Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

NICHT KLASSIFIZIERT

Swiss Government PKI Registrierrichtlinien Klasse A – Qualifizierte und geregelte Zertifikate

Richtlinien für die LRA-Officer zur Ausgabe und Verwaltung von persönlichen Signaturzertifikaten der Klasse A – Qualifizierte und geregelte Zertifikate gemäss ZertES

V1.0, 12.05.2026

Klassifizierung	General
Status	Freigegeben
Projektname	Swiss Government PKI Registrierrichtlinien Klasse A – Qualifizierte und geregelte Zertifikate
Auftraggeber	Swiss Government PKI
Autor	Swiss Government PKI
Bearbeitende	Salvatore Tomasulo, Stefan Good, Silvio Pelli, Cornelia Enke, Mario Lovisi
Prüfende	Product Owner und Security Officer BIT PKI
Genehmigende	Product Owner TRS und Security Officer BIT PKI
Verteiler	LRA-Officer, Auditoren
Doc_ID	0239-RV-Swiss Government PKI Registrierrichtlinien Klasse A - Qualifizierte und geregelte Zertifikate
Kurzbeschreibung	Diese Richtlinien beschreiben die Prozesse und Abläufe, die von den LRA-Officern bei der Ausgabe und Verwaltung von qualifizierten und geregelten Zertifikaten der Klasse A zu befolgen sind. Sie detaillieren die in den CP/CPS der Root und Issuing CA aufgeführten Vorgaben.
Ablageort	ActaNova: 422-SERV/SIGVALD

Änderungskontrolle, Prüfung, Genehmigung

Version	Datum	Beschreibung, Bemerkung	Name oder Rolle
1.0	12.05.2026	Zusammenführung der Registrierrichtlinien für Klasse A – Qualifizierte Zertifikate und geregelte Behördenzertifikate in ein Dokument	Silvio Pelli / Mario Lovisi / Stefan Good

Freigabe

Version	Datum	Name	Rolle
1.0	12.05.2026	Lovisi Mario Weber Jürgen	Product Owner Security Officer

Definitionen, Akronyme und Abkürzungen

Begriff / Abkürzung	Bedeutung
Admin-Directory (AdminDir)	Das Admin-Directory ist ein Verzeichnis der Bundesverwaltung, in welchem unter anderem Zertifikate und die Revokationslisten aufbewahrt werden, so dass die End-Benutzer darauf zugreifen können. Es handelt sich um ein Verzeichnis gemäss der Empfehlung X.500
Aktivierungsdaten	sind Daten, welche ein Benutzer eingeben muss, um ein kryptographisches Modul (z.B. Smartcard) zu aktivieren. Die privaten Schlüssel gehören nicht zu den Aktivierungsdaten.
Antragssteller	Ein Antragssteller ist eine Person, welche einen Antrag für ein Zertifikat stellt. Nach erfolgter Ausstellung wird diese Person als Zertifikatsinhaber bezeichnet.
Issuing CA	Certification Authority: Komponente einer PKI, welche durch Signieren der Schlüsseldaten unter Anwendung einer definierten Policy Zertifikate ausstellt.
CP/CPS	Certificate Policy und Certificate Practice Statement: Dokumente, welche die Templates und Prozesse zur Ausstellung und Verwaltung der Zertifikate, die durch die beschriebene CA ausgestellt werden, beschreibt.
CSP	Certificate Service Provider (Zertifizierungsdienstanbieter): Organisation, die eine PKI betreibt, z.B. die Swiss Government PKI.
Digitale Signatur	Ergebnis der Codierung einer Meldung mit Hilfe eines kryptographischen Systems, welches Schlüssel so benützt, dass der Empfänger der Meldung feststellen kann 1. ob der zur Codierung verwendete Schlüssel dem Signierer (Unterzeichner) gehört 2. ob die Meldung seit dem Zeitpunkt der Codierung verändert wurde.
Geregeltes Behördenzertifikat	Ein nach den Vorschriften des ZertES ausgestelltes Zertifikat für eine juristische Person der öffentlichen Verwaltung.
Hashwert, Fingerprint	Ein Hashwert ist ein numerischer Wert, der aus einem gegebenen Dateninput durch die Anwendung eines sog. Hash-Algorithmus gebildet wird. Da bei einem guten Algorithmus der Hashwert für verschiedene Daten auch verschieden ausfällt, dient er unter anderem als "Fingerprint" zur Sicherung der unverfälschten Übertragung von Dokumenten. Im Falle einer Verfälschung würde der vom Empfänger errechnete Hashwert nicht mehr mit dem vom Absender mit gesandten übereinstimmen. Mit dem geheimen Schlüssel des Absenders verschlüsselter Hashwert wird als digitale Signatur bezeichnet.
Kundendossier	Ein Kundendossier ist die LRA- Ablage von Dokumenten und Evidenzen (Beweise) die jede Ausstellung, Revokation oder Bewegungen der LRA sammelt. Kundendossiers müssen 11 Jahre aufbewahrt werden. Kundendossiers können schriftlich in Papierform (Ordner, Archiv) oder elektronisch (nach gewissen Regeln) geführt werden.

