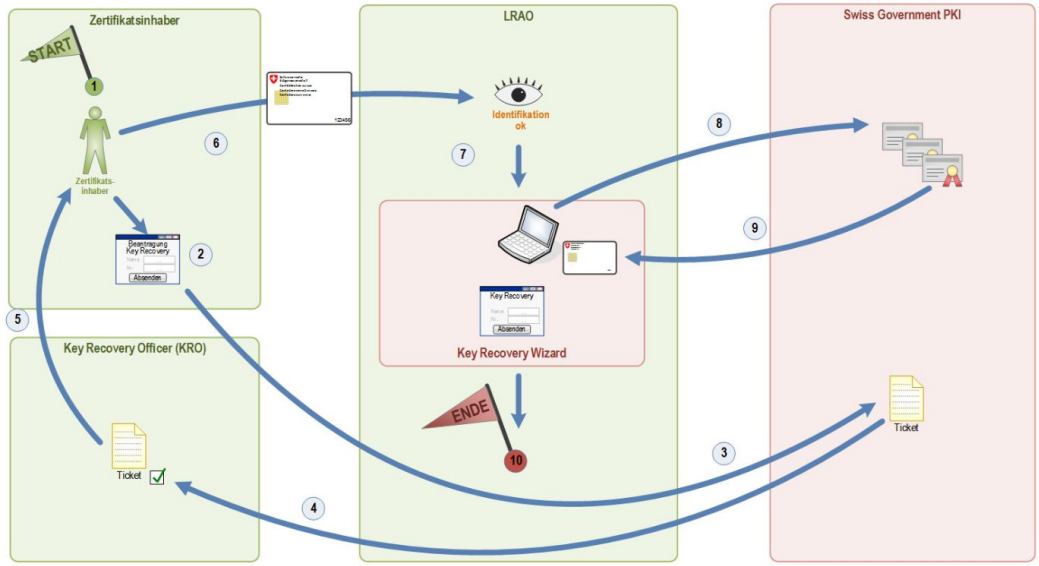
Antragsformular für ein Key Recovery Officer (KRO)

Berechtigungen für die Freigabe von Key Recovery Anträgen

V1.1 25.10.2019

Dieses Formular dient dazu einen RIO, einen Mitarbeiter einer IT-Supportorganisation oder einen Super-User als Key Recovery Officer (KRO) zu berechtigen. Die Berechtigungen zum KRO sind für den 2. Teil des Prozesses «Key Recovery mit KRO» notwendig. Der Benutzer, der ein Key Recovery benötigt, ruft in seinem Browser die Seite zum «Key Recovery» auf (https://keyrecovery.pki.admin.ch/KeyRecoveryRequest/) und erstellt dort ein **eTicket** im zentralen PKI System. Der KRO hat danach die Aufgabe den Antrag zu prüfen und ggf. freizugeben, bevor der Zertifikatsinhaber mit seinem **eTicket** zum LRAO oder zum KRA geht. Danach startet der LRAO/KRA den «Key Recovery Wizard» und gibt die **eTicket**-Nummer ein. Der Wizard zeigt daraufhin alle für diesen Zertifikatsinhaber jemals ausgestellten Verschlüsselungs-Zertifikate an. Der Zertifikatsinhaber gibt diejenigen Schlüssel an, die er wiederherstellen möchte. Nach Eingabe der persönlichen PIN, schreibt der Wizard die gewählten Encryption Keys auf die Smartcard des Zertifikatinhabers.

Key Recovery Prozess mit KRO:



Angaben zur antragstellenden Person:

Name, Vorname, Suffix:

Departement/ Kanton:

Amt:

Funktion:

E-Mailadresse:

Telefonnummer:

S/N Authentisierungszertifikat:

Datum:

Digitale Signatur: _____

Bewilligung (bitte mit Timestamp):

Digitale Signatur Organisationsverantw.:

_____

Digitale Signatur Amtsvorsteher:

_____

Digitale Signatur SG-PKI SecOff:

_____

Berechtigungsentzug:

Bitte entziehen Sie der oben genannten Person (als *antragstellende Person* bezeichnet) die Berechtigungen als Key Recovery Officer (KRO) ☐

NICHT KLASSIFIZIERT

Klasse B: Revokationsantrag für Zertifikate der Klasse B
Swiss Government PKI

V2.4, 20.09.2019

Antragsteller:			
☐ **Zertifikatsinhaber**	☐ **Vorgesetzter**	☐ **HR**	☐ **ISBO**
☐ **PKI Verantwortlicher**	☐ **LRA-Officer**	☐ **PKI Security Officer**	
Name:		Vorname:	
Organisationseinheit:			

Zertifikatsinhaber (*nur ausfüllen, wenn Zertifikatsinhaber nicht der Antragsteller ist):		
Name*:	Vorname*:	Suffix*:
Organisationseinheit*:		
Zertifikatstyp: ☐ Standardzertifikat ☐ Funktionszertifikat Administrator ☐ Funktionszertifikat Test		
☐ Interner Mitarbeiter ☐ Externer Mitarbeiter ☐ Revokationsliste		

Gründe für die Revokation:	
☐ Smartcard verloren	☐ Smartcard defekt
☐ Verdacht auf Kompromittierung	☐ Austritt
☐ Falschausstellung	☐ Missbrauchsverdacht
☐ andere	

Revoziert am:	
Ausführender LRA-Officer (Name, Vorname):	Unterschrift: _____

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

Klasse B: LRAO Journal der Swiss Government PKI

V2.1, 20.09.2019

Fortlaufende #*	Datum*	Kunde*	Tätigkeit*: SZ: Standardzertifikat, FZA: Adminzertifikat, FZT: Testzertifikat A: Ausgestellt, R: Revoziert, K: KeyRecovery	Seriennummer Smart Card	SmartCard eingezogen JA / NEIN*	Visum LRAO*

*(*Diese Felder zwingend ausfüllen)*

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

NICHT KLASSIFIZIERT

Klasse B: Antrag LRA-Officer

V4.5, 20.09.2019

☐ **Neuer LRAO** → Abs. A und B
☐ **Erneuerung LRAO** → Abs. A und B
☐ **Mutation Berechtigungen** → Abs. B
☐ **Revokation LRAO-Zertifikat** → Abs. C

Abschnitt A) Folgende Anforderungen müssen erfüllt sein, bevor der Antrag bearbeitet werden kann:

☐ Schulung besucht, Test bestanden: Kopie des Attests und Bestätigung des bestandenen Tests beigelegt

☐ AdminDir Eintrag in Gelben Seiten vorhanden

☐ LRA-Officer Informationen unter → *Abschnitt B* korrekt und vollständig ausgefüllt

Abschnitt B) Angaben zum LRA-Officer und zu den Ausstellberechtigungen:

Ausstellung Klasse B für BV:
☐ E-Mail-Adresse endet auf admin.ch (Prestaged/ Enhanced CA02)
☐ E-Mail-Adresse endet *nicht* auf admin.ch (Prestaged/ Enhanced CA01)

Ausstellung Klasse B für Extern (Non-BV):
☐ Prestaged (Enhanced CA01)
☐ *Non*-prestaged/ Standard (Enhanced CA01)

Angaben zum LRA Officer (Müssen mit dem Eintrag im AdminDir übereinstimmen; *=Pflichtfelder!)			
Nachname*:		Vorname*:	
Suffix*:		Departement*:	
Amt*:		Tel.*:	
E-Mail*:			
Adresse (Strasse, PLZ, Ort)*:			
Ausstellberechtigungen für (Dep./Amt)*:		☐ neu ☐ entziehen	
Seriennummer Auth. Zert. pers. Klasse B			
Berechtigungen für **Admin-Account** Zertifikate (A-Accounts) (auf Stufe Dep.)	☐ neu ☐ entziehen für Departement: EFD		

Abschnitt C) Folgende Anforderungen müssen erfüllt sein, bevor der Antrag bearbeitet werden kann:

Ausführungsdatum Revokation:

Gibt es einen nachfolgenden LRA-Officer? ☐ Nein ☐ Ja, Name:

☐ LRA-Officer Informationen unter → ***Abschnitt B*** korrekt und vollständig ausgefüllt

Der noch aktive LRA-Officer verpflichtet sich, seinem Nachfolger die Kundendossiers und das Journal zu übergeben. Er ist gebeten seine LRA-Officer Smartcard zurückzusenden.

