



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Spezialthema: RIO

01.03.2017



Rollen

RIO

Der RIO hat folgende Aufgaben:

- Antragsteller identifizieren
- Antragsteller instruieren betreffend:
 - Aktivierungsdaten
 - Schutz der Aktivierungsdaten
 - seinen Rechten und Pflichten
- Antrag prüfen
- Ausweisdokument und Antrag kopieren
- Checkliste ausfüllen
- Ausgefüllte Checkliste, unterschriebene Kopie des Antrags und des gültigen Reisedokuments, sowie die unterschriebene Nutzungsvereinbarung und Guidelines sicher dem Auftrag gebenden LRA Officer per Post, Kurier oder elektronisch zustellen.



Einführung RIO Prozess

Formulare im ausgeteilten Set:

- Einführung RIO
- Definition RIO

Wichtig: Die LRA-Officer führen „Listen“ (siehe Muster) Ihrer RIOs und melden jede Änderung der SG-PKI!

Hinweis

Der ganze RIO-Prozess ist im Dokument «Richtlinien für den Registration Identification Officer» dokumentiert. <https://www.bit.admin.ch/adminpki/02218/02219/index.html?lang=de>



Voraussetzungen für die Wahrnehmung der Rolle eines RIO

- Der RIO hat von einem LRAO den Auftrag erhalten, Antragsteller für digitale Zertifikate zu identifizieren.
- RIO kennt die Postadresse seines Auftrag gebenden LRAO und umgekehrt. Der RIO hat eine Schulung von seinem LRAO bekommen.
- Der RIO hat Zugang zu einem Kopiergerät.
- Der RIO hat Kopien der aktuell gültigen «Benutzervereinbarung und Nutzungsrichtlinien» und der «Guidelines Klasse B Zertifikaten der Swiss Government PKI».
- Dem RIO stehen (prestaged) SmartCards zur Verfügung, die er den Antragstellern aushändigen kann.
- Die SmartCard muss vom LRAO vorgängig im **Register SmartCard Wizard** registriert worden sein, falls diese nicht prestaged sind.
- Der RIO hat Kopien der aktuell gültigen Checkliste RIO. (Im Dokument Richtlinien für den RIO integriert, publiziert auf:
<https://www.bit.admin.ch/adminpki/02218/02219/index.html?lang=de>



Identifikation

Die Identifikation der Teilnehmer

Physische
Person \equiv
Lichtbild im
Dokument

Pass / ID ist
gültig



Die Angaben
sind korrekt





Identifikation

Was muss der LRAO beachten?





RIO – Prozess für RIO (RR für RIO)

1. Antrag ausfüllen / Check der Kunden- Angaben

Der Kunde, sein HR oder die Linie füllen ein Formular für die Aushändigung eines Klasse B Zertifikates via RIO aus. Der Antrag muss nur im 1. Teil ausgefüllt werden und muss vom Kunden unterschrieben sein. Der Antrag wird dem RIO per Mail oder per Post zugestellt, bzw. wird vom Antragsteller zum RIO mitgenommen.

Der RIO überprüft die Angaben im Anmeldeformular mittels der Einträge im Admin-Directory des Bundes und überprüft die Angaben auf dem offiziellen Reisedokument des Kunden (ID/ Pass).

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

RIO Antrag Klasse B
Formular zur Übermittlung der Antragstellerinformationen an den LRAO
1.0, 01.06.2016

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

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

Name, Vorname:

Departement/ Kanton/ Amt:

E-Mailadresse:

Telefonnummer:

Ort, Datum: Unterschrift: *B. Musterberg*

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

Der RIO teilt dem Antragsteller die SmartCard mit folgender Erkennungsnummer (Seriennummer) zu:

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

RIO:	Antragsteller:
Name, Vorname: (in Blockbuchstaben) <input type="text"/>	S/N des Ausweises: <input type="text"/>
Ort / Datum: <input type="text"/>	Ort / Datum: <input type="text"/>

Stimmen die Angaben überein, fährt er mit der persönlichen Identifizierung fort



RIO – Prozess für RIO (RR für RIO)

2. Identifizierung des Kunden

- Hat ihn die persönliche Identifikation überzeugt, schreibt er auf dem Formular die **Nummer des Ausweises** auf, mit dem sich der Kunde identifiziert hat. *(Konnte er den Antragsteller nicht ohne Zweifel identifizieren, verweigert der RIO die Fortsetzung des Identifikationsprozesses und meldet den Verstoß dem Auftrag gebenden LRAO.)*

3. Aushändigen der SmartCard

- Danach händigt er dem Kunden eine vorbereitete (prestaged oder registriert) Karte aus, die er von seinem LRAO erhalten hat. Die Seriennummer der Karte schreibt der RIO auf das Formular. Er informiert den Antragsteller, dass dieser die Smartcard ab diesem Zeitpunkt **unter seiner alleinigen Kontrolle** behalten muss.

4. Bestätigung

- Danach bestätigt der RIO mit seiner Unterschrift, dass die persönliche Identifikation erfolgt ist und übergibt dem Kunden das Formular zur Gegenzeichnung und Bestätigung des Kartenerhalts.

E-Mailadresse: brigitte.musterberg@eaz.admin.ch
Telefonnummer: 789 65 42
Ort, Datum: Bern, 10.01.2017 Unterschrift: B. Musterberg

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

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

Der RIO teilt dem Antragsteller die SmartCard mit folgender Erkennungsnummer (Seriennummer) zu: EB739C027E467829A !

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

RIO:	Antragsteller:
Name, Vorname: <u>Mario Kontroller</u> (in Blockbuchstaben)	S/N des Ausweises: <u>CHE89761234000</u>
Ort / Datum: <u>Bern, 15.01.2017</u>	Ort / Datum: <u>Bern, 15.01.2017</u>
Unterschrift: <u>M. Kontroller</u>	Unterschrift: <u>B. Musterberg</u>

3 Vereinbarungs- und Nutzungsbedingungen
Der RIO stellt sicher dass der Antragsteller den Inhalt der Vereinbarungs- und Nutzungsbedingungen zu den



RIO – Prozess für RIO (RR für RIO)

5. Nutzungsbedingungen und Guidelines zum Zertifikat der Klasse B

Der RIO muss nun dem Kunden seine Rechten und Pflichten mitteilen. Hierfür muss er Kopien der aktuellen «Benutzervereinbarung und Nutzungsrichtlinien» und der «Guidelines Klasse B Zertifikaten der Swiss Government PKI» parat halten und diese dem Kunden erklären.