Begriff / Abkürzung	Bedeutung
Liste der revozierten Zertifizierungsstellen	[ARL: Authority Revocation List]: Die ARL ist eine Liste der Zertifikate von CAs der zweiten Stufe, welche durch die Wurzelzertifizierungsstelle (Root CA) revoziert wurden.
Liste der revozierten Zertifikate	[CRL: Certificate Revocation List]: Die CRL ist eine Liste, welche die Seriennummern derjenigen Zertifikate enthält, welche vor ihrem Ablauf revoziert wurden. Diese Liste wird durch die Zertifizierungsstelle à jour gehalten.
Lokale Registrierstelle [Local Registration Authority- (LRA)]	Eine LRA ist eine Person oder Organisation, welche für die Identifikation und Überprüfung der Berechtigung eines Antragstellers oder Zertifikatsinhabers verantwortlich ist. Die LRA signiert weder das Zertifikat, noch stellt sie es aus. Die LRA lässt sich bestimmte Aufgaben von der CA übertragen. Die Aufgaben der LRA werden von LRA-Officern wahrgenommen. Neben der Hardware (Laptop) und Software (LRA-Client), die für das Bearbeiten der Zertifikate verwendet werden, gehören insbesondere auch die Räumlichkeiten dazu, in denen die Kunden identifiziert, Zertifikate ausgestellt, Kundendossiers aufbewahrt und die Computer der LRA (LRA-Station) betrieben werden. Im Fall der geregelten Behördenzertifikate ist die LRA innerhalb der Organisation der Swiss Government PKI
LRA-Officer (LRAO)	Die als LRAO ernannte Person amtiert im Auftrag der Swiss Government PKI und übernimmt die Aufgaben der LRA (beispielsweise Identifikation des Kunden, Erstellen oder Revozieren eines Zertifikates).
Object Identifier (OID)	Der OID ist eine eindeutige numerische Identifikation eines Objektes oder einer Klasse von Objekten; die Registrierung erfolgt gemäss internationalen Normen.
Public Key Infrastruktur [PKI]	Eine PKI ist die Gesamtheit der Richtlinien, Prozesse, Server, Programme und Arbeitsstationen, welche zur Verwaltung der Schlüssel und der zugehörigen Zertifikate dienen.
Swiss Government PKI (SG-PKI)	Unter Swiss Government PKI wird der TSP für die im Standarddienst angebotenen Zertifikatsklassen verstanden.
Signaturservice (TW4S)	Trustworthy Systems Supporting Server Signing (TW4S) bezeichnet ein sicheres Framework und eine Reihe technischer Spezifikationen für die zentralisierte, serverbasierte digitale Signatur. Es ermöglicht Benutzern, qualifizierte elektronische Signaturen oder geregelte Siegel aus der Ferne zu erstellen und dabei die alleinige Kontrolle über ihre Signaturschlüssel zu behalten.
Swiss Government Regulated CA 03	Der Swiss Government Root CA IV subordinierte Issuing CA, welche Zertifikate der Klasse A – Qualifiziert und Zertifikate der Klasse A – geregeltes Behördenzertifikat herausgibt.
TSP	Trust Service Provider Innerhalb der Bundesverwaltung ist dies das BIT.
Root CA (Wurzelzertifizierungsstelle)	Oberste CA, die durch Signatur der Schlüssel die Zertifikate der subordinierten Issuing CAs ausstellt. Die Root CA stellt keine Nutzerzertifikate (Leaf Certificates) aus.
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate - 943.03 vom 18. März 2016 (Stand am 1. Januar 2020).
Zertifikat	Ein Zertifikat enthält den öffentlichen Schlüssel eines Zertifikatsinhabers, sowie weitere Angaben über diesen. Die vollständige Information wird mit dem privaten Schlüssel der Zertifizierungsstelle (CA), welche das Zertifikat ausstellt, digital signiert. Das Format erfüllt die Empfehlung der X.509 Richtlinie.
Zertifikatsanwender	Ein Zertifikatsanwender ist eine Person, die ein Zertifikat eines Zertifikatsinhabers verwendet. Ein Zertifikatsanwender kann auch eine Organisationseinheit der Bundesverwaltung, ein Informatiksystem, eine Informatikanwendung oder ein Zertifikatsinhaber einer anderen PKI oder auch Kunden oder Lieferanten sein.
Zertifikatsinhaber	Zertifikatsinhaber der Swiss Government PKI Klasse A sind Mitarbeiter oder administrative Einheiten der schweizerischen Bundesverwaltung, der kantonalen oder kommunalen Verwaltung. Im Zertifikat - nach X.509 - wird sie als subject bezeichnet.
Zertifikatsklassen	Die Swiss Government PKI gibt Zertifikate der Klassen A, B, C und E auf unterschiedlichen CAs aus.

