Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

31.07.2025

Swiss Government PKI Registrierrichtlinien Klasse B

Registrierrichtlinien der Swiss Government PKI für die LRA

Status: Freigegeben V7.0

Klassifizierung *	Nicht klassifiziert
Status **	Freigegeben
Auftraggeberin	Swiss Government PKI
Autor	TRF
Bearbeitende	SG-PKI BIT
Prüfende	Beatrice Metaj, Sébastien Farquet, Cornelia Enke
Genehmigende	PKI Management Board
Verteiler	LRAO, RIO, Auditoren
Ablageort	PKI SharePoint
Inkrafttreten	01.08.2025

* Nicht klassifiziert, Intern, Vertraulich

** In Arbeit, In Prüfung, Abgeschlossen, Freigegeben

Änderungskontrolle, Prüfung, Genehmigung

Version	Datum	Name oder Rolle	Beschreibung, Bemerkung
2.91	23.07.2010	Andreas Zürcher	Ersetzt Versionen 2.x, bei der Klasse A und B in einem Dokument abgehandelt werden
2.92		Daniel Stich	Straffung und Sicherung der Konsistenz mit CP/CPS, Checklisten mit Links zu den Richtlinien
2.93		Daniel Stich	Einarbeitung Ergebnisse Review mit A. Zürcher
2.94		Daniel Stich	Einarbeitung Feedback LZPPS
3.00	23.02.2012	Daniel Stich	Final
3.01	23.04.2012	Daniel Stich	Anpassung der PIN-Regeln
3.02	30.01.2013	Daniel Stich	PDF in RIO-Prozessen und Zertifikaterstellung, signierte elektronische Dokumentübermittlung bei RIO-Prozess, Anpassungen an 2-Faktor-Login auf Bundesclients
3.03	22.04.2013	Tomaso Vasella	Einbezug von Funktionszertifikaten Anpassung AdminPKI-> Swiss Government PKI Anpassung Organisationseinheit nach ON BIT
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 Wizard, 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
6.1	29.11.2023	Andreas Ruckstuhl, Adrian Bärlocher	Überarbeitungen für Review durch TRF
6.3	25.04.2024	Beatrice Metaj, Jürgen Weber	Review TRF und Aufbereitung für Prüfung/Genehmigung
6.4	01.05.2024	Beatrice Metaj	Ergänzungen und Korrekturen aus dem Management Board, insb. Kap. 5.2.3.6 (Plausibilisierung) ergänzt
6.5	02.07.2024	Sébastien Farquet	Überarbeitungen für neutrale Formulierung
6.6	29.07.2024	Stephanie Schäfer, Silvio Pelli, Beatrice Metaj, Sébastien Farquet und Adrian Bärlocher	Ergänzungen und Korrekturen aus dem Review
6.7	14.01.2025	Beatrice Metaj, Sébastien Farquet, Cornelia Enke	Final Review vor Publikation
7.0	14.01.2025	Beatrice Metaj	Freigegebene Version zur Publikation

Definitionen, Akronyme, Abkürzungen und Referenzen

- Glossar
- Referenzliste

Hinweis

Die LRA und mindestens ein LRAO werden unter anderem auf Grundlage dieses Dokument auditiert.

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.

1.1 Zielgruppe

Das Dokument richtet sich primär an die ausgebildeten Klasse B LRAO der Ämter und Kantone.

1.2 Verwendete Begriffe und Abkürzungen

Spezielle Begriffe und Abkürzungen, welche in diesem Dokument verwendet werden, sind in der Tabelle «Definitionen, Akronyme und Abkürzungen» auf der www.pki.admin.ch zusammengefasst und werden in kurzer Form erläutert.

1.3 Referenzierte Dokumente

Hinweise auf referenzierte Dokumente werden in eckigen Klammern mit einem entsprechenden Erkennungszeichen angegeben und auf die PKI-Homepage verlinkt. – zum Beispiel [KLB001].

Die referenzierten Dokumente sind mit der jeweiligen zum Zeitpunkt der Publikation dieser Registrierrichtlinien gültigen Version versehen. Neuere Versionen sind, wenn vorhanden, online verfügbar und müssen eingesetzt werden.

1.4 Zweck des Dokuments

Die «Certificate Policy and Certification Practice Statement of the Swiss Government Root CA» (im Folgenden abgekürzt mit „CP/CPS“) [KLB001] ist das massgebende Regelwerk für die Zertifikate der Klasse B. Das Ziel dieser Registrierrichtlinien ist es, die Anforderungen der CP/CPS [KLB001] betreffend der LRA zu konkretisieren.

1.5 Geltungsbereich

Diese Richtlinie gilt für alle Personen, 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 Personen.

1.6 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 der antragstellenden Person abgeben.

Die inhabende Person eines Klasse B Zertifikates ist eine natürliche Person (keine Organisationen, Gruppen, Funktionen) und besitzt in der Regel drei Schlüsselpaare mit den entsprechenden Zertifikaten. Je nach Zertifikatstyp (Klasse B Zertifikat 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 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.

Bei der Erneuerung wird bei den Prestaged Smartcards das nächstfolgenden Schlüsseltriplet von der CA signiert. Anschliessend werden nur die alten Schlüssel und Zertifikate für Signatur und Authentifizierung von der Smartcard gelöscht. Das alte Schlüsselpaar für die Schlüssel- und Datenverschlüsselung wird für spätere Entschlüsselung auf der Smartcard belassen.

Inhabende Personen können sowohl ein Klasse A, ein Klasse B und eines oder mehrere Klasse B Funktionszertifikate besitzen. Klasse A, Klasse B und Funktionszertifikate dürfen nicht auf demselben Security Token abgelegt sein, ein Security Token darf aber mehrere Funktionszertifikate beinhalten. Der oder die Vor- und Nachnamen der Person sind im Zertifikat eindeutig erkennbar und ersichtlich.

1.7 Security Token

Eine Liste der unterstützten Security Token und detaillierte Vorgaben dazu finden sich im vom Bereich Digitale Transformation und IKT-Lenkung (DTI) genehmigten Standard „A006 - Smartcard“ [BV002] und dessen Anhängen.

2 Aufgaben des LRAO und des RIO

2.1 Anforderungsprofil LRAO

- 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 128.31 [GV005] oder Ähnliches (vgl. Kapitel *0*), durchführen zu lassen
- Ein LRAO darf nicht für die Erfassung oder Mutation von Admin-Directory-Einträgen berechtigt sein, vorbehältlich von schriftlichen Ausnahmeregelungen mit der Bestätigung der jeweiligen Amtsleitung und des jeweiligen SG-PKI Security Officer.

2.2 Aufgaben und Pflichten des LRAO

Der LRAO hat folgende Aufgaben:

- Antrag und benötigte Zusatzformulare und –unterlagen prüfen (s. Kapitel *5.2.3.5*)
- Antragstellende Person identifizieren (s. Kapitel *5.2.3.5)*
- Angaben im Admin-Directory verifizieren
- Zertifikat ausstellen
- Zertifikat revozieren
- Antragstellende Person instruieren betreffend:
    - Aktivierungsdaten
    - Schutz der Aktivierungsdaten
    - ihren Rechten und Pflichten
    - «Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B – (für natürliche Personen)» [KLB021]
- Ggf. Checklisten ausfüllen und ablegen
- Journal führen über alle Aktivitäten, welche die Zertifikate und die LRA betreffen
- Dossiers der zertifikatsinhabenden Personen führen und aufbewahren
- Smartcards verwalten, eventuell beschaffen
- Schulung, Qualifikation und Support der RIO sicherstellen
- Den RIO-Kopien der Formulare „RIO Antrag Klasse B“, „Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B“ [KLB021] und die „Checkliste RIO“ zur Verfügung stellen
- Liste der RIO 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
- Sicheres Aufbewahren und Verwalten des LRA-Materials

- Einhaltung der Vorgaben zum Datenschutz (DSG)

2.3 Anforderungsprofil RIO

- Hohe persönliche Integrität
- Genaues Arbeiten nach den Vorschriften der SG-PKI und des auftraggebenden LRAO
- Grundverständnis des Begriffs „Nachvollziehbarkeit“ und Einsicht in die Notwendigkeit dessen Umsetzung in den Tätigkeiten als RIO
- Zuverlässigkeit
- Freude am Umgang mit Kunden
- Ein RIO darf nicht für die Erfassung oder Mutation von Admin-Directory-Einträgen berechtigt sein, vorbehältlich von schriftlichen Ausnahmeregelungen mit der Bestätigung der jeweiligen Amtsleitung und des jeweiligen SG-PKI Security Officer.