Der Kunde muss nun die «Benutzervereinbarung und Nutzungsrichtlinien» im Doppel unterschreiben.

3.

3 Vereinbarungs- und Nutzungsbedingungen

Der RIO stellt sicher dass der Antragsteller den Inhalt der *Vereinbarungs –und Nutzungsbedingungen zu den Klasse B Zertifikaten der Swiss Government PKI* verstanden und eine Kopie davon erhalten hat. Eine zweite Kopie muss vom Antragsteller unterschrieben und vom RIO dem LRA-Officer, zusammen mit diesem ausgefüllten Dokument, inklusive den Kopien der Reisedokumente, zugestellt werden.

4 Kopie des Reisedokumentes



Vorgaben

Guidelines zu den Zertifikaten der Klasse B

**Guidelines zu Klasse B Zertifikaten der S
Erläuterungen zum Bezug und Einsatz von Klasse B
Government PKI**
V0.3, 25.01.2017

1 Zweck von Klasse B Zertifikaten

Zweck

Die Zertifikate der Klasse B sind im Rahmen des Marktmodell Identitäts- und Zugangsverwaltung (IAM) definiert. Klasse B verwendet werden.

- Vertrauenswürdige Signierung von Daten. Dadurch wird die sichergestellt.
- Verschlüsselung von Daten. Die Vertraulichkeit der Daten wird sichergestellt.
- Authentifizierung von Personen. Das Zertifikat stellt den prüfbar, eine gesicherte Identität des Inhabers zur Verfügung.

Durch erweiterte Prüf- und Sicherheitsmechanismen während B Zertifikate wird die Identität des Zertifikatinhabers auf einer Ausgabe von Klasse B Zertifikaten erfolgt immer persönlich und mittels eines gültigen Reisedokumentes.

Ausgeschlossener Zweck

Klasse B Zertifikate erfüllen ausschliesslich die oben genannte Aufschlüsse, Versicherungen oder Garantien. Insbesondere g dass der Inhaber im Umgang mit dem Zertifikat korrekt und le Des Weiteren garantieren Klasse B Zertifikate nicht, dass:

- Der im Zertifikat genannte Inhaber aktiv in die Geschäftstät
- Der im Zertifikat genannte Inhaber sich an die geltenden ge
- Der im Zertifikat genannte Inhaber vertrauenswürdig ist und
- Der im Zertifikat genannte Inhaber die fachliche, technische bestet, dieses Zertifikat korrekt einzusetzen.

2 Qualität der Klasse B Zertifikate

Die Swiss Government PKI (SG-PKI) bestätigt zum Zeitpunkt des folgende Tatsachen:

- Rechtlich gültige Existenz:** Der im Klasse B Zertifikat gen und verfügt über einen persönlichen Eintrag im AdminDir.
- Identität:** Der Name des im Klasse B Zertifikats genannten gültigen Reisedokument überein.

3 Policies

Alle geltenden gesetzlichen Vorgaben, Policies (inkl. der fiktaten sind im Internet auf der Website der SG-PKI public: pkis02240/00367/05012/index.html?lang=de

4 Inhalt und Gültigkeit des Klasse B Zertifikates

Inhalt

Das Klasse B Zertifikat der SG-PKI enthält Informationen

- Herausgeber und ausstellender CA
- Informationen über die Root CA der ausstellenden CA
- Informationen über die geltende Policy
- Ausstellungs- und Ablaufdatum des Zertifikates
- Serialnummer des Zertifikates
- Informationen betreffend der CRL und dem OCSP
- Informationen betreffend der Audatoren der CA
- Informationen betreffend den Inhaber des Zertifikates:
 - Common Name des Inhabers
 - E-Mail-Adresse
 - UPN

Gültigkeit

Das Klasse B Zertifikat der Swiss Government PKI ist ma lauf der 3-Jahres Frist maximal zwei Mal vom Inhaber sel ert werden. Nach Ablauf der 3. Gültigkeitsperiode muss d Agency Officer ein neues Zertifikat mit persönlicher Neui tomatische Erneuerung des Zertifikates steht dem Inhaber

5 Bezug von Klasse B Zertifikaten

Bezug

Für den Bezug von Klasse B Zertifikaten der SG-PKI sind nötig:

- Ein für die Einreise in die Schweiz gültiges Reisedoku
- Ausgefülltes und (elektronisch) signiertes Antragsform PKI, oder eine Anmeldung über die Linie des Amtes, b Internem Prozess.

6 Schutz des privaten Schlüssels und des Zertifikates

Übertragbarkeit

Das Klasse B Zertifikat ist immer persönlich und nicht übertragbar. D der Inhaber werden sowohl im Zertifikat wie auch bei der SG-PKI ge

PIV/PUK

Der PIV-Code für Ihre SmartCard muss unabhängig von den Passwort bewahrt werden. Er muss nicht regelmässig geändert werden, aussie docht, dass ein Dritter Kenntnis des PIN-Codes erlangt hat.

Das Zertifikat (und somit der Zertifikatsträger /Medium, SmartCard, mind. 6-stelligen PIN gesichert werden, wobei rein numerische PINs sind. Um den Missbrauch der eigenen elektronischen Identität zu ver Däten bekanntgegeben werden.

Der PUK der SmartCard muss mindestens 8-stellig, nach den oben g den.

Meldepflicht

Ein allfälliger Verlust der SmartCard muss vom Inhaber umgehend d IT-Senicoorganisation gemeldet werden. In der Folge werden die bevozielt und die Sperrung auf einer öffentlichen elektronischen Sperr SmartCard wieder gefunden werden sollte, bleiben die Zertifikate ge Uemittelbar nach erfolgter Sperrung kann beim zuständigen LRAO d Klasse B Zertifikates beantragt werden. Der Prozess der Ausstellung entspricht der Erstaussstellung.

7 Identifikation

Die persönliche Identifizierung des Antragstellers wird durch die LRA Officer) der Klasse B der SG-PKI bei der Erstaussstellung und spätere tigkeitperiode (nach maximal 9 Jahren) sichergestellt. Bei einer dez katen der Klasse B wird die persönliche Identifizierung von einem Di (Registration Identification Officer) übernommen, der die Bestätigung nung dem LRAO zur Freigabe des Antrages weiterleitet.