Referenzen

Erkennungszeichen	Titel, Quelle
[1]	**Swiss Government PKI - Root CA IV - CP_CPS EN** (0261-RV-CP-CPS Root_CA_IV_(2.16_756_1_17_3_5_0) Version: die jeweils aktuell publizierte Version Quelle: Swiss Government PKI
[2]	**SR 943.03 Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 18.03.2016** Version: vom 18. März 2016 (Stand am 1. Januar 2020) Quelle: https://www.fedlex.admin.ch/eli/cc/2016/752/de
[3]	**SR 943.032 Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23.11.** Version: vom 23. November 2016 (Stand am 1. November 2025) Source: https://www.fedlex.admin.ch/eli/cc/2016/753/de
[4]	**SR 943.032.1 Verordnung des BAKOM über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23.11.2016** Version: vom 23. November 2016 (Stand am 1. November 2025) Source: https://www.fedlex.admin.ch/eli/cc/2016/754/de
[5]	**Benutzervereinbarung und Nutzungsbedingungen für Zertifikate der Klasse A – Geregelte und qualifizierte Zertifikate gemäss ZertES (für juristische und natürliche Personen)** (0094-RV-Terms and Conditions Class A - qualified.docx) jeweils aktuelle veröffentlichte Version Quelle: Swiss Government PKI
[6]	**120.4 Verordnung über die Personensicherheitsprüfungen (PSPV)** Version: vom 4. März 2011 (Stand am 1. September 2023) Quelle: https://www.fedlex.admin.ch/eli/cc/2011/155/de
[7]	Informationsblatt für Zertifikatinhaber der SG-PKI Klasse A (qualifizierte Zertifikate)
[8]	**120.73 Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV)** vom 27. Mai 2020 (Stand am 1. April 2021)Quelle: https://www.fedlex.admin.ch/eli/cc/2020/416/de
[9]	IETF RFC 1309: ITU-T X.500 Technical Overview of Directory Services Using the X.500 Protocol Version: 1992, Status: published März 1992 Quelle: https://tools.ietf.org/pdf/rfc1309.pdf
[10]	IETF RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework Version: 2003, Status: published November 2003 Quelle: https://tools.ietf.org/pdf/rfc3647.pdf
[11]	RFC 2459, Public Key Infrastruktur X.509 Internet, Zertifikats- und CRL-Profile; Version 1999, Status: published Januar 1999 Quelle: https://tools.ietf.org/pdf/rfc2459.pdf
[12]	RFC 2510, Public Key Infrastruktur X.509 Internet, Protokolle für das Zertifikats-Management; Version: März 1999, Status published März 1999 Quelle: https://tools.ietf.org/pdf/rfc2510.pdf
[13]	FIPS 140-2: Sicherheitsanforderungen für kryptographische Module, National Institute of Standards and Technology, Federal Information Processing Standards, 1994
[14]	Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites ETSI TS 119 312 V1.5.1 (2024-12)
[15]	Swiss Government SSCD Evaluation Criteria
[16]	Swiss Government SSCD Protection Profile

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 von Zertifikaten der Klasse A – Qualifiziert für natürliche Personen und geregelten Behördenzertifikaten für juristische Personen der Swiss Government PKI, nachstehend (SG-PKI), zur Anwendung gelangen.

Zielgruppe

Das Dokument richtet sich primär an die ausgebildeten Klasse A LRA-Officer der Ämter und bundesnahen Betrieben.

Verwendete Begriffe und Abkürzungen

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

Referenzierte Dokumente

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

Hinweis auf weibliche und männliche Schreibweise

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

1.1 Zweck des Dokumentes

Die „Swiss Government PKI - Root CA IV - CP_CPS EN" (im Folgenden abgekürzt mit „CP/CPS“) [1] ist das massgebende Regelwerk für die Zertifikate der ‘Klasse A - Qualifiziert’ und geregelten Behördenzertifikaten der SG-PKI. Das Ziel dieses Dokumentes ist es, die Anforderungen der CP/CPS betreffend die ausstellenden Personen der SG-PKI zu konkretisieren.

1.2 Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeitenden, die im Bereich der LRA (Local Registration Authority) von Zertifikaten der ‘Klasse A - Qualifiziert’ und geregelten Behördenzertifikaten tätig sind. Die SG-PKI kann die Aufgaben der LRA Klasse A Qualifiziert an andere Organisationseinheiten delegieren. Diese bestimmen ihrerseits die ausführenden Mitarbeiter. Die Aufgaben für geregelte Behördenzertifikate können nicht an andere Organisationseinheiten delegiert werden.

Für die Zertifikate der ‘Klasse A - Qualifiziert’ und geregelten Behördenzertifikaten existiert ein einziger Ausstellungsprozess:

- Ausstellungsprozess mit persönlicher Identifizierung

1.3 Swiss Government PKI – qualifizierte und geregelte Zertifikate der Klasse A

Ein qualifiziertes Signaturzertifikat oder das geregelte Behördenzertifikat wird auf einem Hardware Security Module (HSM) ausgestellt. Der Zugriff auf den privaten Schlüssel bei der qualifizierten Signatur wird mittels dem Authentisierungszertifikat der Klasse B oder der MobileID aktiviert oder beim geregelten Behördenzertifikat auch über die am Signaturservice registrierte Fachanwendung.

2 Aufgaben des LRA-Officers

2.1 Anforderungsprofil LRA-Officer

- Hohe persönliche Integrität
- Genaues Arbeiten nach den Vorschriften der Swiss Government PKI
- Zuverlässigkeit
- Freude am Umgang mit Kunden
- Bereitschaft, eine Tätigkeit unter Berücksichtigung der Nachvollziehbarkeit, auszuüben
- Bereitschaft, sich einer Vertrauenswürdigkeitsprüfung wie z.B. einer Grundsicherheitsprüfung nach PSPV (Ref. [6]) zu unterziehen (siehe 3.7)
- Ein LRA-Officer darf nicht für die Erfassung oder Mutation von AdminDirectory-Einträgen berechtigt sein
- Für qualifizierte Zertifikate: Mind. 6 Monate aktive Tätigkeit als LRA-Officer Klasse B
- Für geregelte Behördenzertifikate: Nur Mitarbeiter der SG-PKI, welche eine interne Schulung absolviert haben

2.2 Aufgaben des LRA-Officers

Der LRA-Officer hat grundsätzlich folgende Aufgaben:

- Antragsteller identifizieren
- Angaben im AdminDirectory verifizieren
- Zertifikat ausstellen
- Zertifikat revozieren
- Kunden instruieren betreffend:
    - Aktivierungsdaten
    - Schutz der Aktivierungsdaten
    - Seinen Rechten und Pflichten
    - «*Benutzervereinbarung und Nutzungsbedingungen Klasse A – qualifiziert*» (Ref. [5])
- Checklisten ausfüllen
- Journal über alle Aktivitäten, welche die Zertifikate betreffen, führen
- Dossiers der Zertifikatsinhaber führen und aufbewahren
- Kenntnisse über Vorschriften, Prozesse und technische Mittel im Zusammenhang mit geregelten Behördenzertifikaten proaktiv aktuell halten

2.3 Haftung

Dem LRA-Officer ist bewusst, dass er keinen Antrag an die SG-PKI übermitteln darf, wenn die Identifizierung der antragstellenden Person nicht korrekt oder nicht vollständig durchgeführt werden kann.

