Checkliste: Ausstellen von Klasse B Zertifikaten

Registrierrichtlinien der Swiss Government PKI für die LRA (RR)
→ Kapitel 5.2 Prozess Zertifikat ausstellen

V2.3 / 13.11.2025 **PUBLIC**

Nr.	Beschreibung	Referenz
Schritt 1 - Vorbereitung für Zertifikatsausstellung		
1.1	Prüfen, sind noch **genügend Smartcards** vorhanden ➢ *Bei Bedarf Smartcards bestellen* ➢ *Hinweis zur Aufbewahrung und Entsorgung von Smartcards*	• RR-Kapitel 5.2.3.7 • Bestellung Smartcards - Klasse B • RR-Kapitel 3.9 und 3.11
1.2	**Auftrag** (signiertes Mail vom HR/Linie), Ticket oder Antragsformular (vom User unterzeichnet) erhalten?	
1.3	• Ist der User zum Bezug eines Zertifikates der Klasse B berechtigt? • Sind Sie als LRAO für die Ausstellung zuständig (Ast des AdminDirectory)? Haben Sie als LRAO die korrekte Berechtigung für die Ausstellung? ➢ *Wenn der User für den Bezug nicht berechtigt ist und/oder Sie nicht für ihn zuständig sind, weisen Sie den Antrag zurück.*	• RR-Kapitel 5.2.1 • AdminDir
1.4	Sind die **Angaben im Antrag** vollständig und plausibel und stimmen der Name inklusive Suffixes und die E-Mail-Adresse im Antrag mit dem Eintrag im Admin-Directory überein? ➢ *Wenn die Angaben nicht korrekt sind, gehen Sie bitte auf Ihr HR zu und beantragen die Korrektur.*	RR-Kapitel 5.2.3.1 und 5.2.3.2
1.5	**Termin** für die Ausstellung des Zertifikats über die vom User angegebene E-Mail-Adresse vereinbaren. • Den User in der Termineinladung informieren, dass er sein gültiges Reisedokument ID/Pass mitbringen muss. • Der Termineinladung sind die Links zu den folgenden Dokumenten beizulegen ausserdem ist der User zu beauftragen, die Benutzervereinbarung zu lesen und sich mögliche Fragen zu notieren: ○ Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B (für natürliche Personen) der Swiss Government PKI ○ Quick Guide: PIN-Regeln für Smartcards und ○ Quick Guide: Mögliche Fragen für die Revokationsphrasen	• RR-Kapitel 5.2.3.3 • Identifizierung User • Klasse B - Formular- und Dokumentenbibliothek
1.6	**Kundendossier** (Digitaler- und/oder Papierordner) erstellen	RR-Kapitel 3.6

Nr.	Beschreibung	Referenz
Schritt 2 – Zertifikatsausstellung		
2.1	Entsprechen die **Angaben** im **Antrag** denen im **Reisedokument** (ID/Pass) und im **AdminDirectory**, insbesondere Name und Vorname des Users (siehe Dokument «Identitätsüberprüfung antragstellender Personen für Klasse B Zertifikate») überein? • *Wenn die Angaben nicht übereinstimmen, darf KEIN Zertifikat ausgestellt werden. Gehen Sie bitte auf Ihr HR zu und beantragen die Korrektur.*	• RR-Kapitel 5.2.3.1 und 5.2.3.6 • Identifizierung User