2.4 Aufgaben des RIO

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

- Antragstellende Person identifizieren
- Antragstellende Person instruieren betreffend:
  - Aktivierungsdaten
  - Schutz der Aktivierungsdaten
  - deren Rechten und Pflichten
  - «Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B» [KLB021]
- Antrag und benötigte Zusatzformulare und –unterlagen prüfen (s. Kapitel *5.2.3.2*)
- Ausweisdokument und Antrag kopieren
- Checkliste ausfüllen
- Ausgefüllte Checkliste, allfällige Zusatzformulare, unterschriebener Antrag enthaltend eine Kopie des gültigen Reisedokuments sowie die unterschriebene *Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B* [KLB021] sicher dem Auftrag gebenden LRAO per Post, Kurier oder elektronisch zustellen. Falls die elektronische Übermittlung gewählt wird: Einscannen der obigen Dokumente als PDF-Files, digitales Signieren der Files mit dem persönlichen Klasse B Zertifikat und Versand an den LRAO mittels verschlüsselter E-Mail. Alle zur Übermittlung gespeicherten Daten müssen nach der Übermittlung vom eigenen System gelöscht werden.
- Sicheres Aufbewahren und Verwalten von Prestaged Smartcards
- Der RIO ist **nicht** befugt Datensammlungen von Personen für die er die Identifikation an Stelle eines LRAO getätigt hat, auf irgendeine Weise zu speichern. Jegliche Personen-Informationen müssen an den zuständigen LRAO übermittelt oder gelöscht/geschreddert werden.

Ein LRAO kann die Rolle eines RIO einnehmen, aber nicht umgekehrt.

2.5 Vertrauenswürdigkeitsprüfung von LRAO

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

- Personensicherheitsprüfung gemäss Artikel 10 der Verordnung über die Personensicherheitsprüfungen [GV005] bei der Fachstelle PSP des VBS

und / oder

- Vornehmen eigener Massnahmen zur Überprüfung der Vertrauenswürdigkeit der Person, wie beispielsweise:
    - Kontrolle der Identität (Pass oder Identitätskarte);
    - Überprüfung von geschäftlichen und / oder privaten Referenzen;
    - Verifizierung der Vollständigkeit und Schlüssigkeit des Lebenslaufs;
    - 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 der Person gemäss obenstehender Empfehlung oder auf vergleichbare Art und Weise überprüft zu haben. Sie stuft die Person als vertrauenswürdig und integer ein und bestätigt zudem, dass die Person als zukünftiger LRAO über die notwendigen Kompetenzen zur Ausübung seiner zukünftigen Tätigkeit verfügt.

2.6 Vertraulichkeit, Datenschutz

Der LRAO hat eine Vertraulichkeitserklärung zu unterschreiben. Diese ist im «Klasse B: Antrag LRAO» integriert.

Die Gesetze und Verordnungen des Datenschutzes (DSG, DSV) [GV015, GV016] und der Informationssicherheit (ISG, ISV) [GV003, GV004] sind einzuhalten. Die Arbeiten als LRAO werden im Auftrag der SG-PKI ausgeführt. Der LRAO haftet persönlich für die Einhaltung bei seinen Aufgaben.

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

2.7 Ausbildung des Personals

Alle LRAO müssen eine Schulung durchlaufen. Am Ende der Schulung entscheidet ein schriftlicher Test, ob die teilnehmende Person genügend Kenntnisse und Fähigkeiten hat, um als LRAO der Klasse B tätig zu sein.

Besteht der angehende LRAO den Test nicht, erhält diese Person die LRAO-Berechtigungen vorerst nicht. Sie kann bei einem erneuten Kursbesuch und Test zeigen, dass sie über die erforderliche Eignung und die Kompetenzen verfügt. Stellen LRAO Mängel in ihrem Wissen, Fähigkeiten oder Unklarheiten fest und können diese selbst nicht beheben, sind sie verpflichtet, dies bei der Swiss Government PKI zu melden. Die Swiss Government PKI wird zusammen mit dem LRAO eine Lösung suchen.

Die RIO müssen ebenfalls eine Schulung mit reduziertem Umfang absolvieren. Die Schulung erfolgt grundsätzlich durch den sie beauftragenden LRAO. Die Schulung kann auch durch die Swiss Government PKI erfolgen. In der Schulung müssen zumindest die referenzierten Dokumente «*Überprüfung Identität Antragsteller Klasse B*» [KLB003], die «*Richtlinien für den Registration Identification Officer (RIO)*» [KLB027] und die «*Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B*» [KLB021] behandelt werden.

2.8 Auffrischung der Ausbildung

Der LRAO ist verpflichtet das persönliche 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 https://www.pki.admin.ch zur Verfügung. Die Swiss Government PKI verpflichtet sich, wichtige Änderungen per E-Mail anzuzeigen. Der LRAO ist verpflichtet, bei Erhalt eines entsprechenden E-Mails der Swiss Government PKI die entsprechenden Informationen zu lesen.

Weiter ist jeder LRAO verpflichtet, innerhalb einer Beobachtungsperiode von 24 Monaten insgesamt 20 Weiterbildungspunkte zu sammeln. Mit welchen Aktivitäten wie viele solcher Punkte gesammelt werden können, ist in der nachfolgenden Aufstellung auszugsweise beschrieben:

Aktivität	Punktzahl
Basiskurs LRAO (Teilnahme)	
Bestandener Test zum Basiskurs LRAO	
LRAO-Summit (1/2 Tag, Teilnahme und Feedback)	
Kurz-Informationsveranstaltung (virtuell, max. 1 Stunde, Feedback)	
LRAO-Workshop personalisiert (min. 4 Teilnehmer, vor Ort)	5 - 10 (je nach Inhalt)
E-Learning Module (inkl. Test)	max. 5
LRA-Audit (Teilnahme)	
Q&A Sessions (virtuell, max. 1 Stunde, Feedback)	

Tabelle 1: Anzahl Punkte pro LRAO-Anlass

Die Swiss Government PKI bietet regelmässig Weiterbildungs- und Wiederholungskurse für die LRAO an (LRAO-Workshops oder LRAO-Summit). Die LRAO 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 Allgemeine betriebliche Aspekte

3.1 Bedienzeiten der LRA

Die Servicezeiten der LRA werden von den jeweils verantwortlichen Organisationseinheiten festgelegt. Sie sind so zu gestalten, dass dringliche Aufgaben in angemessener Zeit erledigt werden können (z.B. Revokationen sofort ausführen max. innerhalb eines Arbeitstages).

3.2 Unterstützung der LRAO

3.2.1 Unterstützung

Zur Unterstützung der LRAO ist das Betriebsteam der SG-PKI gemäss den Angaben im Service- und Produktkatalog respektive dem geltenden Service Level Agreement erreichbar. Details sind auch auf der Webseite der SG-PKI erläutert.

3.2.2 Störung

Bei Störungen erfolgt der Kontakt zum Betriebsteam über das Service Desk BIT (+41 (0)58 465 88 88) oder der LRAO erstellt via RoBIT Chatbot selbständig ein Ticket. Die LRAO können sich, in dringenden Fällen währen den SLA-Servicezeiten, via Service Desk BIT (+41 (0)58 465 88 88), mit der Swiss Government PKI verbinden lassen.

Störungen mit dem BAB-Client sind ebenfalls beim Service Desk BIT zu melden.

3.2.3 Sicherheit

Bei dringenden sicherheitsrelevanten Mitteilungen und Fragen erfolgt der Kontakt zu einem Swiss Government PKI Security Officer über das Service Desk BIT (+41 (0)58 465 88 88). Für weniger zeitkritische Mitteilungen und Fragen im Bereich Sicherheit steht die E-Mailbox pki-secoff@bit.admin.ch zur Verfügung.

3.2.4 Bestellung

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 E-Mailbox pki-info@bit.admin.ch steht für diese Anliegen nicht mehr zur Verfügung.

3.3 Zutrittskontrolle

Die Einrichtungen der LRA können sich in einem Einzelbüroraum befinden. Nicht zulässig sind jedoch z.B. Sitzungszimmer, Sanitätszimmer oder ähnliche Räume, zu welchen unautorisierte Personen Zutritt haben. Die Räumlichkeiten sollten für die Antragstellenden leicht erreichbar sein und genug Privatsphäre für die Eingabe der persönlichen PIN sowie der Revokationspassphrase gewähren. Werden Grossraumbüros mit Personen ohne LRA-Funktion geteilt, muss sich im Raum ein geschützter oder abtrennbarer Teil für die LRA-Aufgaben befinden. Der Raum muss genug Möglichkeiten für das Wegsperren von LRA-Material, wie Formulare und Kundendaten aufweisen und ausreichend Privatsphäre bei der Ausstellung von Zertifikaten bieten.