Verifizierung

Um die antragstellende Person zu verifizieren, wird das Reisedokument Gültigkeit, Richtigkeit und Echtheit überprüft. Die LRAOs sind zudem merkes mit der vor ihnen stehenden Person zu vergleichen. Ebensoj lung eines persönlichen Zertifikates plausibilisiert (Person arbeitet t tag zugewiesenen Organisationseinheit und benötigt das Zertifikat t rtragsteller ist berechtigt, ein Zertifikat zu beantragen).

Verbindlichkeit

Das Antragsformular (oder der interne Prozess zur Bearbeitung), di ment «Benutzervereinbarung und Nutzungsbedingungen Klasse B u bet und (digital) unterschrieben werden.

8 Inhalt des Zertifikates

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

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

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

9 Akzept/ Bestätigung für Erhalt der SmartCard

Mit Ihrer Unterschrift bestätigen Sie:

- Die Korrektheit der im Zertifikat gespeicherten Daten.
- Den Erhalt der SmartCard.
- Diese Guidelines gelesen und mit dem LRAO besprochen zu haben. Allfällige Fragen wurden vom LRAO verständlich beantwortet.
- Die Rechte und Pflichten in diesem Dokument verstanden und akzeptiert zu haben.
- Die hier beschriebenen Funktionen umzusetzen.

Zusätzliche Fragen können an die Swiss Government PKI unter der Mailadresse pkis02240@bt.admin.ch gestellt werden¹.

CommonName (CN): _____


Ausstellungsdatum: _____ **Unterschrift:** _____

¹ Die hier beschriebenen Funktionen umzusetzen.



Vorgaben

Benutzervereinbarung und Nutzungsbedingungen Klasse B

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

INTERN

Benutzervereinbarung und Nutzungsbedingungen Klasse B
Für persönliche, fortgeschrittene Zertifikate der Swiss Government PKI der Bundesbehörden der Schweizerischen Eidgenossenschaft

0.2. 25.01.2017

Die Swiss Government PKI des BIT, in ihrer Rolle als Certification Service Provider (CSP), betreibt im Auftrag des ISB (Informatiksteuerungsorgan des Bundes) die PKI (Public-Key-Infrastruktur) der Bundesbehörden der Schweizerischen Eidgenossenschaft. Die Zertifikate der Klasse B sind im Rahmen des Marktmodells «SD005 - Marktmodell Standarddienst: Identitäts- und Zugangsverwaltung (IAM)» definiert. Bezug und Nutzung der Klasse B Zertifikate der Swiss Government PKI unterliegen den Bestimmungen dieses Dokuments. Diese werden durch die Swiss Government PKI (SG-PKI) jährlich den jeweils geltenden gesetzlichen Vorschriften und den normativen Anforderungen an Public Key Infrastrukturen angepasst. Letztere bilden integrierenden Bestandteil dieser Benutzervereinbarung und Nutzungsbedingungen. Die jeweils gültige Version ist auf <https://www.bit.admin.ch/admin-bit/07240/00241/056072/06993/in dex.html?lang=de> publiziert. Alle Inhaber werden über die Publikation einer aktualisierten Version dieses Dokuments per E-Mail informiert.

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

Vollständigkeit und Genauigkeit der Informationen

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

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

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

Schutz des privaten Schlüssels und des Zertifikats

Der Inhaber verpflichtet sich dazu, alle angemessenen Vorkehrungen zu treffen, um die alleinige Kontrolle, die Vertraulichkeit und den Schutz vor Verlust und Missbrauch des privaten Schlüssels und der allfällig damit verbundenen Aktivierungsdaten und Medien zu gewährleisten. Der private Schlüssel des

1 Die männliche Form (Inhaber) wird in diesem Dokument der besseren Leslichkeit halber angedeutet, um sowohl für die weibliche und das männliche Geschlecht zu gelten.

und Nutzungsbedingungen Klasse B

INTERN

und darf nur im Zusammenhang mit dem Zertifikat und nur für den im Zertifikat festsignatur, Authentifizierung, Verschlüsselung) eingesetzt werden. Er darf auf keinen Dritten zugänglich gemacht werden. Der Inhaber haftet für jeden Schaden, der aus dem Gebrauch des privaten Schlüssels und der allfällig damit verbundenen Aktivierungsdaten entstanden ist.

Es ist dem Inhaber ausdrücklich zu empfehlen, das Zertifikat bereits bei einem konkreten Verdacht auf Missbrauch oder unzulässige Nutzung zum privaten Schlüssel ohne Vorinformation zu revozieren.

Revoziertes Zertifikates

Der Inhaber verpflichtet sich, sicher, dass ihm Inhalt, Zweck und Wirkung des Einsatzes des Klasse B Zertifikates verpflichtet sich, das Klasse B Zertifikat und dessen privaten Schlüssel nur für autorisierte (Geschäfte) und unter Einhaltung aller geltenden gesetzlichen Vorschriften sonstigen dieses Dokuments einzusetzen.

Revoziertes Zertifikat und Revokation

Der Inhaber verpflichtet sich, sich zu dem Zeitpunkt, das Zertifikat und den dazugehörigen privaten Schlüssel unverzüglich zu revozieren und beim CSP die Revokation zu verlangen, wenn:

- er einen begründeten Verdacht besteht, dass mit dem Zertifikat verdächtige Aktivitäten (Missbrauch von Daten, des Signaturzertifikates oder des Verschlüsselungszertifikates) unterzogen wurden;
- die Informationen im Zertifikat nicht mehr korrekt oder ungenau sind, oder es in naher Zukunft zu einer Kompromittierung kommen;
- er der Ansicht ist, dass das CSP ist bei Verdacht auf Kompromittierung oder Missbrauch des Zertifikates zu leisten.

Der Inhaber ist aus datenschutzrechtlicher Sicht erlaubt, kann der Person, die den Inhaber, das Zertifikat und weitere in unmittelbarem Zusammenhang stehende andere zuständige Stellen, CSPs, Firmen und industrielle Gruppen weiterleiten, wenn:

- es sich um eine Person handelt, die das Zertifikat einsetzt, als Quelle verdächtigter Aktivitäten identifiziert wird;
- es sich um eine Person handelt, die das Zertifikat einsetzt, als Quelle verdächtigter Aktivitäten identifiziert wird, die, welche das Zertifikat beantragt, nicht identifiziert oder verifiziert werden kann;
- es sich um eine Person handelt, die das Zertifikat einsetzt, als Quelle verdächtigter Aktivitäten identifiziert wird, die, welche das Zertifikat beantragt, nicht identifiziert oder verifiziert werden kann;

Der Inhaber verpflichtet sich, das Zertifikat aus weiterführenden Gründen als vom Inhaber angegeben (wie z.B. Kompromittierung, Diebstahl, etc.) revoziert zu werden.