Ein Verstoss gegen diese Pflicht kann zum sofortigen Entzug der LRAO-Berechtigung sowie – falls erforderlich – zu weiteren rechtlichen Schritten führen.

Der LRA-Officer trägt die Verantwortung für alle von ihm identifizierten Antragstellerinnen und Antragsteller. Er haftet für Schäden und Folgen, die aus einer fehlerhaften oder unzureichenden Identifizierung entstehen.

2.4 Meldepflicht

Organisationswechsel, Namenswechsel (z.B. nach Heirat) oder Änderung der E-Mail-Adresse des LRA-Officers müssen unmittelbar der SG-PKI gemeldet werden.

3 Allgemeine betriebliche Aspekte

3.1 Servicezeiten der LRA

Die Servicezeiten der LRA werden von den jeweils verantwortlichen Organisationseinheiten selbst festgelegt.
Die Servicezeiten im BIT sind im jeweiligen Factsheet im online Kundenportal des BIT beschrieben.

3.2 Unterstützung der LRA

Zur Unterstützung der LRA ist das Betriebsteam der Swiss Government PKI gemäss den Angaben im BIT-Produktekatalog respektive dem geltenden SLA erreichbar.

Bei Störungen erfolgt der Kontakt zum Betriebsteam über das Service Desk BIT (058 465 88 88).

Bei dringenden sicherheitsrelevanten Mitteilungen und Fragen erfolgt der Kontakt zu einem Swiss Government PKI Security Officer ebenfalls über das Service Desk BIT (058 465 88 88).

Für weniger zeitkritische Mitteilungen und Fragen im Bereich Sicherheit steht die Mailbox pki-secoff@bit.admin.ch zur Verfügung.
Allgemeine Fragen können an die Mailbox signaturservice@bit.admin.ch geschickt werden.

3.3 Formulare und Kundendaten

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

Kundendossiers (Ablagen mit Antragsformularen, Vollmacht für geregelte Behördenzertifikate, unterschriebene Benutzervereinbarungen, Revokationsanträge, etc.) sind verschlossen aufzubewahren («Cleardesk»-Prinzip). Entweder ist der Raum abgeschlossen oder die Dokumente sind in einem Schrank wegzuschliessen.

Bei der Führung von elektronischen Kundendossiers müssen die Daten in einer Ablage gespeichert werden, auf die nur autorisierte Personen, also LRA-Officer und Auditoren, Zugriff haben. Zudem ist sicherzustellen, dass die unter 3.5 - Aufbewahrungsfristen definierten Bedingungen eingehalten werden. Sämtliche abgelegten Belege müssen als PDF/A Dokument vorhanden und gültig signiert sein.

3.4 Journal

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

- Ausstellung von Zertifikaten
- Revokation von Zertifikaten

LRA-Officer Journale können entweder handgeschrieben (s. aktuelle Vorlage ‚*Journal LRA der Swiss Government PKI für nach ZertES qualifizierte Zertifikate der Klasse A für natürliche Personen*‘) oder elektronisch geführt werden. Bei der elektronischen Führung müssen die Tages-Journale jeweils am Abend ausgedruckt, vom ausführenden LRA-Officer unterschrieben und abgelegt werden. Alternativ können die elektronischen Journale täglich in eine PDF/A-Datei exportiert und mit dem Zertifikat der Klasse B des LRA-Officer signiert und mit dem Zeitstempel des Swiss Government PKI (SG-PKI TSA- Time Stamping Authority) versehen werden. Es ist grundsätzlich erlaubt

mehrere Journale pro LRA zu führen (z.B. pro LRAO, pro Amt, pro Monat, etc…) sofern die Chronologie nachvollziehbar bleibt.

Die Journaldaten müssen nach den Archivierungsfristen gemäss Kap. 3.5 - *Aufbewahrungsfristen* sichergestellt werden.

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

1. Fortlaufende Nummer des Eintrags (Die Chronologie muss nachvollziehbar sein! D.h. es darf jährlich von Neuem begonnen werden, wenn z.B. die Jahreszahl davor geschrieben wird, etc…)
2. Datum
3. Ausführender LRA-Officer
4. Antragsteller
5. Tätigkeit (E: Erstellen, R: Revozieren)
6. Visum oder elektronische Signatur mit Zeitstempel des LRA-Officers
7. Bei geregelten Zertifikaten: CN des Behördenzertifikats

3.5 Aufbewahrungsfristen

Formulare, Kundendaten und Journale gemäss den Kapiteln ‚3.3 - *Formulare und Kundendaten*' und ‚3.4 - *Journal'* müssen in jedem Fall während mindestens 11 Jahren über das Ende der Gültigkeit des jeweiligen Zertifikats hinaus archiviert werden. Das Archiv muss während dieser Zeit für die Auditoren zugänglich sein.

3.6 Entsorgung

Nicht mehr benötigte Papierdokumente betreffend der LRA (Richtlinien, Checklisten, Notizen, Kopien etc.) oder der Kunden (nicht benötigte Teilnehmeranträge, Listen, etc.) sind mit einem Shredder oder einer Sicherheitsbox zu entsorgen.