3.4 Zugangskontrolle

Der Zugang zum BAB-Client mit LRA-Funktion ist durch die 2-Faktor Authentisierung geschützt. Der BAB-Client ist mit einer Diskverschlüsselung ausgerüstet. Die LRA-Applikationen sind nur mit LRAO-Berechtigungen auf dem Authentifizierungszertifikat der Klasse B zugelassen. Der Zugriff von anderen Personen, auch von anderen LRAO, auf persönliche Smartcards mit LRAO-Berechtigungen ist strikt untersagt. Entweder ist die Smartcard immer mitzuführen oder sie muss für sich allein weggeschlossen werden. Arbeitet der LRAO 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 sind die entsprechenden Zertifikate ohne Verzug sperren zu lassen. Dies kann meist durch einen LRAO der gleichen Einheit erfolgen. Ebenfalls muss der Verlust sofort dem Service Desk BIT und der Swiss Government PKI gemeldet werden.

3.5 Policy betreffend den BAB-Client mit LRA-Funktion

Für den Nutzung des BAB-Client mit LRA-Funktion gelten strenge Sicherheitsvorschriften sowie das Informationssicherheitsgesetz [GV003], die Informationssicherheitsverordnung [GV004] und E026 - Einsatzrichtlinie Arbeitsplatzsystem DTI-BK [BV003]. Es ist strikt untersagt:

- Der BAB-Client für andere Aufgaben (LRA-Funktion) als für die ausdrücklich vorgesehenen zu verwenden,
- Software eigenständig zu installieren / bestellen,
- Konfigurationsänderungen an Hardware und Software vorzunehmen.

Der BAB-Client mit LRA-Funktion ist vor dem Zugriff Dritter zu schützen.

3.6 Formulare und Kundendaten

Die von der Swiss Government PKI ausgegebenen Formulare sind zwingend zu verwenden und im Kundendossier abzulegen, 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. Die aktuellen Versionen der Formulare werden online publiziert und sind zu verwenden.

Kundendossiers (Antragsformulare, Informationsblätter, Revokationsanträge, etc.) sind verschlossen aufzubewahren (Clean Desk-Policy). Entweder ist der Raum abgeschlossen und nur für die LRAO zugänglich, oder die Dokumente sind in einem Schrank wegzuschliessen, wo sie ebenfalls nur den LRAO zugänglich sind. Jeder LRAO einer LRA muss Zugriff auf alle Kundendossiers der LRA haben.

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

3.7 Journal

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

- Ausstellung von Zertifikaten
- Revokation von Zertifikaten
- Key Recovery
- Erhalt neuer Prestaged Smartcards
- Ggf. interne Auftragsnummer (z.B. Ticketnummer Auftragserfassungssystem)
- Mutationen LRAO (neu etc.)
- Änderung des/der LRA-Standort(e)
- wesentliche Änderungen in den Prozessen (neue Formulare, neuer Laufweg, neues Archiv etc.)
- aufgetretene Fehler, Probleme und Besonderheiten bei den obigen Prozessen

LRAO-Journale können entweder handgeschrieben (s. Klasse B: LRAO-Journal der Swiss Government PKI) oder elektronisch geführt werden. Bei der elektronischen Führung müssen die jeweiligen Tages-Journale jeweils am Abend ausgedruckt, vom ausführenden LRAO unterschrieben und abgelegt werden. Alternativ können die elektronischen Journale täglich in eine PDF/A-Datei exportiert und mit dem Zertifikat der Klasse B des LRAO signiert und mit dem Zeitstempel des SG-PKI TSA versehen werden. Ebenfalls verwendet werden kann die PDF-Journal Vorlage mit den pro Zeile digital signierbaren Einträgen. Es ist grundsätzlich erlaubt, mehrere Journale pro LRA zu führen (z.B. pro LRAO, pro Amt, pro Monat usw.) sofern die Chronologie und die Lückenlosigkeit gewährleistet bleibt. Ebenfalls müssen alle LRA-Officer Zugriff auf alle Journale haben.

Bei der Führung von elektronischen Journalen müssen die Daten in einer Ablage gespeichert werden, auf die nur autorisierte Personen, also LRAO und Auditoren, Zugriff haben. Zudem ist sicherzustellen, dass die unter dem Kapitel *3.8* definierten Bedingungen eingehalten werden.

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

1. Fortlaufende Nummer des Eintrags
2. Datum
3. Kunde (Antragstellende Person / Zertifikatsinhabende Person)
4. Tätigkeit (Präfix: SZ: Standardzertifikat, FZA: Adminzertifikat, FZT: Testzertifikat, A: Ausgestellt, R: Revoziert, K: Key Recovery)
5. Bei Revokation: alte Smartcard eingezogen ja / nein
6. Visum des ausführenden LRAO

3.8 Aufbewahrungsfristen

Formulare, Kundendaten und Journale gemäss dem Kapitel *3.6 und 3.7* Journalmüssen in jedem Fall für mindestens 11 Jahre nach Ablauf des Zertifikates archiviert werden. Das Archiv muss während dieser Zeit für die LRAO zugänglich und für die SG-PKI einsehbar sein. Der Zugriffsschutz auf diese Daten muss auch bei elektronisch geführten Kundendossiers gewährleistet sein (kein Zugriff auf die Daten für nicht-LRAO).

Bei Abgabe des Amtes ist der LRAO verpflichtet, alle Kundendossiers, Journale und weiteres LRA-Material an die Person zu übergeben, die ihm in der Organisation nachfolgt oder der SG-PKI.

Bestehende Papierdokumente dürfen zur Archivierung eingescannt, als PDF/A abgespeichert, signiert und mit dem Zeitstempel des SG-PKI TSA versehen werden. Falls es sich um Einzeldokumente handelt, reicht die Signatur mit dem Zertifikat der Klasse B des ursprünglich ausführenden LRAO. Falls mehrere Dokumente digitalisiert werden (z.B. Dokumente eines ganzen Monats oder Jahres in ein einziges PDF/A), so sollen 2 LRAO das PDF/A digital signieren und damit den lückenlosen und korrekten Migrationsvorgang von Papier zu elektronisch bestätigen. Die Auffindbarkeit von Einzeldokumenten muss weiterhin gewährleistet sein. Die elektronische Aufbewahrung muss vor Zugriffen von nicht LRAO geschützt sein. Bei Digitalisierung nach diesen Vorgaben dürfen die Papierdokumente danach vernichtet werden.

3.9 Aufbewahrung prestaged Smartcards

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

3.10 Verwendung und Schutz der Zertifikate mit LRAO-Berechtigungen

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

3.11 Entsorgung

3.11.1 Clean Desk Policy

Nicht mehr benötigte Papierdokumente betreffend der LRA (Richtlinien, Checklisten, Notizen etc.) oder der Kundschaft (Zertifikatsanträge, 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 schreddern.

Dokumente, welche weiterhin benötigt werden, dürfen nicht für jeden einsehbar / offen auf den Tischen oder in öffentlich zugängigen Ablagen abgelegt werden und sind sicher zu archivieren.

3.11.2 BAB

Der BAB wird durch den Support des BIT (Service Desk) entsorgt.

3.11.3 Smartcard

Die Smartcard muss vor der Entsorgung vernichtet werden (z.B. mit einem Loch im Chip).

3.12 Regeln für PINs

Die inhabende Person von Zertifikaten verwendet PINs (Passwörter) zur Aktivierung ihrer Security Token bzw. zur Aktivierung ihrer privaten Schlüssel. Die PIN unterscheidet sich grundsätzlich vom Passwort, welches z.B. für die Anmeldung bei Applikationen verwendet wird [Quick Guide: PIN Regeln für Smardcards unter «Ausstellung (Issuing)»]. Jede zertifikatsinhabende Person wählt ihre eigene PIN aus. Die Regelung in Bezug auf die Smartcard-PIN lautet:

- *Länge:* Die PIN muss mindestens 6 Stellen lang sein.
- *Anzahl Versuche:* Die Smartcard 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 Smartcard eine neue PIN gewählt werden.
- *Einmaligkeit:* Eine PIN darf nur für genau eine Smartcard verwendet werden.

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

3.13 Revokationspassphrase

Die Revokationspassphrase besteht aus einer allgemeinen Frage mit der dazugehörigen persönlichen Antwort.

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

Die Revokationspassphrase dient dazu, die zertifikatsinhabende Person im telefonischen Verkehr mit dem LRAO, z.B. bei der Beantragung der Revokation seiner oder ihrer Zertifikate oder im PIN-Reset Prozess gegenüber dem zuständigen Service Desk zu identifizieren.

3.14 PIN-Reset und PUK-Handling

Die SG-PKI hat für Ihre prestaged Smartcards 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 Smartcard für die Entsperrung bereitgestellt wird. Der PUK wird zu keinem Zeitpunkt einer Person angezeigt.