Allgemeine Nutzungsbedingungen für den LRAO

Vertraulichkeitserklärung

Der Antragsteller verpflichtet sich mit seiner Unterschrift, die Smartcard und das zugehörige Passwort vertraulich zu behandeln und die im Rahmen seiner Arbeit als LRA-Officer erhaltenen, personenbezogenen Informationen nicht an Dritte und intern nur an die Mitarbeiter weiterzugeben, welche zur Erfüllung ihrer Aufgaben unbedingt unmittelbaren Zugriff auf diese Informationen benötigen. Mitarbeiter mit LRAO-Funktion sind, soweit dies nicht bereits in ihrem Arbeitsvertrag festgelegt ist, zur Geheimhaltung zu verpflichten. Von den zu bearbeitenden Daten und Informationen sind weder vollständige noch auszugsweise Kopien anzufertigen.

Der LRA-Officer ist verpflichtet, bei Amtsaufgabe das Zertifikat revozieren zu lassen.
Die vorliegende Erklärung ist auch nach der Amtsaufgabe als LRA-Officer und nach Austritt derselben Person wirksam.

Es gelten für das LRA-Officer Zertifikat die «Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI» sowie die «Guidelines zu LRAO-Zertifikaten der Swiss Government PKI» (folgende Seiten) und die «Swiss Government PKI Registrierrichtlinien Klasse B». Mit seiner Unterschrift bestätigt der angehende LRA-Officer, gemäss der geltenden CP/CPS der SG-Root CA I alle in diesen Dokumenten vorhandenen Vorschriften und Verfahren, gelesen, verstanden und akzeptiert zu haben und vollständig einzuhalten. Der angehende LRA-Officer bestätigt mit seiner Unterschrift weiter mit der Ausstellung einer persönlichen LRA-Officer Smartcard zur Ausübung der LRA-Officer Tätigkeit einverstanden zu sein.

Antragsteller (Vorname, Nachname)	**Datum:** **Unterschrift/ Signatur:**

Vertrauenswürdigkeitsprüfung

Die Behörde ergreift die im gesetzlichen Rahmen erlaubten sowie ihr zumutbaren Massnahmen, um die Vertrauenswürdigkeit und Integrität des Kandidaten/ der Kandidatin zu überprüfen. Die SG-PKI empfiehlt der Behörde die Durchführung folgender Massnahmen:

- Personensicherheitsprüfung gemäss Artikel 10 der Verordnung über die Personensicherheitsprüfungen (PSPV, SR 120.4) bei der Fachstelle PSP des VBS.

  und/oder

- Vornahme eigener Massnahmen zur Überprüfung der Vertrauenswürdigkeit, wie beispielsweise:
  - Kontrolle der Identität des Kandidaten/ der Kandidatin (Pass oder Identitätskarte);
  - Überprüfung von geschäftlichen und/oder privaten Referenzen des Kandidaten/ der Kandidatin;
  - Verifizierung der Vollständigkeit und Schlüssigkeit des Lebenslaufs des Kandidaten/ der Kandidatin;
  - Kontrolle der referenzierten akademischen und beruflichen Qualifikationen;
  - Überprüfung von Betreibungs- und Strafregisterauszügen.

Bestätigung

Die unterschriftsberechtigte Person der Behörde bestätigt gegenüber der SG-PKI, die Vertrauenswürdigkeit des Kandidaten/ der Kandidatin gemäss obenstehender Empfehlung oder auf vergleichbare Art und Weise überprüft zu haben. Sie stuft den Kandidaten/ die Kandidatin als vertrauenswürdig und integer ein und bestätigt zudem, dass er/ sie über die notwendigen Kompetenzen zur Ausübung der sicherheitsempfindlichen Tätigkeit als LRA-Officer verfügt.

Unterschriften

Sofern Berechtigungspfade mehrerer Ämter beantragt werden, müssen die Unterschriftsberechtigten von jedem beantragten Amt unterschreiben. Benutzen Sie dazu das zusätzliche Listenformular unter den Klasse B-Formularen auf www.pki.admin.ch.

Unterschriftsberechtigt sind:

- auf **Amtsebene**: ISBOs, PKI-Verantwortliche der Kantone/ Polizeikorps, Sicherheitsbeauftragte von kantonalen Ämtern, sowie das SG-PKI Managementboard
- auf **Departements Ebene**: ISBDs, PKI-Verantwortliche der Kantone/ KAPOs sowie Sicherheitsbeauftragte der Kantone und Kantonspolizei

Unterschriftsberechtigte(r) Amt (Vorname, Nachname/ Funktion)	**Datum:** **Unterschrift/ Signatur:**

Für die Zuteilung von Berechtigungen für A-Accounts (nur BV-intern) ist die Unterschrift des **ISBD** einzuholen (*Berechtigung gilt immer für das gesamte Departement!*). Sofern die Berechtigungen mehrerer Departemente beantragt werden, muss das nachstehende Unterschriftsfeld von den ISBDs aller beantragten Departemente unterschrieben werden. Benutzen Sie dazu das zusätzliche Listenformular unter den Klasse B-Formularen auf www.pki.admin.ch.

Unterschriftsberechtigte(r) Departement (Vorname, Nachname) Dep/ Kt.	**Datum:** **Unterschrift/ Signatur:**

NICHT KLASSIFIZIERT

Guidelines zum LRAO-Zertifikat der Swiss Government PKI

Erläuterungen zum Bezug und Einsatz vom LRAO-Zertifikat der Klassen A und B der Swiss Government PKI

V1.0, 28.08.2018

1 Zweck des LRAO-Zertifikats

Zweck

Im Rahmen des Marktmodells «SD005 - Marktmodell Standarddienst: Identitäts- und Zugangsverwaltung (IAM)» werden die Zertifikate der Klasse A und B definiert. Die LRA-Officer (Local Registration Agency Officer) sind für die Ausstellung der Klasse A und B zuständig. Das LRAO-Zertifikat kann für folgende Zwecke verwendet werden:

- Ausstellung Revokation und Pflege von Klasse A und/oder B Zertifikate der Swiss Government PKI.

Durch erweiterte Prüf- und Sicherheitsmechanismen während des Ausstellungsprozesses der Klassen A und B Zertifikate wird die Identität des Zertifikatsinhabers auf einer hohen Sicherheitsstufe festgestellt. Die Ausgabe von Klasse A und B Zertifikaten erfolgt immer persönlich und nur nach Identifizierung des Inhabers mittels eines gültigen, für die Einreise in die Schweiz zugelassenen Reisedokumentes.