3.7 Vertrauenswürdigkeitsprüfung

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

- Personensicherheitsprüfung: Grundsicherheitsprüfung gemäss der Verordnung über die Personensicherheitsprüfungen (PSPV, SR 120.4) bei der Fachstelle PSP des VBS (s. [6])

und/oder

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

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

Jeder Mitarbeiter der SG-PKI wird durch eine Grundsicherheitsprüfung gemäss PSPV überprüft.

3.8 Vertraulichkeit, Datenschutz

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

Die Gesetze und Verordnungen des Datenschutzes sind vom LRA-Officer sowie von seinen Kunden unbedingt einzuhalten.

Informationen betreffend Kundendaten oder wichtige Daten der LRA oder CA sind verschlüsselt zu übermitteln.

3.9 Ausbildung des Personals

Alle LRA-Officer müssen eine Schulung durchlaufen und eine entsprechende Prüfung bestehen. Voraussetzung zum Besuch einer LRA-Officer Klasse A Schulung ist eine mind. 6 Monate dauernde, aktive Tätigkeit als LRA-Officer Klasse B. Am Ende der Schulung wird festgestellt, ob der Teilnehmer genügend Kenntnisse und Fähigkeiten hat, um als LRA-Officer der Klasse A tätig zu sein.

Erfüllt der Teilnehmer die Bedingungen des Zertifizierungsverfahrens nicht, oder besteht er die schriftliche Prüfung nicht, so darf er diese Aufgaben auch nicht in Stellvertretung ausüben. Er kann aber bei einem erneuten Kursbesuch zeigen, dass er nun über die erforderliche Eignung und Kompetenzen verfügt und hat die Möglichkeit die Prüfung zu wiederholen.

Stellt ein LRA-Officer Mängel in seinem Wissen, Fähigkeiten oder Unklarheiten fest und kann er diese selbst nicht beheben, ist er verpflichtet, dies bei der Swiss Government PKI zu melden. Die Swiss Government PKI wird zusammen mit dem LRA-Officer eine Lösung suchen.

Die Ausstellung von geregelten Behördenzertifikaten wird intern (SG-PKI) geschult.

Bei Zuwiderhandlungen gegen die Registrierrichtlinien kann die SG-PKI die Qualifikation des LRA-Officer entziehen.

3.10 Auffrischung der Ausbildung

Der LRA-Officer ist verpflichtet, sein Wissen, insbesondere in Bezug auf die CP/CPS [1], den *Registrierrichtlinien* (dieses Dokument) und die *Benutzervereinbarung* [5], auf dem aktuellen Stand zu halten. Zu diesem Zweck stellt die SG-PKI die aktuellen Dokumente und Informationen im Kundenbereich des Internetauftritts https://www.pki.admin.ch zur Verfügung. Die SG-PKI verpflichtet sich, wichtige Änderungen per E-Mail anzuzeigen. Der LRA-Officer seinerseits ist verpflichtet, bei Erhalt eines entsprechenden Emails der SG-PKI die entsprechenden Informationen im Kundenbereich des Internetauftritts der SG-PKI zu lesen.

Die SG-PKI bietet regelmässig Weiterbildung- und Wiederholungskurse für die LRA-Officer an. Die LRA-Officer können zur Teilnahme verpflichtet werden.

Stellt der LRA-Officer Mängel in seinem Wissen, Fähigkeiten oder Unklarheiten fest und kann er diese selbst nicht beheben, ist er verpflichtet, dies bei der SG-PKI zu melden. Die SG-PKI wird zusammen mit dem LRA-Officer eine Lösung suchen.

4 Konformitätsprüfung

Die SG-PKI ist verpflichtet, alle 18 Monate die Durchsetzung der CP/CPS zu überprüfen. Dazu gehört besonders die Überprüfung der Einhaltung dieser Registrierrichtlinien durch die LRA-Officer. Die Konformitätsprüfung kann durch die SG-PKI selbst oder durch eine von der SG-PKI beauftragten externen Stelle durchgeführt werden.

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

5 Prozesse der Swiss Government PKI Klasse A – Qualifiziert und geregeltes Behördenzertifikat

5.1 Übersicht

Für Zertifikate der ‘Klasse A – Qualifiziert – für natürliche Personen’ und ‘Klasse A – Geregelte Behördenzertifikate für juristische Personen’ gibt es einen einzigen Ausstellungsprozess

Klasse A – Qualifiziert für natürliche Personen und geregelte Behördenzertifikate
Ein Schlüsselpaar (Signatur)
Keine Suspendierung möglich
Natürliche Personen: Keine Bevollmächtigung möglich Juristische Personen: Bevollmächtigung ist möglich
Kein Key Recovery
Kein Rekeying (Renewal)

Tabelle 1: Prozess Klasse A – Qualifiziert – natürliche Personen und geregelte Zertifikate – juristische Personen

5.2 Prozess Zertifikat ausstellen

Hauptkomponenten des Ausstellungsprozesses:

Prozess
Persönliche Identifikation des Antragstellers nur direkt durch den LRA-Officer Klasse A.
Bei Behördenzertifikat: Vorgängige Überprüfung des eingereichten Antrags inklusive der geforderten Vollmacht und Eintrag im UID-Register.
Überprüfen des Antragsstellers im Admin-Directory durch LRA-Officer
Teilnehmerinstruktion betreffend Aktivierungsdaten und deren Schutz durch LRA-Officer
LRA-Officer erzeugt Antrag für den Teilnehmer.