Für das Support Personal oder die LRAO gelten folgende Grundsätze:

- Um einen PIN-Reset durchführen zu können bedarf es eines PIN-Reset-Superusers. Der PIN-Reset Superuser kann mittels einer Webapplikation ein internes Ticket für eine Smartcard eröffnen, wenn der PIN-Reset Superuser die Person als PIN-inhabende Person erfolgreich identifizieren kann. Die Identifikation darf auch telefonisch unter Verwendung der Revokationspassphrase erfolgen. Erst dann kann die PIN-inhabende Person ihre PIN bei einem sog. PRU zurücksetzen.
- Es bedarf eines PIN-Reset Users (PRU), um die Smartcard zu entsperren. Dieser startet den PIN-Reset-Wizard und bestätigt, die anwesende Person eindeutig als PIN-inhabende Person der gesperrten Smartcard identifiziert zu haben und gibt ihr die Möglichkeit die PIN neu zu setzen.
- Der PRU hat die Funktion der PIN-inhabenden Person seinen bzw. Ihren PC zu «leihen» (da die PIN-inhabende Person zu diesem Zeitpunkt keine 2-Faktor Authentisierung am PC durchführen kann, aufgrund ihrer gesperrten Smartcard). Die betroffene Person muss dazu beim PRU vor Ort sein und ihre Smartcard 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 Smartcards ist in der «Quickguide: PIN-Reset» im Detail dokumentiert.

4 Konformitätsprüfung

Die SG-PKI ist verpflichtet, die Durchsetzung der CP/CPS [KLB001] zu überprüfen. Dazu gehört besonders die Überprüfung der Einhaltung dieser Registrierrichtlinien durch die LRAO. Die Konformitätsprüfung kann durch die SG-PKI selbst oder durch eine von der SG-PKI beauftragten externen Stelle durchgeführt werden. Die LRAO sind verpflichtet bei diesen Kontrollen mitzuwirken und Einsicht in die Prozesse und Dokumente zu gewähren.

Wird diese Konformitätsprüfung nicht bestanden, kann dem Betroffenen die LRAO-Berechtigung entzogen werden. Bei besonders gravierenden Mängeln können sämtliche von diesem fehlbaren LRAO 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 für U-Accounts oder X-Accounts (User-Account)
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 Smartcard geschrieben
Es werden bei der Ausstellung drei Zertifikate, jeweils eines für Signatur, Authentifizierung, Verschlüsselung auf die Smartcard geschrieben
Key Recovery auf einer Drittkarte (Bevollmächtigung) ist nicht möglich
Key Recovery des privaten Verschlüsselungsschlüssels ist möglich
RIO-Prozess möglich
Renewal max. zwei Mal möglich

Tabelle 2: Prozess Klasse B

Klasse B Funktionszertifikat für A-Accounts (Admin-Accounts)
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 Smartcard geschrieben
Es wird bei der Ausstellung lediglich das Zertifikat für die Authentisierung auf der Smartcard geschrieben
Key Recovery auf einer Drittkarte (Bevollmächtigung) ist nicht möglich
Key Recovery des privaten Authentisierungsschlüssels ist nicht möglich
Kein RIO-Prozess vorgesehen
Renewal nicht erlaubt

Tabelle 3: Prozess A-Accounts

Klasse B Funktionszertifikat für T-Accounts (Test-Accounts)
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 Smartcard geschrieben
Es werden bei der Ausstellung drei Zertifikate, jeweils eines für Signatur, Authentifizierung, Verschlüsselung auf die Smartcard geschrieben
Key Recovery auf einer Drittkarte (Bevollmächtigung) ist nicht möglich
Key Recovery des privaten Verschlüsselungsschlüssels ist möglich
RIO-Prozess möglich
Renewal max. zwei Mal möglich

Tabelle 4: Prozess T-Accounts

5.2 Prozess Zertifikat ausstellen

Es ist zwischen zwei Ausprägungen des Ausstellungsprozesses zu unterscheiden:

- Ausstellungsprozess ohne RIO
- 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 der antragstellenden Person direkt durch den LRAO. Als Beweis scannt der LRAO das gültige Reisedokument der antragstellenden Person und allenfalls weitere notwendige Dokumente.	Persönliche Identifikation der antragstellenden Person durch den RIO. Als Beweis kopiert der RIO das gültige Reisedokument auf das korrekt ausgefüllte Antragsformular und allenfalls weitere notwendige Dokumente. Der RIO füllt die Checkliste aus und übermittelt diese Unterlagen und die unterschriebenen „Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B“ [KLB021] dem zuständigen LRAO.
Überprüfen der antragstellenden Person im Admin-Directory durch LRAO.	Überprüfen der antragstellenden Person im Admin-Directory durch RIO.
Instruktion der antragstellenden Person durch LRAO betreffend Aktivierungsdaten und deren Schutz.	Instruktion der antragstellenden Person durch RIO betreffend Aktivierungsdaten und deren Schutz.
Im Walk-In-Wizard stellt der LRAO das Zertifikat für die antragstellende Person aus.	Kontrolle/Freigabe des Antrags, danach Antragstellung für die Ausstellung der Zertifikate durch den LRAO im Walk-In-Wizard und Versand der Unseal-Ticket-Nummer (S-PIN) an die antragstellende Person oder den RIO.
Die antragstellende Person erfasst die persönliche PIN und die Daten zur telefonischen Revokation (Revokationspassphrase) im letzten Schritt des Walk-In-Wizard.	Die antragstellende Person erfasst die persönliche PIN und die Daten zur telefonischen Revokation (Revokationspassphrase) bei der Entsiegelung der Smartcard mit dem Unseal-Wizard.

Tabelle 5: Unterschied mit und ohne RIO

5.2.1 Wer kann ein Zertifikat beantragen?

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

Minderjährige Personen (z.B. Lernende) können auch Zertifikate der Klasse B beantragen, bei deren Ausstellung ist die Informationspflicht durch den LRAO besonders sorgfältig wahrzunehmen.

Die Klasse B Zertifikate eines LRAO müssen bei einem anderen LROA beantragt werden und von diesem ausgestellt werden. Ein LRAO darf in keinem Fall sich selbst ein Klasse B Zertifikat ausstellen.

5.2.2 Wie kann ein Zertifikat beantragt werden

Der LRAO, respektive die PKI-verantwortliche Person bestimmt, auf welchem Wege ein Zertifikat beantragt werden kann (schriftlich mit Formular, Remedy-MAC/DWP etc.). Grundsätzlich muss der Bestellvorgang bis 11 Jahre nach dem Ablauf des Zertifikats nachvollziehbar sein. Die SG-PKI stellt ein

Formular zur Verfügung, welches alle für die Anmeldung benötigten Daten enthält («Klasse B: Antrag für persönliche Zertifikate der Swiss Government PKI Klasse B»).

Werden Zertifikate für Ausnahmefälle beantragt (z.B., wenn die antragstellende Person 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 des LRA-Clients gelten die Schulungsunterlagen LRAO sowie die Quick Guides zu den einzelnen Wizard. Bei widersprüchlichen Vorgaben gilt die vorliegende Richtlinie.

Der LRAO geht anhand der «C*heckliste: Ausstellen von Klasse B Zertifikaten*» vor.

5.2.3.1 Eintrag im Admin-Directory überprüfen

Die antragstellende Person muss zwingend im Admin-Directory 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 A-Accounts muss mit dem Zusatz „Admin", „ADM" oder ähnlich klar gekennzeichnet sein.
   Bei Funktionszertifikaten für T-Accounts: E-Mail-Adresse des T-Accounts muss mit dem Zusatz „Test", „TST" oder ähnlich klar gekennzeichnet sein.
2. Falls mehr als 1 Eintrag vorhanden ist (gleicher Vor- und Nachname): Kann der Eintrag, auf den das Zertifikat ausgestellt wird, eindeutig durch das Namens-Suffix identifiziert werden?

Ist die antragstellende Person nicht oder nicht korrekt im Admin-Directory eingetragen, ist die Änderung durch den Admin-Directory Administrator des Amtes umzusetzen. Das Verfahren kann erst dann fortgesetzt werden, wenn die antragstellende Person korrekt im Admin-Directory eingetragen ist (in der Regel dauert die Replikation der Daten mind. eine Nacht). Der LRAO kann die Überprüfung des Admin-Directory-Eintrages z.B. im Walk-In-Wizard vornehmen.

5.2.3.2 Antragsformular überprüfen

Das Antragsformular ist auf Vollständigkeit und Korrektheit zu überprüfen.

1. Ist die antragstellende Person gemäss Kapitel *5.2.1*Wer kann ein Zertifikat beantragen? berechtigt, bei diesem LRAO einen Antrag zu stellen?
2. Stimmen die Angaben der antragstellenden Person auf dem Formular mit dem Eintrag im Admin-Directory überein?
3. Ist das Formular korrekt datiert und unterschrieben?
   Anstelle von Einzelanträgen kann vom jeweiligen HR auch eine Liste der neu eingetretenen Mitarbeitenden an den zuständigen LRAO geschickt werden. Die Liste muss mindestens dieselben Daten für die Mitarbeitenden enthalten, wie die Pflichtfelder des Antragformulars. BIT-intern steht im Remedy ein MAC für die Bestellung von Zertifikaten der Klasse B zur Verfügung.