Die Revozierungen betreffend der Revokation werden durch den CSP aus Gründen der Nachvollziehbarkeit dokumentiert.

Einsatz des Zertifikates

Der Inhaber verpflichtet sich dazu, den Einsatz des Zertifikates nach dessen Ablauf oder Revokation (grund einer Kompromittierung) sofort zu unterlassen.

Unterschrift: _____

31

Das Klasse B Zertifikat und die zugehörigen privaten Schlüsseln in Abschnitt «Nutzung des Zertifikates» dieses Dokuments diese Vorgabe hat eine Revokation und weitere administrative Folgen. Der Inhaber trägt die Verantwortung für alle durch ihn eingeleiteten Sicherungen und Verschlüsselungen sowie für allfällig daraus resultierenden Schäden.

Erklärung

Der CSP das Zertifikat bereits bei einem begründeten Verdacht auf Missbrauch oder anderen Bestimmungen dieses Dokuments oder eines sonstigen Bestimmungungen unverzüglich revoziert.

Der Inhaber verpflichtet sich, das Zertifikat und dessen privaten Schlüssel nur für autorisierte (Geschäfte) und unter Einhaltung aller geltenden gesetzlichen Vorschriften sonstigen dieses Dokuments einzusetzen.

Unterschrift: _____



RIO – Prozess für RIO (RR für RIO)

6. Reisedokument kopieren und Seiten unterschreiben

Nun muss auf der Rückseite des Antragsformulars die Kopie des Reisedokumentes erstellt werden. Identitätskarten müssen zwingend beidseitig kopiert werden. Passkopien mit den Seiten des Fotos, der Unterschrift und des Gültigkeitsdatums (alle benötigten Seiten!)

Die Rückseite, sowie zusätzlich benötigte Seiten müssen nun von beiden Parteien mit Ort, Datum und Unterschrift versehen werden.

4.

4 Kopie des Reisedokumentes

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



Spezialthemen

RIO – Prozess für RIO (RR für RIO)

2.5 Unterzeichnung aller Seiten

RIO Antrag Klasse B NICHT KLASSIFIZIERT

[Reise/ Identitätsdokumente zum Kopieren hier auflegen]

RIO: _____ **Antragsteller:** _____
Ort / Datum: _____ Ort / Datum: _____

Unterschrift: _____ **Unterschrift:** _____

Status: Freigegeben
Version: 1.0, 01.06.2016 2/2

5.



RIO Antrag Klasse B NICHT KLASSIFIZIERT

Musterdokument

RIO: _____ **Antragsteller:** _____
Ort / Datum: Bern 15.01.2017 Ort / Datum: Bern, 15.01.2017

Unterschrift: M. Kontroller **Unterschrift:** B. Musterberg

Status: Freigegeben
Version: 1.0, 01.06.2016 2/2



Spezialthemen

RIO – Prozess für RIO (RR für RIO)

7

4 Checkliste für den RIO

V 2.0

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

RIO Name/ Vorname	Organisationseinheit:	Ort, Datum:
-------------------	-----------------------	-------------

Unterschrift RIO: _____



RIO – Prozess für RIO (RR für RIO)

8. Versand

- Nun sendet der RIO den vollständigen Antrag an seinen LRAO. (Post oder signierter und verschlüsselter Mail)
- Der vollständige Antrag beinhaltet:
 - Das vollständig ausgefüllte Antragsformular mit Unterschriften, Seriennummer der Karte, Seriennummer des Ausweisdokumentes, Kopie des Ausweisdokumentes und die Unterschriften vom RIO und dem Kunden auf allen Seiten, die benötigt wurden.
 - Die unterzeichnete Kopie der «Benutzervereinbarung und Nutzungsrichtlinien»
 - Die ausgefüllte und unterzeichnete Checkliste für den RIO

Hinweis

Der RIO selbst ist nicht berechtigt, Personen-Daten auf Papier, oder elektronisch aufzubewahren!



RIO – Prozess für RIO (RR für RIO)

9. Token Unseal

- Dem RIO steht es frei, ob er dem Kunden beim Unsealing der Karte behilflich sein will oder nicht.
- Er muss dafür auf die Antwort des LRAO warten, damit er die Karte mit dem Kunden entsiegeln kann. Hat er vom LRAO Bericht bekommen, dass alles bereit ist, so kann der LRAO, statt dem Kunden persönlich, die Unseal-Ticket-Nummer (S-PIN) dem RIO übergeben.
- Mit der S-PIN und dem Unseal-Wizard kann nun die Karte **im Beisein des Kunden** entsiegelt werden. Der Kunde kann dann im Unseal-Prozess die eigene PIN der Karte eingeben.

Hinweis

→ Siehe Anleitung Token-Unseal Wizard:

<https://www.bit.admin.ch/adminpki/00240/00367/00820/06361/index.html?lang=de>



REGISTER SMARTCARD



Register SmartCard

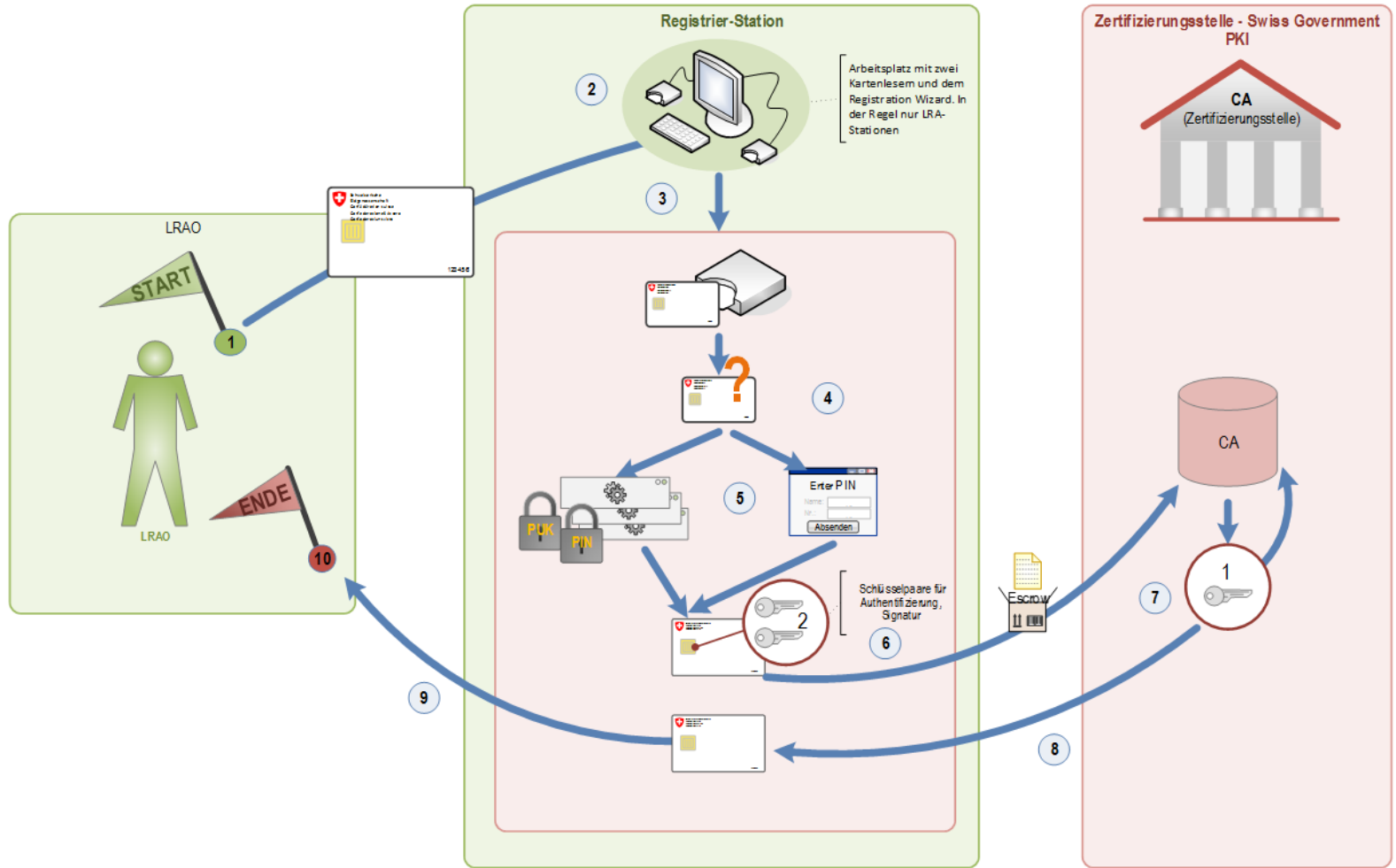
- Erfassen von Smartcards in der zentralen Datenbank der SG-PKI um diese mit den neuen Prozessen benutzen zu können.
- Beim RIO-Prozess muss die Karte vor der Ausstellung der Zertifikate registriert sein, damit das für die Entsiegelung benötigte Ticket erstellt werden kann.
- Der Wizard unterscheidet Fabrikneue Smartcards (Typ A) und Smartcards, die bereits durch ein separates PUK-Verwaltungssystem initialisiert wurden (Typ B).
 - Beim Typ A wird zuerst die Karte initialisiert. Dabei werden PUK und ein Random-PIN gesetzt.
 - Für Typ B Karten wird vom LRAO die Eingabe der Initial-PIN der Karte verlangt.



Prozesse Register SmartCard

Smartcard registrieren (Non-prestaged Smartcard)

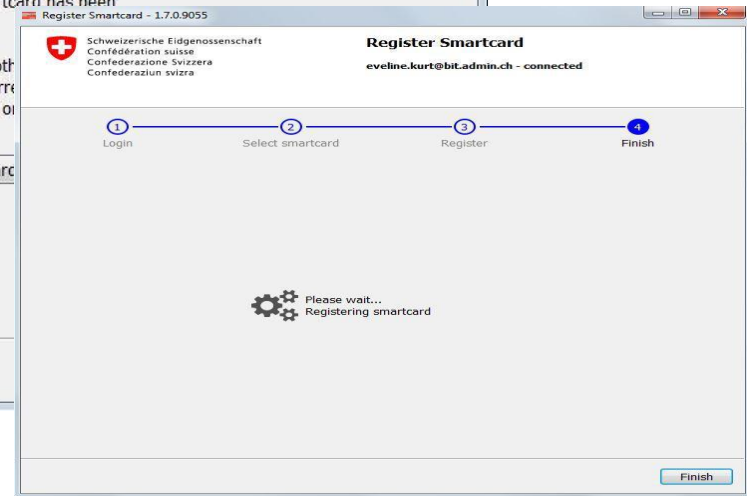
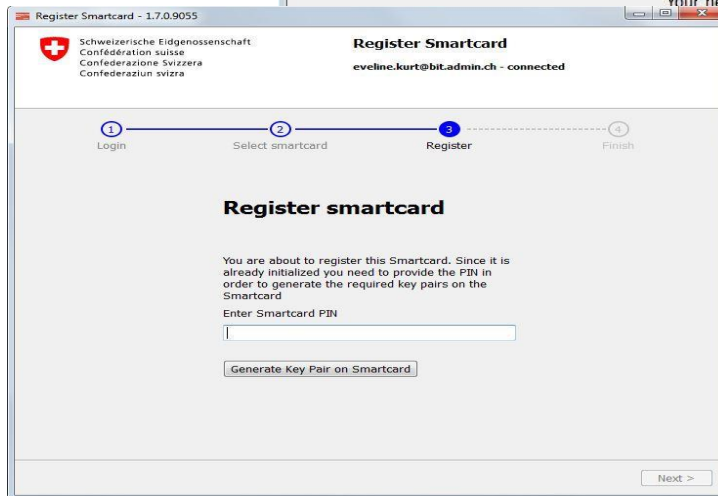
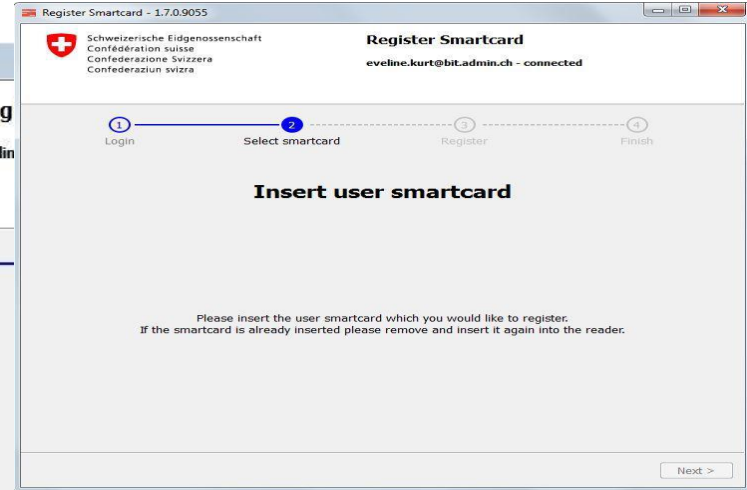
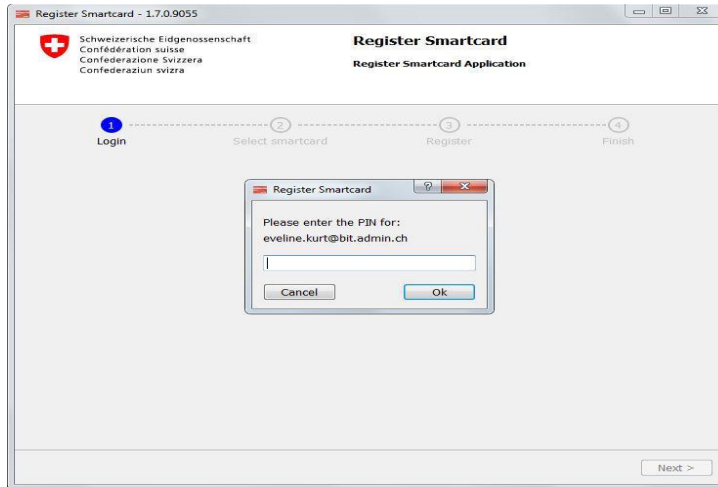
ID: SGPKI-CLB-M00.03 S