2.2	**Reisedokument (ID/Pass) auf Echtheit prüfen**
	• **Art des Reisedokumentes:** Handelt es sich um
	  ○ eine ID/Pass? → OK
	  ○ bei einem «Ausweis F», dürfen Sie als LRAO diesem User das Zertifikat nur ausstellen, wenn Sie vom Sicherheitsbeauftragen ihres Amt/Organisation (Bundesintern ist dies der ISBO/ISBD) das ausgefüllte «Ergänzendes Formular für Antragssteller mit Ausweis F Klasse B» vorliegen haben.
	• Ist das **Reisedokument gültig** (Ablaufdatum)?
	  ○ Wenn das Reisedokument abgelaufen ist (auch nur 1 Tag) muss der User ein neues Reisedokument bestellen Eine Smartcard wird erst mit dem neuen gültigen Reisedokument ausgestellt.
	  ○ Hinweis: Sie können beim PKI Security Officer eine Ausnahmegenehmigung via E-Mail (pki-secoff@bit.admin.ch) beantragen. Das Zertifikat darf jedoch erst nach einer Erteilung einer Ausnahmegenehmigung (verschlüsseltes E-Mail des PKI Security Officers) erstellt werden.
	• Ist das **Reisedokument echt**?
	  ○ ID-Nummer auf Vorder- und Rückseite gleich / Pass-Nummer auf jeder Seite gleich?
	  ○ Merkmale der Reisedokumente (siehe Dokumente unter Identifizierung User).
	  ○ «Ton» der ID, wenn man sie auf den Tisch fallen lässt (der Ton ist anders als z.B. bei einer Kreditkarte)
	  ○ Bei Reisedokumenten aus der EU können sie die Sicherheitsmerkmale über PRADO in Erfahrung bringen.
		• RR-Kapitel 5.2.3.5
		• Identifizierung User

2.3	**Identifikation User** Stimmen die Angaben im Reisedokument mit dem User überein? Kann der User diese Person sein? • Siehe Dokument Identifizierung User • Gesicht des Antragsstellers mit Gesichtsbild im Reisedokument vergleichen (Symmetrie des Gesichtes) • Körpergrösse	• RR-Kapitel 5.2.3.5 • Identifizierung User
2.4	**Reisedokument** (ID/Pass) und ggf. weitere benötigten Dokumente **digitalisieren** (scannen) und speichern.	RR-Kapitel 5.2.3.8
2.5	Users über die Wahl des PIN und der Revokationspassphrase (gemäss Termineinladung und den entsprechenden Quick Guides) informieren.	RR-Kapitel 5.2.3.9

Nr.	Beschreibung	Referenz
2.6	• Zertifikat auf Smartcard, mit Hilfe des Walk-In Wizards, ausstellen. • Der User muss dabei die PIN und die Revokationspassphrase selbst setzen.	RR-Kapitel 5.2.3.10
2.7	User über seine Rechten und Pflichten gemäss «Benutzervereinbarung und Nutzungsbedingungen Klasse B» informieren, seine Fragen beantworten und das Dokument vom User unterzeichnen lassen. • Siehe «Wichtigste Punkte (Seite 4-5) »	• RR-Kapitel 5.2.3.11 • Klasse B - Formular- und Dokumentenbibliothek
2.8	Stimmt die Unterschrift des Users auf der «Benutzervereinbarung und Nutzungsbedingungen Klasse B» mit derjenigen im Reisedokument überein? • *Wenn nicht, klären weshalb.*	
2.9	Die Smartcard, das Reisedokument (ID/Pass), ggf. eine Kopie des Dokuments «Benutzervereinbarung und Nutzungsbedingungen Klasse B» dem User aushändigen.	RR-Kapitel 5.2.3.12
Schritt 3 - Dokumentation (Journaleintrag und Ablage im Kundendossier)		
3.1	Eintrag im Journal vornehmen (Digitaler- und/oder Papierform)	RR-Kapitel 5.2.3.13
3.2	Ggf. gespeicherte Reisedokumente inkl. allfällige zu deren Versand benutzte Mails von lokalen Systemen löschen	RR-Kapitel 5.2.3.14
3.3	Alle Evidenzen im vorbereiteten Kundendossier ablegen. Dies sind: • Unterzeichnete «Benutzervereinbarung und Nutzungsbedingungen Klasse B» (letzte Seite) • Antrag Persönliches Zertifikat der Klasse B oder HR-Auftrag	RR-Kapitel 5.2.3.15 und 3.6
Hinweis: Aufbewahrungsfristen		
	Sie müssen 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. **Wir empfehlen eine Aufbewahrungsfrist von 15 Jahren.**	RR-Kapitel 3.6 und 6.1

Wichtigste Punkte:
Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B (für natürliche Personen) der Swiss Government PKI (V2.0)

Kapitel 1: Vollständigkeit und Genauigkeit der Informationen

- Die Inhabende Person eines Zertifikats der Klasse B (User) muss sicherstellen, dass die Informationen, die für den Ausstellungsprozess und den Inhalt des Zertifikats benötigt werden, korrekt und vollständig sind.
- Die Identität der Antragstellerin wird durch eine persönliche Identifizierung und eine Überprüfung des Reisedokuments festgestellt.