Sowohl bei einer Erstausstellung wie auch bei jeder späteren Wiederausstellung wird ein Antragsformular benötigt.

Das Antragsformular darf auch erst am Ausstelltermin ausgefüllt und unterzeichnet werden.

5.2.3.3 Terminvereinbarung

Mit der antragstellenden Person muss ein Termin für die Ausstellung des Zertifikats vereinbart werden. Dazu wird eine E-Mail an die auf dem Antrag aufgeführte E-Mail-Adresse geschickt (Ausnahme: ADM-Accounts ohne Mailbox). Diese E-Mail sollte folgenden Inhalt haben:

1. Terminvorschlag / -vorschläge für die Zertifikatserstellung
2. Aufforderung an die antragstellende Person, 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*)
3. Aufforderung an die antragstellende Person, sich eine PIN zurecht zu legen. Die geltenden Regeln für die PIN gemäss Kapitel *3.12* werden nochmals in Erinnerung gerufen.
4. Aufforderung an die antragstellende Person, eine Revokationspassphrase vorzubereiten.
5. Kontaktdetails des LRAO für Fragen und die Lösung von Terminkollisionen

Bei Neueintritten kann die Terminvereinbarung auch durch das zuständige HR oder den zukünftigen Vorgesetzten koordiniert werden. Der antragstellenden Person sind dabei die oben aufgeführten Informationen auf jeden Fall vorgängig zu kommunizieren.

5.2.3.4 Ausstellungsprozess starten

Nach Eintreffen der antragstellenden Person startet der LRAO 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 die antragstellende Person mit dem Namen oder E-Mail-Adresse in der Ausstellapplikation gesucht und der korrekte Eintrag ausgewählt. Das Admin-Directory fungiert hier als Datenquelle.

5.2.3.5 Identität der antragstellenden Person überprüfen

Für die Überprüfung der Identität muss die antragstellende Person persönlich beim LRAO anwesend sein. Die Identifizierung muss mittels eines gültigen Reisepasses oder einer für die Einreise in die Schweiz gültigen Identitätskarte vorgenommen werden. Die Überprüfung der Identität der antragstellenden Person 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)
2. Persönliche Identifikation der antragstellenden Person durch Vergleich der Person mit 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?
    c. Stimmt die Unterschrift im Reisedokument mit derjenigen auf dem Antragsformular überein?
3. Überprüfen, ob die Angaben im Reisedokument mit denjenigen im Antrag und im Admin-Directory übereinstimmen. Insbesondere muss die Übereinstimmung von Name(n) und Vorname(n) im Dokument mit demjenigen des Admin-Directory nach den untenstehenden Regeln 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-Wizard 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" [KLB003] 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" [KLB003] nicht mit dem Reisedokument überein, sind jedoch plausibel. Die antragstellende Person hat bereits ein Zertifikat mit diesem Namen und 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. Die antragstellende Person 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 LRAO getrackt werden.

Regel 5: Die Felder «Name gem. Ausweis» und «Vorname gem. Ausweis» sind nicht ausgefüllt. «Name» und «Vorname» stimmen nicht mit dem Reisedokument überein. Es existiert kein früheres Zertifikat der antragstellenden Person.
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 (und danach im Kundendossier abgelegt) werden:

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

5.2.3.6 Plausibilisierung des Antrages

Anhaltspunkte sind unter anderem:

- Kann die antragstellende Person identifiziert werden?
- Arbeitet Sie für die angegebene Organisation?
- Ist die HR-Stelle oder die vorgesetzte Person zuständig für die antragstellende Person?

Der LRAO kann eine Ausstellung verweigern, wenn er davon ausgehen kann, dass die antragstellende Person nicht weiss, wie sie mit ihren Zertifikaten umzugehen hat. Gleiches gilt, falls sich im Gespräch die Gefahr herausstellt, dass sie sich nicht an die Richtlinien in der Benutzervereinbarung halten wird.

5.2.3.7 Smartcard vorbereiten

Es wird die Prestaged Smartcard eingesetzt. Diese Smartcards werden zentral für den Einsatz bei der SG-PKI vorbereitet und müssen deshalb nicht separat initialisiert werden.

5.2.3.8 Dokumente digitalisieren

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

Bei einer Identitätskarte ist Vorder- und Rückseite einzuscannen, beim Pass jeweils die Doppelseite mit Foto und Unterschrift. Andere Dokumente, die zur Identifikation notwendig sind, sind ebenfalls einzuscannen. Der Scan muss gut lesbar sein.

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

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

Ist kein Scanner am LRA-Client angeschlossen, kann der Scan an einem Multifunktionsgerät erfolgen und die gescannten Ausweise dürfen auf die persönliche E-Mail-Adresse des LRAO gesandt werden. Der Versand muss wenn möglich verschlüsselt sein.

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.

5.2.3.9 Information antragstellende Person über PIN und Revokationspassphrase

Die antragstellende Person wird nochmals über Sinn und Zweck der Revokationspassphrase orientiert und, falls sie sich noch keine Passphrase zurechtgelegt hat, aufgefordert, sich eine solche gemäss den Vorgaben in Kapitel *3.13* zu überlegen. Ebenfalls werden nochmals die Regeln für die PIN-Bildung gemäss Kapitel *3.12* in Erinnerung gerufen.

5.2.3.10 Zertifikate beantragen und auf Smartcard speichern

Die Smartcard der antragstellenden Person wird in den zweiten Kartenleser eingesteckt. Standardzertifikate dürfen nicht mit Klasse A Zertifikaten oder Klasse B Funktionszertifikaten auf derselben Smartcard erstellt werden. Mehrere Klasse B Funktionszertifikate (z.B. ein Administrator-Zertifikat und mehrere Test-Zertifikate) dürfen jedoch auf der gleichen Smartcard 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 Kapitel *5.2.3.8* beschrieben.

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

Die antragstellende Person wird aufgefordert, ihre persönliche PIN und die Revokationspassphrase selber einzugeben. Danach werden die Zertifikate auf die Smartcard der antragstellenden Person geschrieben und die Smartcard mit der persönlichen PIN des Users gesichert.

5.2.3.11 Erhalt quittieren lassen / Unterzeichnung der Benutzervereinbarung

Im Anschluss an die Zertifikatsausstellung wird die *«Bestätigung für Erhalt und Umgang mit der Smartcard»* mit den «Fingerprints» (eindeutige Erkennungszahl für ein Zertifikat) angezeigt. Der Druck und die Aushändigung dieses Dokumentes sind freiwillig. Die antragstellende Person muss mündlich anhand des Dokuments *«Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B»* [KLB021] auf ihre 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 für fortgeschrittene Zertifikate der Klasse B*» [KLB021] muss zum Schluss von der antragstellenden Person unterschrieben werden (sowohl bei einer Erstausstellung wie auch bei jeder späteren Wiederausstellung). Damit bezeugt sie, die Informationen gelesen und zur Kenntnis genommen und die Smartcard mit den Zertifikaten erhalten zu haben. Der LRAO vergleicht die Unterschrift auf diesem Formular mit derjenigen auf dem Antragsformular. Die *«Bestätigung für Erhalt und Umgang mit der Smartcard»* mit den Fingerprints wird nicht mehr benötigt und kann ignoriert werden. Alternativ zur Papierkopie ist dem LRAO frei gestellt die Benutzervereinbarung der antragstellenden Person elektronisch zur Verfügung zu stellen. Der LRAO muss jedoch dafür besorgt sein, die mit dem Klasse B Zertifikat signierte Version des Dokuments innerhalb von 5 Arbeitstagen zu erhalten und diese gemäss den Vorgaben im Kapitel *3.8* elektronisch zu archivieren. Erhält der LRAO die signierte Benutzervereinbarung nicht zurück, müssen die entsprechenden Zertifikate sofort revoziert werden.

5.2.3.12 Abschluss Ausstellung

Zum Abschluss werden der antragstellenden Person

- die neue Smartcard
- die nicht unterschriebene Kopie der «Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B» [KLB021]
- ihre Reisedokumente sowie die weiteren benötigten Unterlagen

ausgehändigt.

5.2.3.13 Journal führen

Die durchgeführten Aktivitäten müssen vom LRAO im LRA-Journal festgehalten werden. Dabei gelten die unter Kapitel *3.7* aufgeführten Regeln.

5.2.3.14 Gespeicherte Dateien von lokalen Systemen löschen

Falls Scans der Reisedokumente ausserhalb des Walk-In-Wizard 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 E-Mail Accounts gespeichert bleibt (siehe auch Kapitel *5.2.3.8*).

Bemerkung: Dies muss gemacht werden, weil es sich sonst um eine nicht angemeldete Datensammlung i.S. des Datenschutzgesetzes handeln würde. Die Dateien werden während des Ausstellungsprozesses in der Datenbank der Swiss Government PKI abgelegt (welche nach DSG [GV015] gemeldet ist).