Ausgeschlossener Zweck

Das LRAO-Zertifikat erfüllt ausschliesslich die oben genannten Zwecke und gibt keinerlei weitere Aufschlüsse, Versicherungen oder Garantien. Insbesondere garantiert das LRAO-Zertifikat nicht, dass der Inhaber im Umgang mit dem Zertifikat korrekt und legal handelt.
Des Weiteren garantiert das LRAO-Zertifikat nicht, dass:

- Der im Zertifikat genannte Inhaber aktiv in die Geschäftstätigkeiten involviert ist;
- Der im Zertifikat genannte Inhaber sich an die geltenden gesetzlichen Vorschriften hält;
- Der im Zertifikat genannte Inhaber im Geschäftsumfeld seriös handelt;

2 Qualität des LRAO-Zertifikats

Die SG-PKI hält sich an die in den Registrierrichtlinien vorgegebenen Prozesse, welche die notwendigen und zumutbaren Schritte zur Bestätigung folgender Tatsachen zum Zeitpunkt der Erstausstellung eines LRAO-Zertifikates festlegen:

- **Rechtlich gültige Existenz:** Der im LRAO-Zertifikat genannte Inhaber existiert als natürliche Person und verfügt über einen persönlichen Eintrag im AdminDirectory.
- **Identität:** Der Name des im LRAO-Zertifikats genannten Inhabers stimmt mit dem Namen im AdminDirectory und im aktuell gültigen Reisedokument überein.
- **Autorisierung:** Der im LRAO-Zertifikat genannte Inhaber ist zum Bezug des Zertifikates durch die unterschriftsberechtigte Person seines Amtes autorisiert worden.
- **Richtigkeit der Daten:** Alle im Zertifikat enthaltenen Daten und Informationen sind korrekt.
- **Vereinbarung/ Nutzungsbedingungen:** Der im LRAO-Zertifikat genannte Inhaber hat die in der «*Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI*» beschriebenen Rechte und Pflichten gelesen, verstanden und mit der Unterschrift auf dem Antragsformular für das LRA-Officer Zertifikat der SG-PKI akzeptiert. Seine Fragen diesbezüglich wurden von der SG-PKI verständlich beantwortet.
- **Status:** Die SG-PKI stellt den Status des Zertifikats sowie Informationen über dessen Gültigkeit/ Revokation online abrufbar zur Verfügung.

- **Revokation:** Die SG-PKI kann das LRAO-Zertifikat gegebenenfalls aus den in der/n «*Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI*» genannten Gründen unverzüglich revozieren.

3 Policies

Alle geltenden gesetzlichen Vorgaben, Policies (inkl. der CP/CPS der SG Root CA I) und Registrierrichtlinien von Zertifikaten der SG-PKI, sowie die «*Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI*» und diese Guidelines sind im Internet auf der Website der SG-PKI publiziert: www.pki.admin.ch.

Der angehende LRAO verpflichtet sich mit der Unterschrift auf dem Formular: «*Klasse B: Antrag LRAO*», sich an die geltenden Richtlinien und Gesetzgebungen zu halten und seine Arbeiten danach auszuführen. Insbesondere sind dies:

- Die CP/CPS der SG Root CA I: («*Certificate Policy and Certification Practice Statement of the Swiss Government Root CA I*») (insbesondere zu erwähnen sind die in Kap. 5.3.1 und 5.5.2 beschriebenen Verpflichtungen)
- Die «*Swiss Government PKI Registrierrichtlinien Klasse B*»
- Die «*Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI*»
- Die «*Guidelines zum LRAO-Zertifikat der Swiss Government PKI*» (Dieses Dokument).

Inhalt

Das LRAO-Zertifikat der SG-PKI enthält Informationen betreffend:

- Herausgeber und ausstellender CA
- die Root CA der ausstellenden CA
- die angewandte Policy
- Ausstell- und Ablaufdatum des Zertifikates
- Seriennummer des Zertifikates
- Verwendungszweck des Zertifikates
- der CRL und dem OCSP
- die Auditoren der CA
- den Inhaber des Zertifikates gemäss Eintrag im AdminDirectory zum Zeitpunkt der Erstausstellung:
    1) Common Name des Inhabers
    2) E-Mail-Adresse
    3) UPN

Gültigkeit

Das LRAO-Zertifikat der SG-PKI ist max. 3 Jahre gültig. Nach Ablauf der Gültigkeit muss das LRAO-Zertifikat durch den LRAO-Officer neu bei der SG-PKI, analog dem Erstausstellungsprozess, beantragt und von der SG-PKI ausgestellt werden.

4 Bezug des LRAO-Zertifikats

Bezug

Für den Bezug des LRAO-Zertifikats der SG-PKI sind folgende Dokumente bzw. Registrierungen nötig:

- Ein gültiges, für die Einreise in die Schweiz zugelassenes Reisedokument (ID/ Pass), ausgestellt auf den Antragsteller. Die Identität wird während der obligatorischen LRAO-Schulung vom Kursleiter überprüft
- Ein persönlicher Eintrag im AdminDirectory, mit Nachname(n), Vorname(n) (gemäss Reisedokument), gültiger E-Mailadresse und optional einem UPN Eintrag (User Principal Name)
- Ein Attest, welches den erfolgreichen Besuch der obligatorischen LRA-Officer Schulung und die bestandene Prüfung bezeugt
- Ein ausgefülltes und (elektronisch) signiertes Antragsformular für LRA-Officer Zertifikate der Swiss Government PKI, in welchem
    1) der angehende LRAO
        - eine Vertraulichkeitserklärung
        - die Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI
        - diese Guidelines

mit seiner Unterschrift als akzeptiert erklärt und die LRAO-Smartcard bestellt.

2) die Unterschriftsberechtigte Person der anstellenden Behörde die Vertrauenswürdigkeit des angehenden LRA-Officer, gemäss den Vorgaben im Antragsformular unter dem Kapitel «Vertrauenswürdigkeitsprüfung», mit seiner Unterschrift bestätigt.

Identifizierung

Um die antragstellende Person zu identifizieren, wird das Reisedokument auf Gültigkeit, Richtigkeit und Echtheit während der LRAO-Schulung überprüft. Die SG-PKI Kursleiter sind zudem verpflichtet, das Bild des Dokumentes mit der vor Ihnen stehenden und am Kurs teilnehmende Person zu validieren. Ebenso wird der Antrag vor der Ausstellung eines persönlichen Zertifikates von der SG-PKI plausibilisiert (Person arbeitet tatsächlich in der im AdminDirectory Eintrag zugewiesenen Organisationseinheit und benötigt das Zertifikat im geschäftlichen Alltag; der Antragsteller ist berechtigt ein Zertifikat zu beantragen).

Verbindlichkeit

Der Antrag muss durch die zuständigen Stellen freigegeben sein. Diese Guidelines und das Dokument «*Benutzervereinbarung und Nutzungsbedingungen für LRAO der SG-PKI*» müssen vom Antragsteller verstanden und im Antragsformular für LRAO mit der (digitalen) Unterschrift akzeptiert worden sein.

5 Schutz des privaten Schlüssels und des Zertifikates

Übertragbarkeit

Das LRAO-Zertifikat ist immer persönlich und nicht übertragbar. Die persönlichen Angaben über den Inhaber werden sowohl im Zertifikat wie auch bei der SG-PKI gespeichert.