Prozesse

Register SmartCard Wizard





Prozesse

Register SmartCard (Ausstellung mit RIO, Ablauf beim LRAO W-I-W)

The screenshots illustrate the 'Walk In Wizard' process for smartcard registration. The steps are:

- Richtlinie auswählen**: Selecting a policy, such as 'Class B pre-staged (BV)'. A 'RIO-Antrag' checkbox is visible.
- Benutzer suchen**: Searching for a user.
- Benutzer auswählen**: Selecting a user.
- Dokument laden**: Loading a document.
- Smartcard Seriennummer**: Entering the smartcard serial number.
- Fertigstellen**: Finalizing the process.

The final screen displays the activation code: **Kopieren des Aktivierungscodes 1FC6-9F2A-E8C2-99D9**.



TOKEN-UNSEAL



SmartCard Entsiegeln (Token- Unseal)

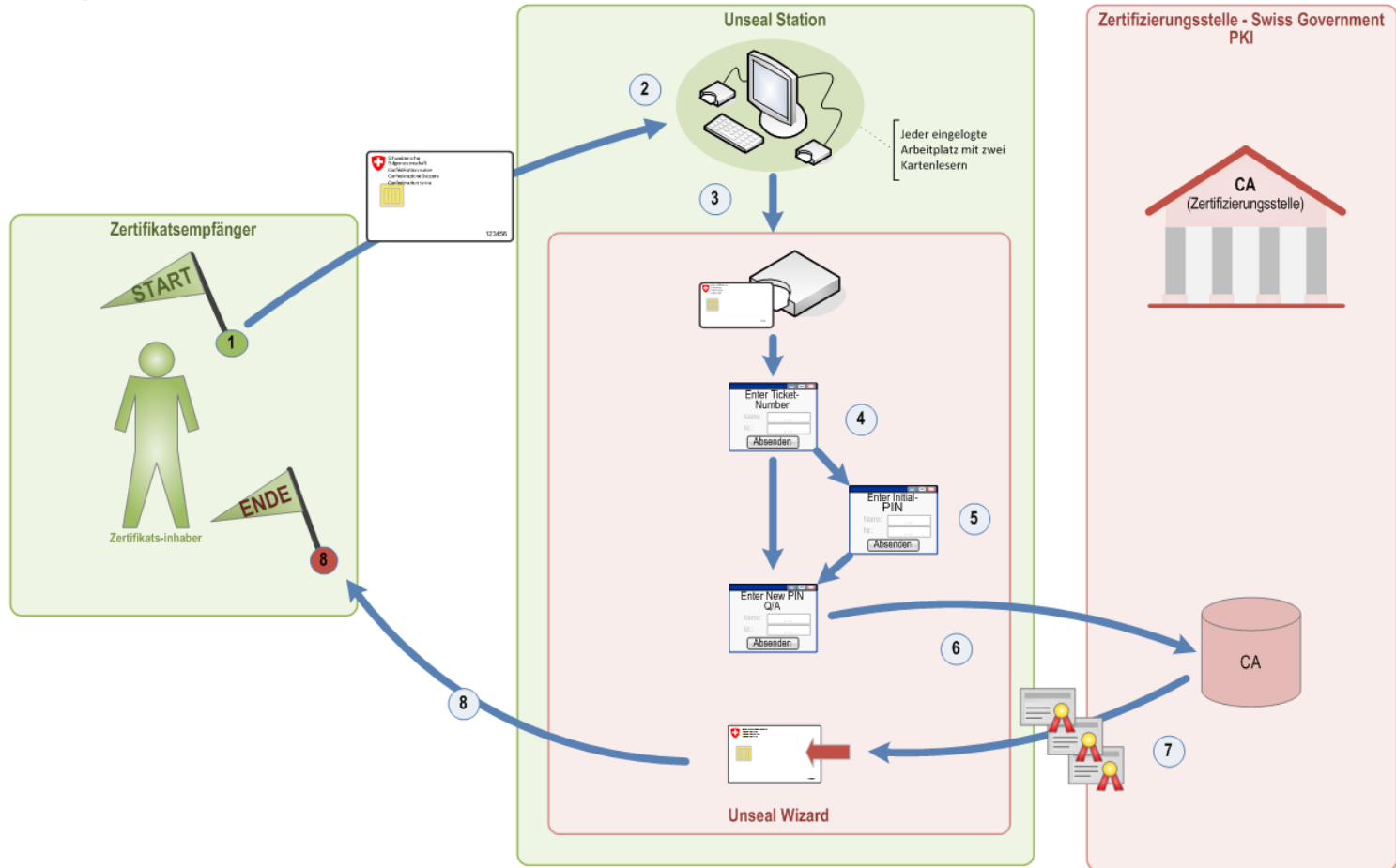
- Eine Entsiegelung der Karte ist bei einer asynchronen Ausstellung (RIO) notwendig
- Erst bei der Entsiegelung werden die Zertifikate zu den Schlüsseln erstellt
- Durch die Entsiegelung der Karte wird eine persönliche PIN auf die Karte generiert.
- Der Aktivierungs-Code ist dafür notwendig