5.2.3.15 Ablage Kundendossier

Der ausgeführte Antrag, die unterschriebene Kopie der *«Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B»* [KLB021] werden im Kundendossier abgelegt. Sind zusätzliche Formulare (z.B. bei Ausstellung mit Ausweis F) oder weitere Unterlagen notwendig, werden auch diese 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 abgespeichert werden, dass:

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

5.2.4 Ausstellen mit RIO

Im Prozess «Ausstellen mit RIO» delegiert der LRAO die Identifikation der antragstellenden Person und weitere Aufgaben an den RIO. Die antragstellende Person und der RIO befinden sich dabei an einem vom LRAO entfernten Ort. Der Prozess wird auch asynchroner Ausstellungsprozess genannt. Administrations- und Testzertifikate dürfen nicht über diesen Prozess ausgestellt werden.

Weitere zu befolgenden Dokumenten zu diesem Prozess sind die «*Richtlinien für den Registration Identification Officer (RIO)*» [KLB027] und die «Quick Guide Walk-In-Wizard - RIO» (unter «RIO (Registration Identification Officers)»). Bei widersprüchlichen Anweisungen gilt diese Richtlinie.

Die gesamte Dokumentenablage erfolgt durch den LRAO, der RIO führt keine dauerhafte Ablage.

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

Die antragstellende Person füllt auf dem Formular «Klasse B: RIO Antrag zur Ausstellung von Klasse B Zertifikaten» den Abschnitt 1 mit den Angaben zu ihrer Person und ihrer Organisations- und Kommunikationsdaten aus. Sie datiert und unterschreibt diesen Abschnitt.

5.2.4.2 Identifikation der antragstellenden Person durch den RIO

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

1. Die antragstellende Person meldet sich mit ihrem Identifikationsmittel (gültiger, nicht abgelaufener Reisepass oder einer für die Einreise in die Schweiz gültigen 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 der antragstellenden Person mit dem Gesichtsbild des Reisedokumentes übereinstimmt. Bei Nichtübereinstimmung verweigert der RIO die Fortsetzung des Identifikationsprozesses und meldet den Verstoss dem zuständigen LRAO. Alternative Identifikationsmittel nach Ausnahmeregelungen und die dabei anzuwendenden Prozesse sind im Kapitel *5.2.3.5* aufgeführt. Die dortige Auflistung ist abschliessend.
4. Bei Übereinstimmung übergibt der RIO der antragstellenden Person eine neue prestaged 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 die antragstellende Person darauf aufmerksam, dass diese die neue Smartcard ab sofort unter ihrer alleinigen Kontrolle behalten muss.
5. Der RIO und die antragstellende Person bestätigen mit ihrer Unterschrift in Abschnitt 2 des Antragsformulars, dass eine persönliche Begegnung und die Identifikation anhand eines gültigen Reisedokumentes stattgefunden haben und dass die antragstellende Person die bezeichnete Smartcard erhalten hat.
6. Der RIO stellt sicher, dass die antragstellende Person den Inhalt der «*Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B*» [KLB021] verstanden und eine Kopie davon erhalten hat. Eine zweite Kopie muss von der antragstellenden Person unterschrieben werden.
7. Der RIO legt die 2. Seite des Antragsformulars und das Reisedokument so auf das Kopiergerät, dass das Reisedokument mit sichtbarem Gesichtsbild auf der Kopie im vorgesehenen Feld des Antragsformulars erscheinen wird.
   IDs müssen beidseitig kopiert werden, beim Pass ist die Doppelseite mit Bild und Unterschrift zu kopieren.
8. Der RIO kopiert die 2. Seite des Antragsformulars und das Reisedokument sowie sämtliche, für die Ausstellung benötigten Zusatzformulare und Dokumente. Die antragstellende Person und der RIO unterzeichnen die 2. Seite, mit der vorher ausgefüllten 1. Seite wird nun das vollständige Antragsformular zusammengestellt.
9. Der RIO schickt die beiden unterschriebenen Dokumente (Antragsformular und unterschriebene «Benutzervereinbarung» [KLB021]), die Kopien allfälliger Zusatzdokumente sowie die ausgefüllte Checkliste an den zuständigen LRAO. Die Zustellung kann auf eine der beiden nachfolgend beschriebenen Arten vorgenommen werden:

a. Die unterschriebenen Dokumente werden per Post oder Kurier an den zuständigen LRAO geschickt.

b. Der RIO scannt die Dokumente im PDF/A Format, signiert sie mit dem persönlichen, gültigen Klasse B Zertifikat und versendet sie dann per verschlüsselter E-Mail an den zuständigen LRAO. Die Voraussetzungen für dieses Vorgehen sind:

   i. Der RIO ist im Besitz eines gültigen Klasse B Zertifikats

   ii. Der RIO hat Zugang zum öffentlichen Encryption Key des LRAO

   iii. Der RIO-Arbeitsplatz ist mit einer Scanmöglichkeit ausgerüstet

10. Führt der LRAO keine elektronischen Kundendossiers gemäss Spezifikationen in Kapitel *5.2.4.3* und wurden die Dokumente elektronisch übermittelt, so müssen die originalen Papierdokumente nachträglich per Briefpost an den LRAO zur Ablage im physischen Kundendossier geschickt werden. Der LRAO muss den Eingang überprüfen und sicherstellen.

11. Die Originale der Dokumente, die zur Identifikation benützt wurden, werden der antragstellenden Person zurückgegeben. Alle Kopien und Formulare müssen entweder dem LRAO gesandt oder vernichtet werden (schreddern). Auch digitale Kopien, zum Beispiel in der E-Mailbox, sind zu löschen und der Papierkorb ist zu leeren. Der RIO behält keine Dokumente und führt keine Kundendossiers.

5.2.4.3 Genehmigung Antrag durch LRAO und Ausstellung der Zertifikate

Nach Erhalt und Kontrolle der unter Kapitel *5.2.4.2* ausgefertigten Dokumente kann der LRAO den Antrag genehmigen und die Generierung der Zertifikate freigeben. Dazu werden die folgenden Schritte aus der Checkliste «Ausstellen mit RIO» ausgeführt:

1. Der LRAO überprüft, ob alle Dokumente beigelegt sind und das Antragsformular von einem autorisierten RIO unterzeichnet ist. Die benötigten Dokumente sind:
   - Mehrfach unterzeichnetes Antragsformular «Klasse B: RIO Antrag zur Ausstellung von Klasse B Zertifikaten»
   - Unterzeichnete «Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B» [KLB021]
   - Unterzeichnete «Checkliste RIO»
   - Weitere, im Falle einer Ausnahmeregelung verlangte Dokumente und Ausweise
2. Wurden die Dokumente elektronisch übermittelt, überprüft der LRAO, ob
   - die Dokumente verschlüsselt übermittelt wurden und
   - die Dokumente mit der gültigen Signatur des RIO elektronisch unterschrieben sind.
3. Der LRAO startet auf dem LRA-Client mit der persönlichen Smartcard den Walk-In-Wizard im RIO-Modus. Der LRAO sucht die antragstellende Person im System durch Eingabe ihres Namens oder ihrer E-Mail-Adresse.
4. Der LRAO überprüft, ob die Angaben auf dem Antragsformular mit denjenigen der Ausweiskopie und dem Eintrag der antragstellenden Person im Admin-Directory übereinstimmen (s. Kapitel *5.2.3.5*).
5. Stimmen die 3 Angaben gemäss den Vorgaben überein, so kann die Genehmigung des Antrags fortgesetzt werden, ansonsten muss der Prozess abgebrochen werden und eine Korrektur des Admin-Directory oder des Antragsformulars verlangt werden.
6. Elektronisch erhaltene Dokumente können direkt im Wizard eingebunden werden.

   Wurden die Formulare in Papierform übermittelt, scannt der LRAO das vom RIO erhaltene, ausgefüllte und unterzeichneten Antragsformular und die unterzeichnete «Checkliste RIO» sowie weitere, im Falle einer Ausnahmeregelung verlangte Dokumente und Ausweise.

Um qualitativ gute Resultate zu erzielen, sollten folgende Einstellungen verwendet werden:

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

Die Dokumente lädt der LRAO dann in den Walk-In-Wizard.