PIN/PUK

Die PIN muss unabhängig von anderen Passwörtern gewählt werden und darf für Dritte nicht zugänglich sein. Sie muss nicht regelmässig geändert werden, ausser es besteht der konkrete Verdacht, dass ein Dritter Kenntnis davon erlangt hat.

Das Zertifikat (und somit der Zertifikatsträger: Smartcard, USB-Stick, etc.) muss mit einer mind. 6-stelligen PIN gesichert werden, wobei rein numerische PINs, sowie auch gemischte PINs erlaubt sind. Um den Missbrauch der eigenen elektronischen Identität zu vermeiden, darf die PIN niemals Dritten bekanntgegeben werden.

Der PUK der Smartcard muss mindestens 8-stellig nach den oben genannten Regeln gewählt werden.

Meldepflicht

Ein allfälliger Verlust der Smartcard muss vom LRAO umgehend der SG-PKI gemeldet werden. In der Folge wird das betroffene Zertifikat gesperrt (revoziert) und die Sperrung auf einer öffentlichen elektronischen Sperrliste publiziert. Selbst wenn die Smartcard wiedergefunden werden sollte, bleibt das Zertifikat gesperrt und somit ungültig. Unmittelbar nach erfolgter Sperrung kann bei der SG-PKI die Ausstellung eines neuen LRAO-Zertifikates beantragt werden. Der Prozess der Ausstellung eines neuen LRAO-Zertifikats entspricht der Erstausstellung.

Organisationswechsel, Namenswechsel (z.B. nach Heirat) oder Änderung der E-Mail-Adresse bedingen die Ausstellung eines neuen Zertifikates (Erstausstellung).

6 Revokation

Revokationen müssen bei der SG-PKI beantragt werden. Dazu steht den befugten Personen (siehe abschliessende Liste unten) ein Formular auf der Homepage der SG-PKI www.pki.admin.ch zur Verfügung. Wird die Revokation per Telefon beantragt, wird die SG-PKI den Antragsteller mit Hilfe der Revokationspassphrase und

den persönlichen Daten (Geburtstag, Geburtsort, etc.) identifizieren. Lediglich der Antragsteller selbst ist befugt, eine Revokation per Telefon zu beantragen. Weitere Personen, die eine Revokation beantragen dürfen, müssen die Anfrage schriftlich einreichen.

Befugte Personen sind:

- der Zertifikatsinhaber selbst
- der SG-PKI Verantwortliche
- SG-PKI Security Officer
- die für den Zertifikatsinhaber zuständigen:
  - Mitarbeiter des HR (Personaldienst),
  - Linienvorgesetzte
  - LRA Officer
  - ISBO
  - ISBD
  - PKI Verantwortliche der Organisation

7 Inhalt des Zertifikates

Authentifizierungszertifikat (Authentication Key)
Fingerprint (SHA-1):
Certificate Validity:
Serial #:

8 Akzept/ Bestätigung für Erhalt der Smartcard

Mit der Unterschrift auf dem Empfangsformular für LRAO-Zertifikate bestätigt der Zertifikatsinhaber nach Erhalt der LRAO-Smartcard:

- Die Korrektheit der im Zertifikat gespeicherten Daten.
- Den Erhalt der LRAO-Smartcard.
- Diese Guidelines und die Rechte und Pflichten, die aus diesen Guidelines erwachsen, verstanden und akzeptiert zu haben. Allfällige Fragen wurden von der SG-PKI verständlich beantwortet.
- Die Revokationspassphrase sowie die restlichen zur telefonischen Identifikation der Person und des Zertifikates benötigten Felder korrekt ausgefüllt zu haben.

Ausserdem verpflichtet sich der angehende LRAO, die hier beschriebenen Richtlinien, die in der CP/CPS («*Certificate Policy and Certification Practice Statement of the Swiss Government Root CA I*») beschriebenen, sowie auch die in den «*Swiss Government PKI Registrierrichtlinien Klasse B*» Anforderungen und Aufgaben zu erfüllen und umzusetzen.

Zusätzliche Fragen können an die Swiss Government PKI unter der Mailadresse pki-info@bit.admin.ch gestellt werden.

NICHT KLASSIFIZIERT

Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI

Zur Ausstellung von persönlichen Zertifikaten der Klassen A (qualifizierte und geregelte) und B (fortgeschrittene) Zertifikate der Swiss Government PKI, der Bundesbehörde der Schweizerischen Eidgenossenschaft

V1.0, 28.08.2018

Die Swiss Government PKI des BIT, in ihrer Rolle als Trust Service Provider (TSP), betreibt im Auftrag des ISB (Informatiksteuerungsorgan des Bundes) die PKI (Public-Key-Infrastruktur) der Bundesbehörden der Schweizerischen Eidgenossenschaft. Im Rahmen des Marktmodells «SD005 - Marktmodell Standarddienst: Identitäts- und Zugangsverwaltung (IAM)» werden die Zertifikate der Klasse A und B definiert. Die LRA-Officer (Local Registration Agency Officer) sind für die Ausstellung von Zertifikaten der Klasse A und B zuständig. Bezug und Nutzung der LRAO-Zertifikate der Klassen A und B unterliegen den Bestimmungen der «*Benutzervereinbarung und Nutzungsbedingungen Klasse A/B*». Diese werden durch die Swiss Government PKI (SG-PKI) jährlich den jeweils geltenden gesetzlichen Vorschriften und den normativen Anforderungen an Public Key Infrastrukturen angepasst. Letztere bilden die Basis dieser Benutzervereinbarung und Nutzungsbedingungen. Die jeweils gültige Version ist auf www.pki.admin.ch publiziert. Alle Inhaber von Zertifikaten werden über die Publikation einer aktualisierten Version der Dokumente per E-Mail informiert.
Zu beachten sind des Weiteren die «*Guidelines zu den LRAO-Zertifikaten der SG-PKI*». Diese müssen beim Bezug eines LRAO-Zertifikats ebenfalls akzeptiert werden.

Vollständigkeit und Genauigkeit der Informationen

Der Inhaber eines LRAO-Zertifikates der Swiss Government PKI (in Folge «Inhaber oder LRAO» genannt[3]) verpflichtet sich dazu, dem TSP die für den Ausstellungsprozess sowie auch für den Inhalt des Zertifikats benötigten Informationen jederzeit korrekt und vollständig zu liefern. Vor der Ausstellung des Zertifikats muss der LRAO bei persönlicher Anwesenheit anhand eines gültigen Reisedokuments identifiziert werden. Das Zertifikat ist untrennbar an diesen LRAO gebunden. Vorname(n)/ Nachname(n), Suffix und e-Mailadresse des LRAO werden immer im Zertifikat aufgeführt.

Der Inhaber verpflichtet sich ebenfalls, die Daten seiner Kunden (=Bezüger von Zertifikaten der Klassen A und/ oder B) gemäss den «*Registrierrichtlinien für die Klasse A bzw. B*» zu prüfen.

Der LRAO ist verpflichtet, den TSP zu informieren, sobald sich seine persönlichen Daten, insbesondere Vorname, Nachname, Suffix (seines Eintrages im Admin-Directory des Bundes) oder die e-Mailadresse ändern.