Kapitel 2: Schutz der privaten Schlüssel und der Zertifikate

- Die privaten Schlüssel der Zertifikate der Klasse B müssen durch eine PIN gesichert werden, die nur für eine Smartcard verwendet werden darf.
- Die Inhaberin muss alle angemessenen Vorkehrungen treffen, um die alleinige Kontrolle, die Vertraulichkeit und den Schutz vor Verlust und Missbrauch der privaten Schlüssel und der Smartcard zu gewährleisten.

Kapitel 3: Annahme des Zertifikats

Die Inhabende Person (User) muss den Inhalt des Zertifikats bei Erhalt überprüfen und sicherstellen, dass dieser über die gesamte Laufzeit korrekt ist.

Kapitel 4: Nutzung der Zertifikate

Die Zertifikate der Klasse B können für die

- vertrauenswürdige Signierung von Daten
- die Verschlüsselung von Daten und
- die Authentisierung von Personen verwendet werden.

Die Inhabende Person (User) muss sicherstellen, dass die Zertifikate und die privaten Schlüssel nur für autorisierte Geschäfte und unter Einhaltung der geltenden gesetzlichen Vorschriften eingesetzt werden.

Kapitel 5: Berichterstattung und Revokation

Die Inhabende Person (User)

- muss den Trust Service Provider (TSP), d.h. die Swiss Government PKI BIT unverzüglich informieren, wenn ein Verdacht auf Missbrauch oder unautorisierten Zugang zum privaten Schlüssel besteht.
- kann die Revokation persönlich oder per Telefon beantragen.

Der Trust Service Provider (TSP), d.h. die Swiss Government PKI BIT ist berechtigt im Schadensfall Daten und Informationen an andere zuständige Stellen, TSPs, Firmen oder industrielle Gruppen weiterzuleiten.

Kapitel 6: Beendigung des Einsatzes der Zertifikate
Die Inhabende Person (User) muss den Einsatz der Zertifikate nach deren Ablauf oder Revokation sofort unterlassen.

Kapitel 7: Verantwortung / Haftung
Die Inhabende Person (User)

- ist dafür verantwortlich, dass die Zertifikate Klasse B und die zugehörigen privaten Schlüssel nur unter Einhaltung der Bestimmungen in Abschnitt Nutzung der Zertifikate eingesetzt werden.
- trägt die Verantwortung für alle durch sie vorgenommenen Signaturen, Authentisierungen und Verschlüsselungen sowie für allfällige, aus pflichtwidriger Verwendung resultierende Schäden und deren Folgen.

Kapitel 8: Rechtliche Grundlagen, Gültigkeit der Dokumente und Vertragsbestandteile
Das Dokument «Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B» ist integrierender Bestandteil der rechtlichen Grundlagen.

Kapitel 9: Inhalt und Gültigkeit der fortgeschrittenen Zertifikate Klasse B
Die Zertifikate der Swiss Government PKI enthalten Informationen betreffend den Herausgeber, die ausstellende Certificate Authority, die geltende Policy, das Ausstell- und Ablaufdatum des Zertifikats, die Seriennummer des Zertifikats und Informationen betreffend der Inhabende Person (User) des Zertifikats.

Kapitel 10: Antrag und Bezug von Zertifikaten Klasse B
Für den Bezug von fortgeschrittenen Zertifikaten der Klasse B sind ein für die Einreise in die Schweiz gültiges Reisedokument, ein signierter Auftrag (z.B. Antragsformular, signiertes Mail vom HR usw.), ein persönlicher Eintrag im Admin-Directory des Bundes und eine unterschriebene Benutzervereinbarung und Nutzungsbedingungen erforderlich.

Kapitel 11: Anerkennungs- und Einverständniserklärung
Die antragstellende Person

- nimmt zur Kenntnis, dass der Trust Service Provider (TSP), d.h. die Swiss Government PKI BIT, 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.
- bezeugt mit ihrer Unterschrift, dass sie das vorliegende Dokument gelesen und verstanden hat und die darin aufgeführten Bestimmungen akzeptiert.