Tabelle 2: Ausstellungsprozess

5.2.1 Wer kann ein Zertifikat beantragen?

Natürliche Person:
Über die Vergabe qualifizierter Zertifikate entscheiden die jeweiligen Organisationseinheiten.

Juristische Person:
Grundvoraussetzung für den Erhalt eines geregelten Behördenzertifikates ist, dass die Organisation eine UID-Einheit im Sinne von Artikel 3 Absatz 1 Buchstabe c des Bundesgesetzes vom 18. Juni 2014 über die Unternehmens-Identifikationsnummer (UIDG) ist. Der Antragsteller muss für die jeweilige UID-Einheit zeichnungsberechtigt sein. Diese Berechtigung muss er entweder durch einen beglaubigten Handelsregisterauszug oder durch eine rechtswirksam unterzeichnete Vertretungsermächtigung nachweisen können.

5.2.2 Wie kann ein Zertifikat beantragt werden

Die Bestellung von qualifizierten und geregelten Zertifikaten erfolgt über Digital Workplace (DWP).

Grundsätzlich muss jedoch der Bestellvorgang nachvollziehbar sein. Die SG-PKI stellt ein Formular zur Verfügung, welches alle für die Anmeldung benötigten Daten gemäss Art. 7 Abs. 3 Bst. a des ZertES und Art 5 des VZertES enthält [2] [3].

5.2.3 Ausstellen

Der LRA-Officer geht gemäss der aktuellen Checkliste «*Walkthrough und Checkliste für die Ausstellung qualifizierter Zertifikate für natürliche Personen»* vor. Die Checkliste ist Teil der Dokumentation der Ausstellung und muss ausgefüllt, digital signiert und archiviert werden.

5.2.3.1 Eintrag im Admin-Directory überprüfen (natürliche Person)

Der Antragsteller 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 ‚E-Mail' spezifiziert?
   Neben der Terminvereinbarung dient dieser Schritt gleichzeitig der Verifizierung der E-Mail Adresse des Antragsstellers und darf nicht übersprungen werden (gem. 2. Punkt in der Checkliste).
2. Falls mehr als 1 Eintrag vorhanden ist: Kann der Eintrag, auf den das Zertifikat ausgestellt wird, eindeutig durch das Namens-Suffix identifiziert werden?

Ist der Antragsteller nicht oder nicht korrekt im Admin-Directory eingetragen, ist der Eintrag oder die Änderung via Personaldatensystem des Amtes zu veranlassen. Das Verfahren kann erst fortgesetzt werden, wenn der Antragsteller korrekt im Admin-Directory eingetragen ist.

5.2.3.2 Eintrag im öffentlichen Register (juristische Person)

Voraussetzung für die Ausstellung der Zertifikate ist, dass die im Antrag genannte Behörde als juristische Person existiert und über einen Eintrag im öffentlichen UID-Register (www.uid.admin.ch) verfügt.

Ist die Behörde nicht oder nicht korrekt in einem öffentlichen Register eingetragen, ist entweder die Erstellung des Eintrags oder dessen Korrektur durch die Behörde zu veranlassen. Die maximale Behördenbezeichnung darf die 64 Zeichen nicht überschreiten. Sind im Register nicht alle relevanten Daten öffentlich zugänglich, muss der Antragsteller eine beglaubigte Kopie aller erforderlichen Kerndaten beilegen. Das Verfahren kann erst fortgesetzt werden, wenn alle Unterlagen und Einträge korrekt und vollständig vorhanden sind.

5.2.3.3 Antragsformular überprüfen

Antragsformular auf Vollständigkeit und Korrektheit überprüfen.

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

Zusätzlich bei juristischer Person

4. Der Eintrag im UID-Register ist vorhanden. (Auszug UID-Register. Falls nicht alle Daten zu den Kernmerkmalen im UID-Register veröffentlicht sind, dann ist der aktuell beglaubigte Auszug bei-zulegen)
5. Eine Vollmacht oder Zeichnungsberechtigung für den Bezug des Zertifikates ist vorhanden (beglaubigter Handelsregisterauszug oder rechtswirksam unterzeichnete Vertretungsermächtigung)

5.2.3.4 Terminvereinbarung

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

1. Terminvorschlag/-vorschläge für die Zertifikatserstellung

2. Aufforderung an den Antragssteller, ein gültiges Reisedokument mitzubringen. Das Reisedokument darf zum Zeitpunkt der Registrierung nicht abgelaufen sein.
3. Kontaktdetails des LRA-Officers für Fragen und die Lösung von Terminkollisionen

5.2.3.5 Identität des Antragstellers überprüfen

Der Antragssteller muss persönlich beim LRA-Officer erscheinen. Die Identifizierung des Antragstellers muss mittels eines gültigen Reisepasses oder einer für die Einreise in die Schweiz gültigen Identitätskarte vorgenommen werden. Die Überprüfung der Identität des Antragsstellers beinhaltet zwei Elemente:

1. Überprüfung der Echtheit des vorgelegten Reisedokuments. Dabei muss es sich um einen Reisepass oder eine von der Schweiz ausgestellte, resp. für die Einreise in die Schweiz anerkannte Identitätskarte handeln. Zum Beispiel genügt ein 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. Im Zweifelsfall ist eine Person mit fundierten Kenntnissen in der Verifikation von Reisedokumenten beizuziehen.
    c. Entsprechen die Angaben im Dokument denjenigen des Antrags.
    d. Stimmt die Unterschrift im Reisedokument mit derjenigen auf dem Antragsformular überein?
2. Persönliche Identifikation des Antragsstellers durch Vergleich der Person mit der Fotografie auf der Ausweisschrift.
3. Überprüfung der Vollmacht: Die Vollmachtsbescheinigungen sind zu prüfen.