Schutz des privaten Schlüssels und des Zertifikats

Der LRAO verpflichtet sich dazu, alle angemessenen Vorkehrungen zu treffen, um die alleinige Kontrolle, die Vertraulichkeit und den Schutz vor Verlust und Missbrauch des privaten Schlüssels und der allfällig damit verbundenen Aktivierungsdaten (z.B. PIN/ PUK) und Medien (z.B. Smartcard), zu gewährleisten. Der private Schlüssel des Zertifikats kann und darf nur im Zusammenhang mit dem Zertifikat und nur für die im Zertifikat festgelegten Zwecke (Ausstellung/Revokation/Management von Klasse A und B Zertifikate) eingesetzt werden. Sie dürfen auf keinen Fall unberechtigten Dritten zugänglich gemacht werden. Der Inhaber haftet für jeden Schaden, der durch die Weitergabe des privaten Schlüssels und der allfällig damit verbundenen Aktivierungsdaten und Medien an Dritte entstanden ist.

Der TSP behält sich vor, das Zertifikat bereits bei einem konkreten Verdacht auf Missbrauch oder unautorisierten Zugang zum privaten Schlüssel ohne Vorinformation zu revozieren.

[3] Die männliche Form «Inhaber» wird in diesem Dokument der besseren Leserlichkeit dienend gleichermassen für das weibliche und das männliche Geschlecht benutzt.

Nutzung des Zertifikats

Der LRAO stellt sicher, dass ihm Inhalt, Zweck und Wirkung des Einsatzes des LRAO-Zertifikates bekannt sind. Er verpflichtet sich, den auf der LRAO-Smartcard vorhandenen Zertifikat und den privaten Schlüssel nur für autorisierte Geschäfte und unter Einhaltung aller geltenden gesetzlichen Vorschriften sowie den Bestimmungen dieses Dokuments einzusetzen.

Berichterstattung und Revokation

Der LRAO verpflichtet sich dazu, das Zertifikat und den dazugehörigen privaten Schlüssel unverzüglich nicht mehr einzusetzen und beim TSP die Revokation zu verlangen, wenn:

- der konkrete Verdacht besteht, dass mit dem Zertifikat verdächtige Aktivitäten (Missbrauch der Aktivierungsdaten) unternommen wurden;
- die Informationen im Zertifikat nicht mehr korrekt oder ungenau sind oder es in naher Zukunft sein werden;

Den Anweisungen des TSP ist bei Verdacht auf Kompromittierung oder Missbrauch des Zertifikats unmittelbar Folge zu leisten.

Wenn aus Sicherheitsgründen erforderlich und aus datenschutzrechtlicher Sicht erlaubt, kann der TSP Daten über den LRAO, das Zertifikat und weitere in unmittelbarem Zusammenhang stehende Informationen an andere zuständige Stellen, TSPs, Firmen und industrielle Gruppen weiterleiten, wenn das Zertifikat oder die Person, die das Zertifikat einsetzt, als Quellen einer missbräuchlichen Verwendung identifiziert werden.

Alle Informationen betreffend die Revokation werden durch den TSP aus Gründen der Nachvollziehbarkeit archiviert.

Beendigung des Einsatzes des Zertifikats

Der LRAO verpflichtet sich dazu, den Einsatz des Zertifikats nach dessen Ablauf oder Revokation (insbesondere aufgrund einer Kompromittierung) sofort zu unterlassen.

Verantwortung / Haftung

Der LRAO ist dafür verantwortlich, dass das LRAO-Zertifikat und der zugehörige private Schlüssel nur unter Einhaltung der Bestimmungen in Abschnitt «Nutzung des LRAO-Zertifikates» dieses Dokuments eingesetzt werden. Ein Verstoss gegen diese Vorgabe hat eine Revokation und weitere administrative und gegebenenfalls juristische Massnahmen zur Folge. Der LRAO trägt die Verantwortung für alle durch ihn mit dem Zertifikat auf der LRAO-Smartcard vorgenommenen Tätigkeiten sowie für allfällig daraus resultierende Schäden und deren Folgen.

Anerkennungs- und Einverständniserklärung

Der LRAO nimmt zur Kenntnis, dass der TSP das Zertifikat bereits bei einem begründeten Verdacht eines Missbrauchs, einer Verletzung der Bestimmungen dieses Dokuments oder eines sonstigen Verstosses gegen geltende gesetzliche Bestimmungen unverzüglich revoziert.

Der LRAO bezeugt mit seiner Unterschrift im jeweiligen Anmeldeformular Klasse A/B: Antrag LRA-Officer, dass er das vorliegende Dokument «*Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI*» gelesen und verstanden hat und die darin aufgeführten Bestimmungen akzeptiert.

NICHT KLASSIFIZIERT

Benutzervereinbarung und Nutzungsbedingungen Klasse B

Für persönliche, fortgeschrittene Zertifikate der Swiss Government PKI der Bundesbehörden der Schweizerischen Eidgenossenschaft

V1.1, 31.03.2017

Die Swiss Government PKI des BIT, in ihrer Rolle als Certification Service Provider (CSP), betreibt im Auftrag des ISB (Informatiksteuerungsorgan des Bundes) die PKI (Public-Key-Infrastruktur) der Bundesbehörden der Schweizerischen Eidgenossenschaft. Die Zertifikate der Klasse B sind im Rahmen des Marktmodells «SD005 - Marktmodell Standarddienst: Identitäts- und Zugangsverwaltung (IAM) » definiert. Bezug und Nutzung der Klasse B Zertifikate der Swiss Government PKI unterliegen den Bestimmungen dieses Dokuments. Diese werden durch die Swiss Government PKI (SG-PKI) jährlich den jeweils geltenden gesetzlichen Vorschriften und den normativen Anforderungen an Public Key Infrastrukturen angepasst. Letztere bilden integrierenden Bestandteil dieser Benutzervereinbarung und Nutzungsbedingungen. Die jeweils gültige Version ist auf www.pki.admin.ch publiziert. Alle Inhaber werden über die Publikation einer aktualisierten Version dieses Dokuments per E-Mail informiert.

Zu beachten sind des Weiteren die «*Guidelines zu Klasse B Zertifikaten der Swiss Government PKI*». Diese müssen beim Bezug eines Zertifikats der Klasse B separat akzeptiert werden.

Vollständigkeit und Genauigkeit der Informationen

Der Inhaber von Klasse B Zertifikaten der Swiss Government PKI (in Folge «Inhaber» genannt[4]) verpflichtet sich dazu, dem CSP die für den Ausstellungsprozess sowie auch für den Inhalt des Zertifikats benötigten Informationen jederzeit korrekt und vollständig zu liefern. Vor der Ausstellung des Zertifikats muss der Kunde bei persönlicher Anwesenheit anhand eines gültigen Reisedokuments identifiziert werden. Das Zertifikat ist untrennbar an diesen Kunden gebunden.

Vorname(n)/ Nachname(n), Suffix und e-Mailadresse des Kunden werden immer im Zertifikat aufgeführt. Es werden weitere persönliche Angaben über den Inhaber, wie Revokationspassphrasen und der Scan des gültigen Reisedokumentes bei der Swiss Government PKI erfasst.

Der Kunde ist verpflichtet, den CSP zu informieren, sobald sich seine persönlichen Daten, insbesondere Vorname, Nachname, Suffix (seines Eintrages im Admin-Directory des Bundes) oder die e-Mailadresse ändern.