7. Der LRAO gibt die Seriennummer der an die antragstellende Person ausgehändigten Smartcard ein und stellt das Zertifikat auf dem Server (via Walk-In-Wizard) aus.
8. Der frei gegebene Antrag wird im Hintergrund in einem Ticket angelegt und an die CA zur Zertifizierung übermittelt. Die Ticketnummer wird in einem sogenannten Unseal-Dokument (pdf-Format) festgehalten, dieses kann ausgedruckt werden.
9. Der LRAO leitet das Unseal-Dokument oder den Unseal-Code («E-Ticket-Nummer») entweder direkt an die antragstellende Person oder an den RIO weiter.
10. Der LRAO trägt den Vorgang im Journal ein.
11. Der LRAO legt das unterzeichnete Formular «Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B» [KLB021] im Kundendossier ab. Wird das Dossier elektronisch geführt, muss entweder die vom RIO signierte elektronische Version abgelegt werden oder der LRAO erstellt aus den Papierdokumenten eine PDF/A Version. Das Dokument wird dann vom LRAO mit seinem persönlichen Klasse B Zertifikat unterzeichnet, bevor es abgelegt wird. Die elektronischen Kundendossiers müssen bezüglich Aufbewahrungssicherheit, Datenschutz, Aufbewahrungsdauer und Revisionsfähigkeit die Anforderungen in den Kapitel *5.2.3.14* Gespeicherte Dateien von lokalen Systemen löschenund Kapitel *3.8* dieser Richtlinien erfüllen.
12. Beide Parteien lösche sämtliche digitalisierte Kopien der ID oder des Passes aus Ihren persönlichen Ablagen (Mailbox (auch «gesendete» Kopien etc.).

5.2.4.4 Aktivierung der Smartcard durch Übertragen der Zertifikate auf die Smartcard

Als letzter Schritt müssen die Zertifikate noch auf die Smartcard der antragstellenden Person übertragen werden.

1. Nach erfolgter Zertifikatsausstellung erhält die antragstellende Person per E-Mail oder via RIO das Unseal-Dokument mit der E-Ticket-Nummer.
2. Die antragstellende Person startet den Unseal-Wizard auf einem am Netz angemeldeten Client und schiebt ihre Smartcard ins Lesegerät. Falls der Client den 2-Faktor-Login für Windows verlangt, muss für diesen Schritt ein zweites Kartenlesegerät installiert sein. Die antragstellende Person 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 die antragstellende Person aufgefordert, ihre persönliche PIN zu wählen und die Revokationspassphrase einzugeben.
4. Der Wizard speichert die Revokationspassphrase in der zentralen Datenbank ab, lädt die Zertifikate auf die Smartcard und sichert die Smartcard mit der neuen persönlichen PIN.

Damit ist die Smartcard aktiviert und kann nun von der antragstellenden Person benutzt werden.

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:

- die zertifikatsinhabende Person selbst,
- die vorgesetzten Personen der zertifikatsinhabenden Person,
- der / die PKI-Verantwortliche,
- der SG-PKI Security Officer,
- der zuständige LRAO der SG-PKI,
- der / die ISBO oder der / die ISBD bzw. die informationssicherheitsbeauftragte Person der Organisation,
- die Mitarbeitenden des für die zertifikatsinhabende Person zuständigen HR (Personaldienst).

5.3.2 Wie kann eine Revokation beantragt werden?

Zertifikatsinhabende Personen können die Revokation beim LRAO persönlich, via E-Mail oder per Telefon beantragen. Der LRAO identifiziert die antragstellende Person, z.B. über die Revokationspassphrase und plausibilisiert den Request.

Die HR-Stellen und die vorgesetzten Personen können Revokationsanträge auch als Listen (z.B. Excel-Files) an den LRAO schicken. Dies ist vor allem bei Austritten oder Wechseln von Mitarbeitenden der Fall, wobei die Revokation in die jeweiligen Austrittsprozesse zu integrieren sind. Der LRAO überprüft die Zuständigkeit. Der LRAO darf Revokationsanträge von Drittpersonen nur schriftlich entgegennehmen (signierte E-Mail, signierte Revokationsanträge). Die telefonische Revokation ist nur für zertifikatsinhabende Personen bestimmt.

Die LRAO müssen in die Austrittsprozesse ihrer Einheit eingebunden sein. Es muss sichergestellt werden, dass Zertifikate von austretenden Mitarbeitenden zeitgerecht revoziert werden. Die Revokation hat bei Rückgabe der Smartcard sofort zu erfolgen, ansonsten spätestens am 1. Arbeitstag nach Austritt.

Der LRAO, der PKI Security Officer und der oder die Swiss Government PKI-Verantwortliche können ein Zertifikat direkt im Revoke-Wizard 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
- Die Rückgabe der Smartcard (z.B. an Vorgesetzten, LRAO, HR)
- Die Beendigung des Arbeitsverhältnisses
- Die Änderung von Daten, die im Zertifikat enthalten sind (Name, E-Mailadresse, etc.)
- Der Verdacht auf Kompromittierung (bekannt werden) des privaten Schlüssels (andere Person konnte einen Dienst nutzen, z.B. eine E-Mail signieren)
- Der Verstoss gegen Richtlinien (z.B. Nicht-Befolgen der Benutzervereinbarung [KLB021])
- Der LRAO hält eine Revokation aus anderen Gründen angezeigt

5.3.4 Vorgehen

Ein Revokationsantrag ist **immer sofort** zu bearbeiten. Herrscht betreffend die Gültigkeit eines Revokationsantrags Unsicherheit (z.B. bei einem telefonischen Antrag), ist folgendes zu beachten: Das Ziel der Revokation ist es, die inhabende Person und die Organisation vor einem möglichen Schaden

durch den Missbrauch ihrer Zertifikate zu bewahren. Ein betrügerischer Revokationsantrag und nachfolgende Revokation können aber auch Schaden anrichten, indem die Dienstleistungen von der Kundschaft nicht mehr genutzt werden können oder eine Amtshandlung verhindert wird. Der LRAO hat also den potenziellen Schaden einer Nichtrevokation und einer betrügerischen Revokation abzuschätzen.

Der LRAO geht wie folgt vor:

5.3.4.1 Plausibilisieren des Antrags

Anhaltspunkte sind:

- Kann die antragstellende Person identifiziert werden? (Stimme, Telefonnummer, Revokationspassphrase)?
- Ist die HR-Stelle oder die vorgesetzte Person zuständig für die zertifikatsinhabende Person?
- Ist es der oder die zuständige ISBO oder ISBD?

5.3.4.2 Formular für Revokation

Wird ein Revokationsantrag durch Drittpersonen (also nicht der LRAO und nicht die zertifikatsinhabende Person selbst) veranlasst (vgl. hierzu Kapitel *5.3.1*), so muss der Revokationsantrag schriftlich, mittels «*Revokation Zertifikate der Swiss Government PKI Klasse B*» erfolgen. Die HR-Stellen oder die vorgesetzte Person können Revokationsanträge auch als Listen (z.B. Excel-Files) an den LRAO schicken. Wird der Antrag nicht in Papierform vorgelegt ist dabei zu achten, dass das Dokument, oder die E-Mail mit der Anlage von der antragstellenden Person signiert wurden.

Ebenso ist ein Formular für die Revokation dann notwendig, wenn die Informationen (Grund, Auftraggeber) zur Revokation nicht im Revoke-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 Revoke-Wizard auf dem LRA-Client gestartet und die zertifikatsinhabende Person gesucht. Danach werden die zu revozierende Zertifikate ausgewählt. Der LRAO erhält eine Seite mit den für das Zertifikat gespeicherten Identitätsdokumenten. Die Überprüfung der Identität der zertifikatsinhabenden Person erfolgt durch den LRAO mithilfe dieser Dokumente.

Nach erfolgter Identifizierung werden die gewählten Zertifikate revoziert. Die zertifikatsinhabende Person erhält automatisch eine Mitteilung per E-Mail über die Revokation.

Wenn möglich wird die Smartcard eingezogen, vernichtet und entsorgt gemäss Kapitel *3.11*Entsorgung.

5.3.4.4 Administrativer Abschluss

Ist ein Revokationsformular vorhanden, wird es im Kundendossier abgelegt. Wird das Kundendossier elektronisch geführt, gelten dazu die Anforderungen im Kapitel *3.8* und Kapitel *5.2.3.15*. Der Revokationsvorgang wird im Journal gemäss Kapitel *3.7* dokumentiert.

5.4 Prozess Zertifikate erneuern

Zertifikate können innerhalb ihrer Gültigkeitsdauer bis zu zwei Mal durch die inhabende Person selbstständig erneuert werden. Dieser Vorgang wird Renewal genannt. Voraussetzung ist, dass die aktuelle Version des Renewal-Wizard auf dem Client der benutzenden Person installiert ist und dass sich auf der Smartcard noch genügend Speicherplatz befindet. Da Prestaged Smartcards bereits drei

Schlüsselsätze auf der Smartcard haben, ist diese Bedingung für diesen Kartentyp in der Regel gegeben. Das Vorgehen ist dabei wie folgt:

- Starten des Renewal-Wizard auf der persönlichen Arbeitsstation mit dem noch gültigen Klasse B Zertifikat
- Die sich im Kartenleser befindliche Smartcard wird angezeigt
- Bestätigen, dass es sich um die korrekte Smartcard 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 LRAO ausgestellt werden. Das Verfahren ist das gleiche wie bei der Erstausgabe der Zertifikate.