5.2.3.6 Information über Rechte und Pflichten des Antragstellers

Der Antragsteller muss mündlich auf seine Rechte und Pflichten aufmerksam gemacht werden. Hierbei werden die geltenden «*Benutzervereinbarung und Nutzungsbedingungen Klasse A- Geregelte und qualifizierte Zertifikate gemäss ZertES*» dem Kunden mündlich erklärt.

Der LRA-Officer entscheidet, ob der Antragsteller nun über das nötige Grundwissen für die angemessene Verwendung des privaten Signierschlüssels und des Zertifikates verfügt und seine Rechte und Pflichten kennt. Wenn der Antragsteller Anlass gibt zur Vermutung, dass er seine Rechte und Pflichten nicht wahrnehmen kann oder will, verweigert der LRA-Officer die Beendigung des Prozesses.

5.2.3.7 Ausstellung für Signaturservice vorbereiten

Der LRAO erfasst basierend auf dem geprüften Antrag die Angaben im Admin UI des Signaturservice. Sind alle Angaben erfasst kann der CSR erzeugt werden.

5.2.3.8 Zertifikate beantragen

Die Beantragung des Zertifikats wird durch den LRA-Officer mit Hilfe des CRW-Tools durchgeführt. Nach dem Login wählt der LRA-Officer in der Anwendung zuerst die korrekte Policy für Klasse A - Qualified oder das geregelte Behördenzertifikat aus.

5.2.3.9 DN des geregelten Behördenzertifikats

Der DN des geregelten Behördenzertifikats wird gemäss folgenden Regeln eingegeben:

Distinguished Name des Zertifikates		
C	CH oder LI Länderkürzel nach ISO 3166-1. Es bezeichnet das Land, der unter dem RDN „O“ bezeichneten Behörde.	obligatorisch
O	Der O muss mit dem Namen im UID-Register übereinstimmen (muss von der CSP geprüft werden, max. 64 Charakteren)	obligatorisch
CN	Allgemein gebräuchlicher Name der Verwaltungsstelle. Der Name muss nicht mit genau mit dem registrierten Namen übereinstimmen (Bezeichnung gemäss UID-Register.)	obligatorisch
OI[1]	UID Nummer der ausstellenden Behörde (gemäss UID-Register), wie durch die ZertES verlangt wird	obligatorisch
OU_{1-2}	Nähere Bezeichnung der Organisationseinheit (Departement, Abteilung, etc.), die dem Zertifikat zugeordnet ist. Es können zwei OU Felder angegeben werden.	optional
OU_3	Behörden-Identifikation: GE - 0220 – Amtskürzel oder -bezeichnung Bundesbehörde (Bundesamt) GE - 0221 - Kantonskürzel - Amtskürzel oder -bezeichnung kantonale Behörde GE - 0222 - Kantonskürzel - Hist. BFSNR - Amtskürzel oder -bezeichnung Behörde eines Bezirks GE - 0223 - Hist. BFSNR - Amtskürzel oder -bezeichnung kommunale Behörde	obligatorisch
L	Bezeichnung der Gemeinde in der die Behörde Ihren Sitz hat.	optional
SP	Bezeichnung des Kantons in dem die Behörde Ihren Sitz hat.	optional
E-Mail des Zertifikates (z.B.: «info@amt.admin.ch»)		
E-Mail	Mail-Adresse, die bei einer automatisierten Prüfung eines elektronisch gesiegelten Dokumentes ggf. in einem Prüfbericht aufgeführt wird, um die Auskunftstelle für den signierten Dokumententyp anzuzeigen.	optional

5.2.3.10 Zertifikats-Ausstellung

Im AIS wird der CSR generiert und anschliessend über das CRW signiert, wo das Zertifikat ausgestellt wird. Danach kann das Zertifikat heruntergeladen und im Admin UI des Signaturservers hochgeladen werden.

5.2.3.11 Journal führen und Checkliste unterschreiben

Die durchgeführten Aktivitäten müssen vom LRA-Officer im LRA-Journal festgehalten werden. Dabei gelten die unter ‚3.4 - *Journal*‘ aufgeführten Regeln.

Die Checkliste muss auf Vollständigkeit der Daten überprüft und dann vom LRA-Officer ebenfalls unterschrieben werden.

5.2.3.12 Ablage Kundendossier

Der ausgefüllte und signierte Antrag inkl. Benutzervereinbarung- und Nutzungsbedingungen Klasse A, die unterschriebene Checkliste sowie die weiteren Belege für das geregelte Behördenzertifikat werden im Kundendossier abgelegt.

5.3 Prozess Zertifikat revozieren

5.3.1 Wer kann eine Revokation beantragen?

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

- der Inhaber selbst.
- Mitarbeiter des HR (Personaldienst)
- Linienvorgesetzte
- der SG-PKI Verantwortliche
- der SG-PKI Security Officer
- der zuständige LRAO
- der ISBO
- Zusätzlich beim Behördenzertifikat: Unterzeichnungsberechtigte Personen gemäss Eintrag im UID oder Handelsregister

5.3.2 Wie kann eine Revokation beantragt werden?

Die Revokation kann von den in Kapitel 5.3.1 erwähnten Personen jederzeit mittels signierten Formulars per Mail bei der SG-PKI beantragt werden. Der LRA-Officer, der PKI Security Officer und der PKI-Verantwortliche können ein Zertifikat direkt in der LRA-Anwendung revozieren.