Schutz der privaten Schlüssel und der Zertifikate

Der Inhaber verpflichtet sich dazu, alle angemessenen Vorkehrungen zu treffen, um die alleinige Kontrolle, die Vertraulichkeit und den Schutz vor Verlust und Missbrauch der privaten Schlüssel und der allfällig damit verbundenen Aktivierungsdaten (z.B. PIN/ PUK) und Medien (z.B. Smartcard), zu gewährleisten. Die privaten Schlüssel der Zertifikate können und dürfen nur im Zusammenhang mit den Zertifikaten und nur für den in den Zertifikaten festgelegten Zwecken (Signatur, Authentifizierung, Verschlüsselung) eingesetzt werden. Sie dürfen auf keinen Fall unberechtigten Dritten zugänglich gemacht werden. Der Inhaber haftet für jeden Schaden, der durch die Weitergabe der privaten Schlüssel und der allfällig damit verbundenen Aktivierungsdaten und Medien an Dritte entstanden ist.

Der CSP behält sich vor, die Zertifikate bereits bei einem konkreten Verdacht auf Missbrauch oder unautorisierten Zugang zu den privaten Schlüsseln ohne Vorinformation zu revozieren.

[4] Die männliche Form «Inhaber» wird in diesem Dokument der besseren Leserlichkeit dienend gleichermassen für das weibliche und das männliche Geschlecht benutzt.

Nutzung der Zertifikate

Der Inhaber stellt sicher, dass ihm Inhalt, Zweck und Wirkung des Einsatzes der Klasse B Zertifikate bekannt sind. Er verpflichtet sich, die Klasse B Zertifikate und deren privaten Schlüssel nur für autorisierte Geschäfte und unter Einhaltung aller geltenden gesetzlichen Vorschriften sowie den Bestimmungen dieses Dokuments einzusetzen.

Berichterstattung und Revokation

Der Inhaber verpflichtet sich dazu, die Zertifikate und die dazugehörigen privaten Schlüssel unverzüglich nicht mehr einzusetzen und beim CSP die Revokation zu verlangen, wenn:

- der konkrete Verdacht besteht, dass mit einem Zertifikat verdächtige Aktivitäten (Missbrauch der Aktivierungsdaten, des Signaturzertifikates oder des Verschlüsselungszertifikates) unternommen wurden;
- die Informationen in den Zertifikaten nicht mehr korrekt oder ungenau sind, oder es in naher Zukunft sein werden;

Den Anweisungen des CSP ist bei Verdacht auf Kompromittierung oder Missbrauch der Zertifikate unmittelbar Folge zu leisten.

Wenn aus Sicherheitsgründen erforderlich und aus datenschutzrechtlicher Sicht erlaubt, kann der CSP Daten über den Inhaber, die Zertifikate und weitere in unmittelbarem Zusammenhang stehende Informationen an andere zuständige Stellen, CSPs, Firmen und industrielle Gruppen weiterleiten, wenn die Zertifikate oder die Person, die die Zertifikate einsetzt, als Quellen einer missbräuchlichen Verwendung identifiziert werden.

Alle Informationen betreffend die Revokation werden durch den CSP aus Gründen der Nachvollziehbarkeit archiviert.

Beendigung des Einsatzes der Zertifikate

Der Inhaber verpflichtet sich dazu, den Einsatz der Zertifikate nach deren Ablauf oder Revokation (insbesondere aufgrund einer Kompromittierung) sofort zu unterlassen.

Verantwortung / Haftung

Der Inhaber ist dafür verantwortlich, dass die Klasse B Zertifikate und die zugehörigen privaten Schlüssel nur unter Einhaltung der Bestimmungen in Abschnitt «Nutzung des Zertifikates» dieses Dokuments eingesetzt werden. Ein Verstoss gegen diese Vorgabe hat eine Revokation und weitere administrative und gegebenenfalls juristische Massnahmen zur Folge. Der Inhaber trägt die Verantwortung für alle durch ihn vorgenommenen Signaturen, Authentisierungen und Verschlüsselungen sowie für allfällig daraus resultierende Schäden und deren Folgen.

Anerkennungs- und Einverständniserklärung

Der Inhaber nimmt zur Kenntnis, dass der CSP die Zertifikate bereits bei einem begründeten Verdacht eines Missbrauchs, einer Verletzung der Bestimmungen dieses Dokuments oder eines sonstigen Verstosses gegen geltende gesetzliche Bestimmungen unverzüglich revoziert.

Der Inhaber bezeugt mit seiner Unterschrift, dass er das vorliegende Dokument «*Benutzervereinbarung und Nutzungsbedingungen Klasse B*» gelesen und verstanden hat und die darin aufgeführten Bestimmungen akzeptiert.

Ort, Datum: _____ Unterschrift: _____

NICHT KLASSIFIZIERT

Guidelines zu Klasse B Zertifikaten der Swiss Government PKI

Erläuterungen zum Bezug und Einsatz von Klasse B Zertifikate der Swiss Government PKI

V1.0, 09.03.2017

1 Zweck von Klasse B Zertifikaten

Zweck

Die Zertifikate der Klasse B sind im Rahmen des Marktmodells «SD005 - Marktmodell Standarddienst: Identitäts- und Zugangsverwaltung (IAM)» definiert. Klasse B Zertifikate können für folgende Zwecke verwendet werden:

- Vertrauenswürdige Signierung von Daten. Dadurch wird die Authentizität und Unversehrtheit der Daten sichergestellt.
- Verschlüsselung von Daten. Die Vertraulichkeit der Daten wir sichergestellt.
- Authentisierung von Personen. Das Zertifikat stellt den prüfenden Komponenten wie z.B. Eingangsportalen, eine gesicherte Identität des Inhabers zur Verfügung.

Durch erweiterte Prüf- und Sicherheitsmechanismen während des Ausstellungsprozesses der Klasse B Zertifikate wird die Identität des Zertifikatsinhabers auf einer hohen Sicherheitsstufe festgestellt. Die Ausgabe von Klasse B Zertifikaten erfolgt immer persönlich und nur nach Identifizierung des Inhabers mittels eines gültigen, für die Einreise in die Schweiz zugelassenen Reisedokumentes.

Ausgeschlossener Zweck

Klasse B Zertifikate erfüllen ausschliesslich die oben genannten Zwecke und geben keinerlei weitere Aufschlüsse, Versicherungen oder Garantien. Insbesondere garantieren Klasse B Zertifikate nicht, dass der Inhaber im Umgang mit dem Zertifikat korrekt und legal handelt.
Des Weiteren garantieren Klasse B Zertifikate nicht, dass:

- Der im Zertifikat genannte Inhaber aktiv in die Geschäftstätigkeiten involviert ist;
- Der im Zertifikat genannte Inhaber sich an die geltenden gesetzlichen Vorschriften hält;
- Der im Zertifikat genannte Inhaber vertrauenswürdig ist und im Geschäftsumfeld seriös handelt; oder
- Der im Zertifikat genannte Inhaber die fachliche, technische, organisatorische oder sonstige Kompetenz besitzt, dieses Zertifikat korrekt einzusetzen.

2 Qualität der Klasse B Zertifikate

Der LRA-Officer der SG-PKI hält sich an die in den Registrierrichtlinien vorgegebenen Prozesse, welche die notwendigen und zumutbaren Schritte zur Bestätigung folgender Tatsachen zum Zeitpunkt der Erstausstellung eines Klasse B Zertifikates festlegen:

- **Rechtlich gültige Existenz:** Der im Klasse B Zertifikat genannte Inhaber existiert als natürliche Person und verfügt über einen persönlichen Eintrag im AdminDir.
- **Identität:** Der Name des im Klasse B Zertifikats genannten Inhabers stimmt mit dem Namen in seinem gültigen Reisedokument überein.
- **Autorisierung:** Der im Klasse B Zertifikat genannte Inhaber ist zum Bezug des Zertifikates autorisiert.
- **Richtigkeit der Daten:** Alle im Zertifikat enthaltenen Daten und Informationen sind korrekt.