5.5 Prozess Key Recovery eigener Schlüssel

Eine zertifikatsinhabende Person kann für ihre eigenen Verschlüsselungsschlüssel selbstständig ein Key Recovery beantragen. Das Vorgehen ist dabei wie folgt:

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

Diese identifizieren die inhabende Person der Smartcard und starten den Key Recovery-Wizard. Sie stecken die Smartcard der inhabenden Person in einen freien Kartenleser und geben die Nummer des E-Tickets ein. Danach werden der inhabende Person der Smartcard ihre 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 persönliche Smartcard der zertifikatsinhabenden Person geschrieben werden.

In ausserordentlichen Fällen kann es aber dennoch nötig sein, den oder die Encryption Keys einer Person auf einer separaten Smartcard einer berechtigten Person abzugeben. Gründe dafür können sein:

- Die zertifikatsinhabende Person ist nicht mehr für das Amt tätig
- Die zertifikatsinhabende Person ist für längere Zeit krankheitsbedingt abwesend
- Die zertifikatsinhabende Person ist verstorben
- Rechtliche Fälle

Da damit alle verschlüsselten E-Mails und Dokumente der zertifikatsinhabenden Person gelesen werden können (sofern sich auch die verschlüsselten Daten im Besitz der schlüsselhaltenden Person befinden), muss jeder dieser Fälle separat durch die SG-PKI und der rechtlichen Abteilung des BIT beurteilt werden. Zu diesem Zweck muss ein detailliert begründeter Antrag an die zuständigen Personen der SG-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 auf der Webseite 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 die antragstellende Person den «*Klasse B: Antrag für persönliche Zertifikate der Swiss Government PKI Klasse B*» ausfüllen. Das Formular kann von der Webseite der Swiss Government PKI heruntergeladen werden. Es steht die Kundschaft 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 die Kundschaft zum Voraus abgegeben werden, damit diese genügende Zeit haben, sich eine PIN sowie eine Revokationspassphrase zu überlegen. Die Kundschaft unterschreibt das Antragsformular und bestätigt somit die Korrektheit der Informationen.

Alternativ können Ämter, Klasse B Zertifikate auch via Ihr internes Auftragserfassungssystem (z.B. Remedy-MAC/DWP, Gever etc.) beantragen. Dabei ist sicherzustellen, dass die Anträge den Ausstellungen eindeutig zugeordnet werden können und die Antragsdokumentation sowie die verwendetet Evidenzen auch 11 Jahre nach dem Ablauf des Zertifikats abrufbar sind. (vgl. Kapitel *5.2.3.15* und Kapitel *3.8*).

In der Bundesverwaltung ist die Erstausgabe des Standardzertifikats in der Regel in den HR-Prozess «Eintritt neue Mitarbeitende» integriert. Die neu eintretenden Mitarbeitenden können vom zuständigen HR dem LRAO 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*Ausstellen mit RIO) wird das Formular «*Klasse B: RIO-Antrag zur Ausstellung von Klasse B Zertifikaten»* verwendet.

6.1.1 Ergänzendes Formular für antragstellende Personen mit Ausweis F

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

6.2 Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B

Das Formular «Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B» [KLB021] enthält nur die wichtigsten Informationen; es wurde speziell für die Endbenutzer erstellt. Die vollständige Information ist in der CP/CPS [KLB001] enthalten. Das Formular ist Bestandteil der auditrelevanten Dokumentation eines Ausstellungsprozesses. Das momentan noch vorhandene Formular «Bestätigung für Erhalt und Umgang mit der Smartcard» enthält die Fingerprints der Zertifikate. Am Ende des Dokumentes kann die Smartcard Nummer, falls vorhanden, eingetragen werden. Diese Nummer kann bei Problemen mit der Smartcard (Verlust oder Beschädigung) hilfreich sein. Diese Bestätigung ist nicht Bestandteil der Auditrelevanten Dokumentation eines Ausstellungsprozesses.

6.3 Formular zur Revokation

Bei der Revokation mit dem Revoke-Wizard müssen die Auftraggeber und die Gründe für die Revokation im Wizard hinterlegt werden, in diesen Fällen muss das Revokationsformular nicht ausgefüllt und nicht abgelegt werden. Andernfalls gehört das Formular zur auditrelevanten Dokumentation eines Revokationsprozesses - Vgl. hierzu Kapitel *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 die PKI-Verantwortliche oder den PKI-Verantwortlichen des BIT gestellt werden. Die dazu benötigten Unterlagen sind Bestandteil der auditrelevanten Dokumentation für das Key Recovery.

6.5 Checkliste Zertifikat ausstellen ohne RIO

Diese Checkliste «Ausstellen von Klasse B Zertifikaten» dient dem LRAO als Behelf bei der Ausstellung und muss nicht ausgefüllt oder pro ausgestelltes Zertifikat abgelegt werden.

6.6 Checkliste Zertifikat ausstellen mit RIO

Diese Checkliste «Ausstellen mit RIO» dient dem LRAO als Behelf bei der Ausstellung und muss nicht ausgefüllt oder pro ausgestelltes 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 LRAO geschickt und von diesem im Kundendossier abgelegt werden. Diese Checkliste ist Bestandteil der auditrelevanten Dokumentation eines Ausstellungsprozesses.

6.8 Checkliste Zertifikat revozieren

Diese Checkliste «Revokation von Klasse B Zertifikaten» dient dem LRAO als Behelf bei der Ausstellung und muss nicht ausgefüllt oder pro revoziertes Zertifikat abgelegt werden.

7 Verletzung dieser Richtlinien

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

8 Eskalationsverfahren

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

9 Änderungsvorschläge

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

Product Owner Trust Frontend
Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI – Trust Frontend (PS- PSC- TRU)
Eichenweg 3
CH-3052 Zollikofen
E-Mail: pki-info@bit.admin.ch

Anhang A: Dokument Änderungshistorie

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

RR Versio	Thema	Kapitel
	Checklisten – Diverse Korrekturen	Anhang A
	Formulare – Diverse Aktualisierungen und Korrekturen, neues Formular für Ausweis F	Anhang B
	Formulare – aufgrund Vollständigkeit noch LRAO-Formulare und BV und GL hinzugefügt	Anhang B
	Dokument Änderungshistorie und Stand und Inkrafttreten des Dokuments	Neuer Anhang: Anhang C
	Checklisten und Formulare angepasst	Anhang B
	Formular PIN-Reset Superuser und KRA-Antrag eingefügt in die RR	Anhang B
	Versionierungsänderung vor Abnahme	V5.2 RR
	Kap. 3.12 ‘Reparatur’ gestrichen	Ehem. 3.12
	Versionierung nach Freigabe	Versionierung
	LRA-Station durch LRA-Client oder BAB-Client ersetzt, nur noch prestaged Smartcards	Diverse Kapitel
	Geschlechtergerechte Sprache umformuliert (Officer ist ein englischer Ausdruck und wird nicht eingedeutscht, d.h. weder im Geschlecht noch Casus oder Numerus angepasst)	Gesamtes Dokument
	Unnötige Referenzen entfernt, DSG, ISG und ISV eingefügt (anstatt WIsB und BinfV)	Referenzen, Kap. 3.13, diverse Kapitel
	Diverse Definitionen, Akronyme und Abkürzungen angepasst oder hinzugefügt	Definitionen, Akronyme und Abkürzungen
	Anhang A: Prozess Checklisten und Anhang B: Formulare für Klasse B Zertifikate entfernt. Die aktuellen Dokumente sind auf der Webseite der SG-PKI zu finden, Referenzen entfernt	Anhang A, Anhang B
	Guidelines im Dokument entfernt (wird durch erweiterte Benutzervereinbarung ersetzt)	Diverse Kapitel
	Support und Erreichbarkeit SG-PKI angepasst	Kap. 3.2
	Bsp. der notwendige Journaleinträge erweitert	Kap. 3.7
	Ausführungen zur nachträglichen elektronischen Archivierung von Papierdokumenten hinzugefügt	Kap. 3.8
	Haftung des LRAO ergänzt	Kap 3.13
	Liste der Weiterbildungspunkte angepasst	Kap 3.15
	Ausstellungsprozess teilweise leicht angepasst/ergänzt	Kap 5.2
	Notwendige Einbindung der LRAO in die Austrittsprozesse ergänzt	Kap 5.3.2.3
	Einsatzrichtlinie Arbeitsplatzsystem (BAB-Client) hinzugefügt als neue einzuhaltende Richtlinie	Kap 3.5
	Div. Anpassungen beim RIO-Prozess, z.B. 2. Seite des Antragsformulars darf nicht im Kundendossier abgelegt werden	Kap 5.2.4 ff
	Neue Version des Dokumentes nach div. Anpassungen und Ergänzungen (gem. Änderungshistore) und Genderneutralität des Dokumentes	

Stand Version 7.0: 14.01.2025

Inkrafttreten der Version: 01.08.2025