5.3.3 Welches sind Gründe für eine Revokation?

Die Gründe für eine Revokation sind insbesondere:

- Die Smartcard ist gestohlen worden oder kann nicht mehr gefunden werden.
- Die Smartcard ist defekt.
- Der Inhaber hat PIN und PUK für die Smartcard vergessen.
- Beendigung des Arbeitsverhältnisses.
- Änderung von Daten, die im Zertifikat enthalten sind (Name, E-Mail-Adresse, Behördenname etc.).
- Verdacht auf Kompromittierung (bekannt werden) des privaten Schlüssels (andere Person konnte einen Dienst nutzen, z.B. eine E-Mail signieren).
- Reorganisation
- Der Inhaber/bevollmächtigte aktuelle Nutzer hält sich nicht an die Richtlinien (Nicht-Befolgen der CP/CPS oder Benutzervereinbarung).
- Der LRA-Officer hält eine Revokation aus anderen Gründen angezeigt.

5.3.4 Vorgehen

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

Der LRA-Officer geht wie folgt vor:

5.3.4.1 Plausibilisieren des Antrags

Anhaltspunkte sind:

- Kann der Antragsteller identifiziert werden? (Stimme, Telefonnummer, Revokations-passphrase)?
- Ist die HR-Stelle oder der Vorgesetzte zuständig für die Zertifikatsinhaber?
- Ist die anfragende Stelle zuständig für das Behördenzertifikat und darf die Stelle den Revokationsantrag stellen?

5.3.4.2 Formular für Revokation ausfüllen

Da bei der Klasse A die Revokation auf dem CMC-Tool stattfindet müssen die Gründe für die Revokation auf dem *Revokationsformular* festgehalten werden. Falls das Formular nicht vom Antragsteller ausgefüllt wurde, so übernimmt der LRA-Officer diese Aufgabe, füllt das Formular aus und legt es im Kundendossier ab.

5.3.4.3 Revokation

Natürliche Person:
Für die Revokation wird der Zertifikatsinhaber in der LRA-Anwendung gesucht.

Juristische Person:
Für die Revokation wird das Zertifikat anhand des CNs (Common Name) oder der E-Mail-Adresse und der Seriennummer in der LRA-Anwendung gesucht.

Danach wird das zu revozierende Zertifikat ausgewählt und revoziert. Der Zertifikatsinhaber erhält automatisch eine Mitteilung per Mail an die im Zertifikat angegebene E-Mail-Adresse über die Revokation.

5.3.4.4 Administrativer Abschluss

Das Revokationsformular wird im Original oder als Kopie im Kundendossier abgelegt. Der Revokationsvorgang wird im Journal gemäss ‚3.4 - *Journal*' dokumentiert.

6 Formulare und Checklisten

Für die obengenannten Prozesse wurden folgende Formulare und Checklisten ausgearbeitet. Alle Formulare und Checklisten können als separate Dokumente beim PKI-Verantwortlichen bezogen werden.

6.1 Formular Zertifikatsantrag

Es steht den Kunden frei, für ihre Organisation ein eigenes Formular für diesen Zweck zu entwerfen. Dabei müssen mindestens folgende Daten erhoben werden:

- Name, Vorname
- Organisationseinheit
- Art des Reisedokumentes (Reisepass oder ID)
- Nr. des Reisedokumentes
- E-Mail
- Heimatort
- Geburtsdatum

Der Kunde unterschreibt das Antragsformular und bestätigt die Korrektheit der Informationen sowie die Einhaltung der Nutzungsbedingungen. Das Formular ist Bestandteil der auditrelevanten Dokumentation eines Ausstellprozesses.

Ämter, die vom BIT unterstützt werden, bestellen das Klasse A Zertifikat für natürliche Personen auch via DWP.

6.2 Formular Benutzervereinbarung und Nutzungsbedingungen Klasse A – qualifiziert

Das Formular „Benutzervereinbarung *und Nutzungsbedingungen Klasse A – qualifiziert" [5]* enthält die wichtigsten Informationen; es wurde speziell für den Endbenutzer erstellt. Die vollständige Information ist in der CP/CPS [1] enthalten. Das Formular ist Bestandteil der auditrelevanten Dokumentation eines Ausstellprozesses.

6.3 Formular zur Revokation

Der *Revokationsantrag für qualifizierte Zertifikate für natürliche Personen* muss, wenn nicht vom Antragsteller bereits ausgefüllt geliefert, durch den LRA-Officer ausgefüllt und unterschrieben werden. Das Formular ist Bestandteil der auditrelevanten Dokumentation eines Revokationsprozesses.

Wird die Revokation eines qualifizierten Signaturzertifikates das mit dem Signaturservice benutzt wird beantragt, so muss sowohl das qualifizierte Signaturzertifikat als auch das zugehörige Schlüsselmaterial auf dem HSM des Signaturservice gelöscht werden.

6.4 Walkthrough und Checkliste Zertifikat ausstellen

Die *Walkthrough und Checkliste für die Ausstellung qualifizierter Zertifikate für natürliche Personen* dient dem LRA-Officer als Behelf bei der Ausstellung und muss ausgefüllt, unterschrieben und abgelegt werden.

6.5 Journal

Das Journal ist Bestandteil der auditrelevanten Dokumentation und wird bei jeder LRAO-Aktion mit und für Klasse A Zertifikate für natürliche Personen nachgeführt.

7 Eskalationsverfahren

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

8 Änderungsvorschläge

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

Security Officer Swiss Government PKI

Bundesamt für Informatik und Telekommunikation BIT
Campus Meielen
Eichenweg 3
CH-3003 Bern

E-Mail: pki-secoff@bit.admin.ch