- **Vereinbarung/ Nutzungsbedingungen:** Der im Klasse B Zertifikat genannte Inhaber wurde vom LRAO (Local Registration Authority Officer) über die in der «*Benutzervereinbarung und Nutzungsbedingungen Klasse B*» beschriebenen Rechte und Pflichten informiert. Seine Fragen diesbezüglich wurden vom LRAO verständlich beantwortet. Der Inhaber hat die «*Benutzervereinbarung und Nutzungsbedingungen Klasse B*» gelesen, akzeptiert und unterzeichnet.
- **Status:** Die SG-PKI stellt den Status des Zertifikats sowie Informationen über dessen Gültigkeit/Revokation online abrufbar zur Verfügung.
- **Revokation:** Die SG-PKI kann das Klasse B Zertifikat gegebenenfalls aus den in der/n «*Benutzervereinbarung und Nutzungsbedingungen Klasse B*» genannten Gründen unverzüglich revozieren.

3 Policies

Alle geltenden gesetzlichen Vorgaben, Policies (inkl. der CP/CPS) und Richtlinien von Klasse B Zertifikaten sind im Internet auf der Website der SG-PKI publiziert: www.pki.admin.ch.

4 Inhalt und Gültigkeit des Klasse B Zertifikates

Inhalt

Das Klasse B Zertifikat der SG-PKI enthält Informationen betreffend:

- Herausgeber und ausstellender CA
- Informationen über die Root CA der ausstellenden CA
- Informationen über die angewandte Policy
- Ausstell- und Ablaufdatum des Zertifikates
- Seriennummer des Zertifikates
- Verwendungszweck des Zertifikates
- Informationen betreffend der CRL und dem OCSP
- Informationen betreffend der Auditoren der CA
- Informationen betreffend den Inhaber des Zertifikates gemäss Eintrag im AdminDir zum Zeitpunkt der Erstausstellung:
    1) Common Name des Inhabers
    2) E-Mail-Adresse
    3) UPN

Gültigkeit

Das Klasse B Zertifikat der SG-PKI ist max. 3 Jahre gültig. Das Zertifikat kann vor Ablauf der 3-Jahres-Frist maximal zwei Mal vom Inhaber selbst für weitere drei Jahre erneuert werden. Für die Erneuerung des Zertifikates steht dem Inhaber der Rekeying Wizard zur Verfügung. Nach Ablauf der 3. Gültigkeitsperiode muss durch den LRA-Officer ein neues Zertifikat wie im Prozess der Erstausstellung ausgestellt werden.

5 Bezug von Klasse B Zertifikaten

Bezug

Für den Bezug von Klasse B Zertifikaten der SG-PKI sind folgende Dokumente bzw. Registrierungen nötig:

- Ein gültiges, für die Einreise in die Schweiz zugelassenes Reisedokument (ID/ Pass), ausgestellt auf den Antragsteller.
- Ein ausgefülltes und (elektronisch) signiertes Antragsformular für Klasse B Zertifikate der Swiss Government PKI, oder eine Anmeldung über die Linie des Amtes, bzw. über den internen festgelegten HR-Prozess.
- Die unterschriebene «*Benutzervereinbarung und Nutzungsbedingungen Klasse B*» (wird bei jeder Ausstellung von Klasse B Zertifikaten am Schluss vom LRA-Officer zusammen mit diesem Dokument ausgedruckt).
- Ein persönlicher Eintrag im AdminDir, mit Nachname(n), Vorname(n) (gemäss Reisedokument), gültiger E-Mailadresse und optional einem UPN Eintrag (User Principal Name)

Identifizierung

Die persönliche Identifizierung des Antragstellers wird durch die LRAOs der Klasse B der SG-PKI bei der Erstausstellung und spätestens nach Ablauf der dritten Gültigkeitsperiode sichergestellt. Bei einer dezentralen Ausstellung von Zertifikaten der Klasse B wird die persönliche Identifizierung von einem Delegierten des LRAOs, dem RIO (Registration Identification Officer) übernommen, der die Bestätigung der durchgeführten Identifizierung dem LRAO zur Freigabe des Antrages weiterleitet.

Um die antragstellende Person zu identifizieren, wird das Reisedokument auf Gültigkeit, Richtigkeit und Echtheit überprüft. Die LRAOs sind zudem verpflichtet, das Bild des Dokumentes mit der vor Ihnen stehenden Person zu validieren. Ebenso wird der Antrag vor der Ausstellung eines persönlichen Zertifikates plausibilisiert (Person arbeitet tatsächlich in der im AdminDir Eintrag zugewiesenen Organisationseinheit und benötigt das Zertifikat im geschäftlichen Alltag; der Antragsteller ist berechtigt ein Zertifikat zu beantragen).

Verbindlichkeit

Der Antrag, oder der interne Prozess zur Beantragung muss durch die zuständigen Stellen freigegeben sein. Diese Guidelines und das Dokument «*Benutzervereinbarung und Nutzungsbedingungen Klasse B*» müssen vom Antragsteller akzeptiert und (digital) unterschrieben werden.

6 Schutz des privaten Schlüssels und des Zertifikates

Übertragbarkeit

Das Klasse B Zertifikat ist immer persönlich und nicht übertragbar. Die persönlichen Angaben über den Inhaber werden sowohl im Zertifikat wie auch bei der SG-PKI gespeichert.

PIN/PUK

Die PIN muss unabhängig von anderen Passwörtern gewählt werden und darf für Dritte nicht zugänglich sein. Sie muss nicht regelmässig geändert werden, ausser es besteht der konkrete Verdacht, dass ein Dritter Kenntnis davon erlangt hat.

Das Zertifikat (und somit der Zertifikatsträger: Smartcard, USB-Stick, etc.) muss mit einer mind. 6-stelligen PIN gesichert werden, wobei rein numerische PINs, sowie gemischte PINs erlaubt sind. Um den Missbrauch der eigenen elektronischen Identität zu vermeiden, darf die PIN niemals Dritten bekanntgegeben werden.

Der PUK der Smartcard muss mindestens 8-stellig nach den oben genannten Regeln gewählt werden.

Meldepflicht

Ein allfälliger Verlust der Smartcard muss vom Inhaber umgehend dem zuständigen LRAO oder der IT-Serviceorganisation gemeldet werden. In der Folge werden die betroffenen Zertifikate gesperrt (revoziert) und die Sperrung auf einer öffentlichen elektronischen Sperrliste publiziert. Selbst wenn die Smartcard wiedergefunden werden sollte, bleiben die Zertifikate gesperrt und sind somit ungültig. Unmittelbar nach erfolgter Sperrung kann beim zuständigen LRAO die Ausstellung eines neuen Klasse B Zertifikates beantragt werden. Der Prozess der Ausstellung eines neuen Klasse B Zertifikats entspricht der Erstausstellung.

Organisationswechsel, Namenswechsel (z.B. nach Heirat) oder Änderung der E-Mail-Adresse bedingen die Ausstellung eines neuen Zertifikates (Erstausstellung).