SmartCard Entsiegeln (Unseal)

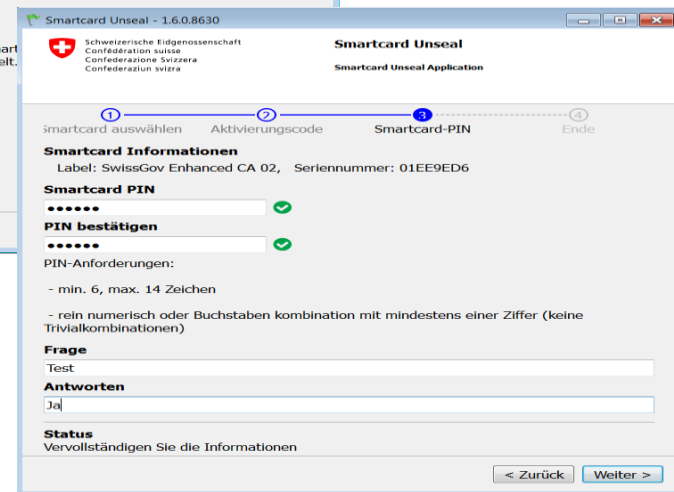
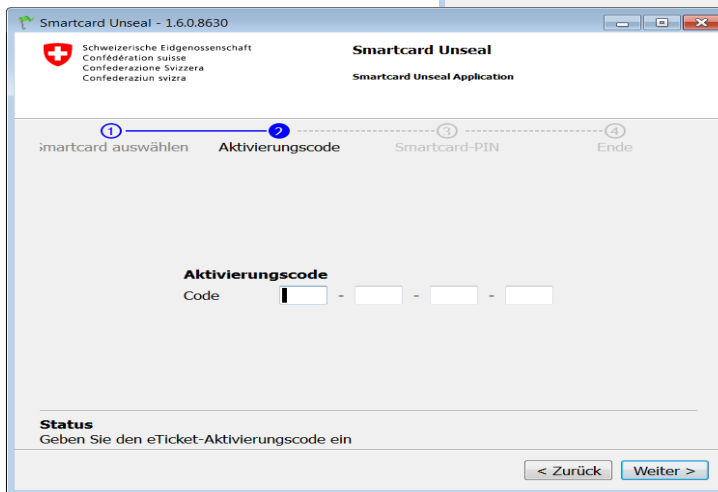
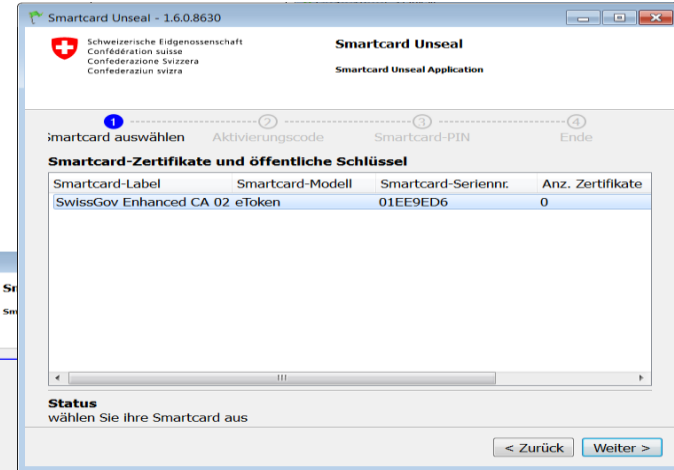
Smartcard entsiegeln