7 Revokation

Revokationen müssen beim LRAO beantragt werden. Dazu steht den befugten Personen (siehe abschliessende Liste unten) ein Formular auf der Homepage der SG-PKI www.pki.admin.ch zur Verfügung. Wird die Revokation per Telefon beantragt, wird der LRAO den Antragsteller mit Hilfe der Revokationspassphrase und

den persönlichen Daten (Geburtstag, Geburtsort, etc.) identifizieren. Lediglich der Antragsteller selbst ist befugt eine Revokation per Telefon zu beantragen. Weitere Personen, die eine Revokation beantragen dürfen, müssen die Anfrage schriftlich einreichen.

Befugte Personen sind:

- der Zertifikatsinhaber selbst.
- der SG-PKI Verantwortliche
- SG-PKI Security Officer
- Die für den Zertifikatsinhaber zuständigen:
  - Mitarbeiter des HR (Personaldienst),
  - Linienvorgesetzte
  - LRA Officer
  - ISBO
  - ISBD
  - PKI Verantwortliche der Organisation

8 Inhalt des Zertifikates

Authentifizierungszertifikat (Authentication Key)
Fingerprint (SHA-1):
Certificate Validity:
Serial #:

Verschlüsselungszertifikat (Encryption Key)
Fingerprint (SHA-1):
Certificate Validity:
Serial #:

Unterschriftszertifikat (Signing Key)
Fingerprint (SHA-1):
Certificate Validity:
Serial #:

9 Akzept/ Bestätigung für Erhalt der Smartcard

Mit der Unterschrift bestätigt der Zertifikatsinhaber:

- Die Korrektheit der im Zertifikat gespeicherten Daten.
- Den Erhalt der Smartcard.
- Diese Guidelines gelesen und mit dem LRAO besprochen zu haben. Allfällige Fragen wurden vom LRAO verständlich beantwortet.
- Die Rechte und Pflichten, die aus diesen Guidelines erwachsen verstanden und akzeptiert zu haben.
- Die hier beschriebenen Richtlinien umzusetzen.

Zusätzliche Fragen können an die Swiss Government PKI unter der Mailadresse pki-info@bit.admin.ch gestellt werden[5].

Common Name (CN):

Ausstelldatum: **Unterschrift:** _____

[5] Bitte lesen Sie auch die Benutzer*vereinbarung und Nutzungsbedingungen für Klasse B Zertifikate der Swiss Government PKI*. Bei Ihrer Klasse B Bestellung wird eine signierte Kopie dieses Dokuments verlangt. www.pki.admin.ch .

Anhang C: Dokument Änderungshistorie

RR Version	Thema	Kapitel
V5.2	Definitionen, Akronyme und Abkürzungen – Diverse Ergänzungen und Korrekturen	Definitionen, Akronyme und Abkürzungen
V5.2	Ref. [29]-[32] Ergänzt	Referenzen
V5.2	Präzisierung: Klasse B Zertifikate werden nur für natürliche Personen ausgestellt	1.3
V5.2	Personensicherheitsprüfung: Es wird die PSP oder eine äquivalente Vertrauenswürdigkeitsprüfung durch das anstellende Amt verlangt.	2.1 / 3.13
V5.2	Unterstützung der LRA neu über das Service Desk BIT oder mittels Remedy Ticket / MAC-Antrag	3.2 / 3.11 / 3.12
V5.2	Zutrittskontrolle: Anforderungen an Lokalitäten der LRA neu definiert	3.3
V5.2	Zugangskontrolle: Anforderungen an Schutz des LRAO PCs angepasst an Anforderungen an ein Bundesclient	3.4 / 3.5
V5.2	Formulare und Kundendaten: Präzisierung zur Aufbewahrung	3.6
V5.2	Journal: Neue Richtlinien zur Führung eines (elektronischen) Journals, und Zugriffsregelung	3.7
V5.2	Präzisierungen für den (elektronischer) Zugriffsschutz und Aufbewahrungsfristen für elektronische Dokumente	3.8 / 3.9
V5.2	Ablösung spezielles LRAO-Zertifikat durch Berechtigungserteilung auf die persönlichen Zertifikate der Klasse B	3.10
V5.2	Schutz der privaten Schlüssel der LRA-Station	Ehem. Kap. 3.10 - wurde entfernt
V5.2	Ablösung LRA-Station durch BAB-Clients mit LRA-Officer Funktionen	3.11 / 3.12
V5.2	Präzisierungen zu den geltenden Gesetzen für den Schutz persönlicher Daten	3.14
V5.2	Präzisierungen in Bezug auf die Ausbildung und Weiterbildung der LRAOs, Korrektur und weitere Hinweise bezüglich der benötigten Punktzahl	3.15 / 3.16
V5.2	PIN-Reset und PUK Handling	Neues Kapitel: 3.19
V5.2	Konformitätsprüfung: Textrevidierung	4
V5.2	Prozess ohne RIO: Ergänzungen zum Ausstellprozess mit «Ausweis F»	5.2 / 5.2.3.2 / 5.2.3.7 / 5.2.4.2
V5.2	Eingabe eines Ausstellungsauftrages mittels Auftragserfassungssysteme (MAC, Gever) und Freigabe Identifikation mittels den «Ausweis F» inkl. zusätzliches Formular	5.2.2 / 5.2.3.2
V5.2	Einführung Felder 4 und 5 («adminGivenNameLong» und «adminSurNameLong») im AdminDir und LRAO-Tools und die möglichen Entscheidungsvarianten für die Ausstellung des Zertifikates	5.2.3.1
V5.2	Einbindung der Ausweisdokumente via Scan	5.2.3.7
V5.2	Elektronisches Datenhandling und Archivierung (Scandateien)	3.7/ 3.8 / 5.2.3.6 / 5.2.3.8 / 5.2.3.12 / 5.2.3.13
V5.2	Revokation: Präzisierung im Fall von telefonischen Anfragen	5.3.2
V5.2	Revokationsformular: Neue Richtlinien bei Revokation über den Revokation Wizard	5.3.4.2 / 5.3.4.4 / 6.3
V5.2	Auditrelevante Formulare: Die Relevanz wurde im entsprechenden Kapitel ergänzt	6.1 ff.
V5.2	Antragsformular: Anforderungen an verlangte Daten angepasst	6.1
V5.2	Neue Richtlinien im Umgang mit der «*Bestätigung Erhalt Smartcard*»	6.2
V5.2	Ergänzendes Formular für Antragsteller mit Ausweis F	Neues Kap.: 6.1.1
V5.2	Checklisten – Diverse Korrekturen	Anhang A

V5.2	Formulare – Diverse Aktualisierungen/Korrekturen und neues Formular für Ausweis F	Anhang B
V5.2	Formulare – aufgrund Vollständigkeit noch LRAO Formulare und BV und GL hinzugefügt	Anhang B
V5.2	Dokument Änderungshistorie und Stand/Inkrafttreten des Dokuments	Neuer Anhang: Anhang C
V5.2	Checklisten und Formulare angepasst	Anhang B
V5.2	Formular PIN-Reset Superuser und KRA-Antrag eingefügt in die RR	Anhang B
V5.9	Versionierungsänderung vor Abnahme	V5.2 RR
V5.9	Kap. 3.12 'Reparatur' gestrichen	Ehem. 3.12
V6.0	Versionierung nach Freigabe	Versionierung

Stand Version 6.0: 01.11.2019

Inkrafttreten der Version: 01.01.2020