ID: Zeichenblatt-1





Prozess Token Unseal Wizard





MÖGLICHE SZENARIEN



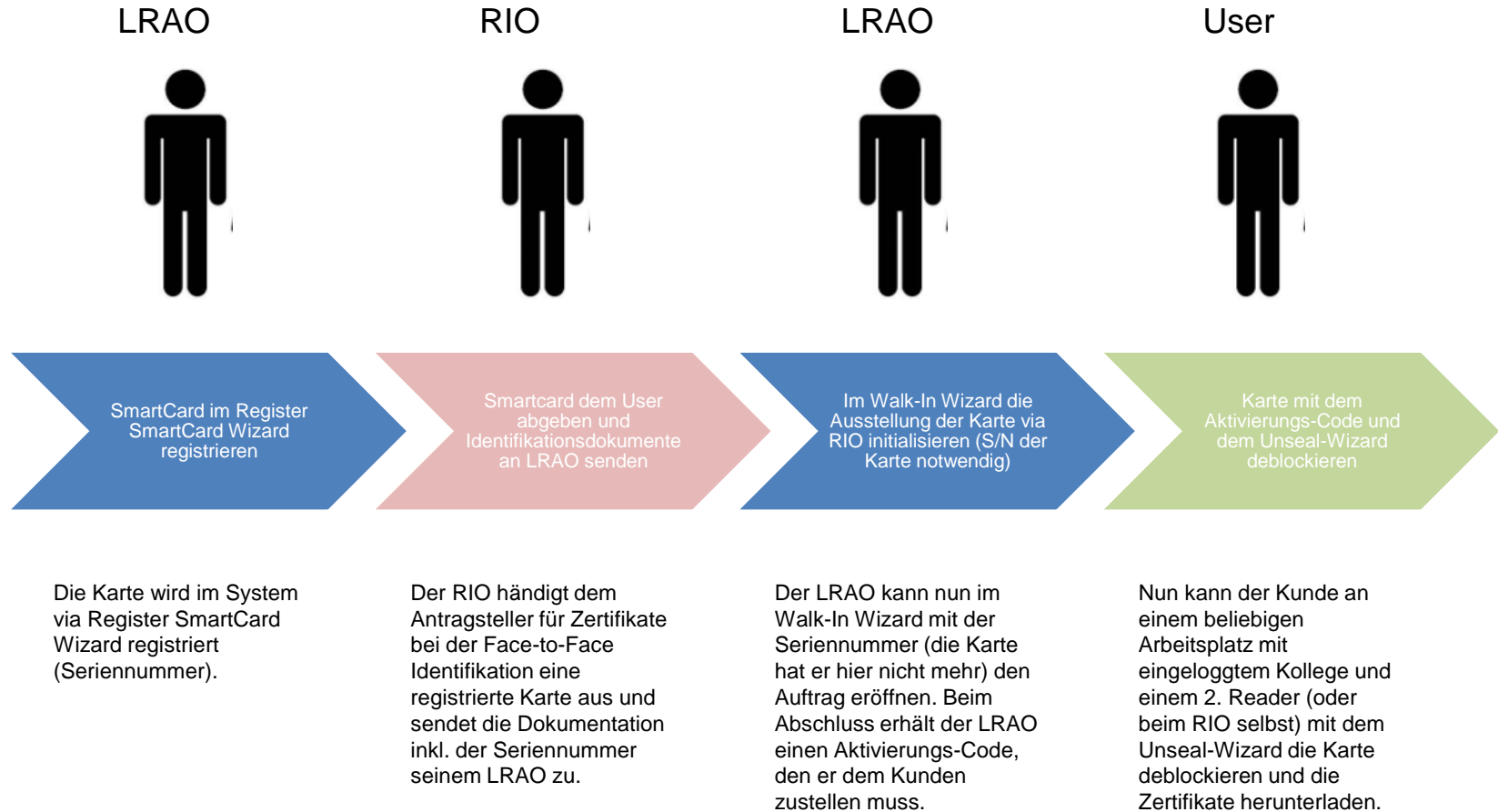
Prozesse

Workflow 1: Klasse B Standardzertifikat mit Fabrikneuer Karte, PUK-Management im BIT



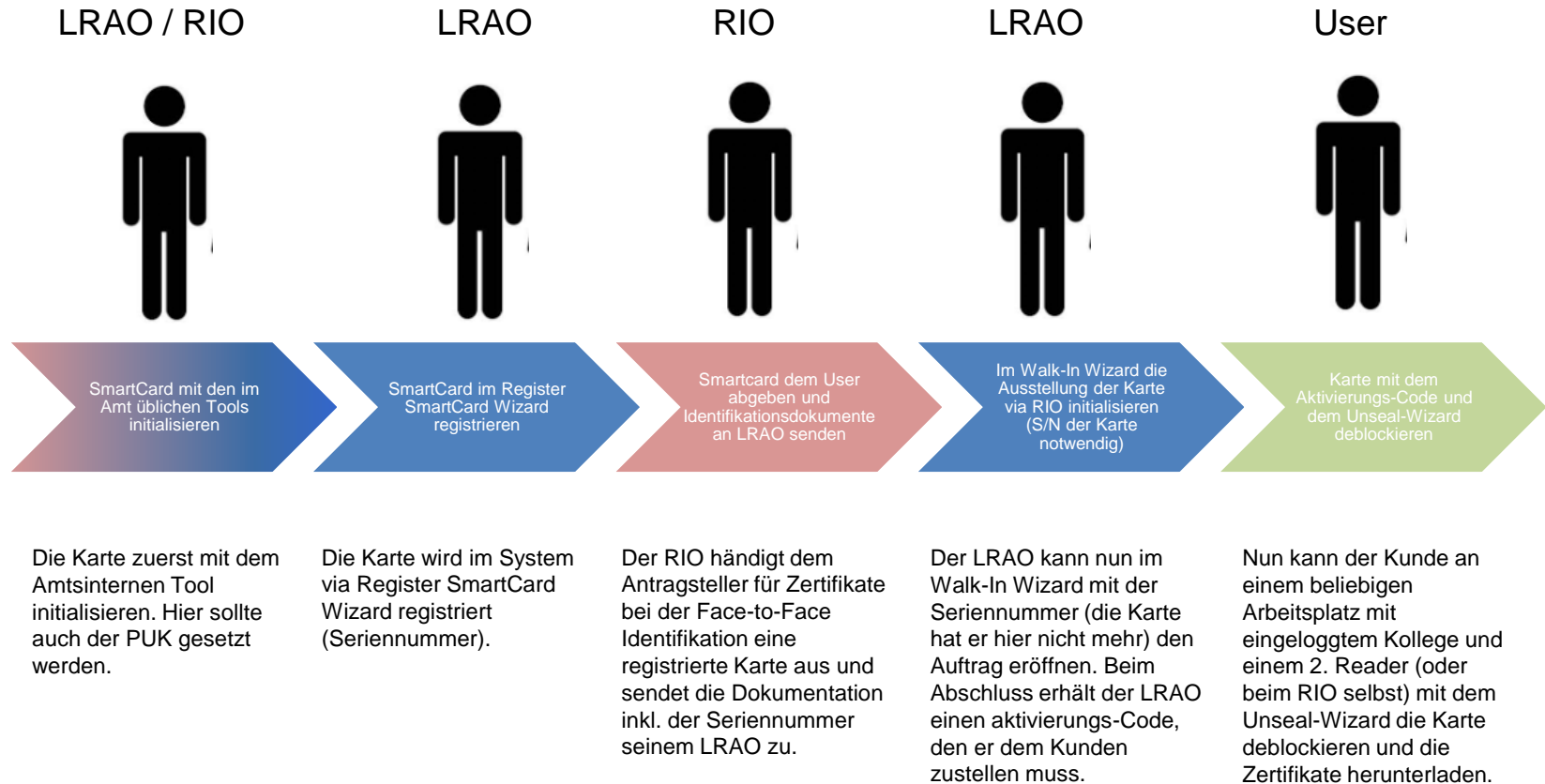


Workflow 2: Klasse B Standardzertifikat mit initialisierter Karte, PUK-Management im eigenen Amt





Workflow 3: Klasse B Standardzertifikat mit fabrikneuer Karte, PUK-Management im eigenen Amt





Prozesse

Workflow 4: Klasse B Standardzertifikat mit initialisierter Karte, PUK-Management im BIT





Links

- Links:
 - Benutzerformular, Prozess, Use-Cases:
 - <https://www.bit.admin.ch/adminpki/00240/00367/00820/00822/index.html?lang=de>
 - Token Unseal:
 - <https://www.bit.admin.ch/adminpki/00240/00367/00820/06361/index.html?lang=de>
 - Register SmartCard:
 - <https://www.bit.admin.ch/adminpki/00240/00367/00820/05067/index.html?lang=de>
 - Terms of Usage / Guidelines:
 - <https://www.bit.admin.ch/adminpki/00240/00367/05012/index.html?lang=de> (noch nicht online)



Ende

Fragen?





Ende

DANKE!

