Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

25.06.2025

Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B (für natürliche Personen) der Swiss Government PKI

Inkrafttretung: 01.08.2025 V2.0

Die Swiss Government PKI (SG-PKI) des Bundesamtes für Informatik (BIT), in ihrer Rolle als Trust Service Provider (TSP), betreibt im Auftrag des DTI (Digitale Transformation und IKT-Lenkung) die PKI (Public-Key-Infrastruktur) der Bundesbehörden der Schweizerischen Eidgenossenschaft. Die Zertifikate der Klasse B für die fortgeschrittene Signatur nach ZertES, für die Authentisierung und die Verschlüsselung sind im Rahmen des Standarddienstes «SD005 - Marktmodell Standarddienst: Identitäts- und Zugangsverwaltung (IAM)» definiert.

Bezug und Nutzung dieser Zertifikate der SG-PKI unterliegen den Bestimmungen dieses Dokuments. Diese werden durch die SG-PKI jährlich überprüft und falls notwendig den jeweils geltenden gesetzlichen Vorschriften und den normativen Anforderungen an Public Key Infrastrukturen angepasst.

Die jeweils gültige Version ist auf der Homepage der Swiss Government PKI publiziert. Alle Inhabende solcher Zertifikate werden über die Publikation einer aktualisierten Version dieses Dokuments per E-Mail informiert. 30 Tage nach Versand dieser Information gilt die neue Version als stillschweigend akzeptiert, ausser es erfolgt in dieser Zeit ein Auftrag zur sofortigen Revokation der Zertifikate.

Hinweis: Das Glossar finden Sie auf der PKI-Homepage.

Inhalt

Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B (für natürliche Personen) der Swiss Government PKI 1
1. Vollständigkeit und Genauigkeit der Informationen 2
2. Schutz der privaten Schlüssel und der Zertifikate 2
3. Annahme des Zertifikats 3
4. Nutzung der Zertifikate 3
5. Berichterstattung und Revokation 4
6. Beendigung des Einsatzes der Zertifikate 5
7. Verantwortung / Haftung 5
8. Rechtliche Grundlagen, Gültigkeit der Dokumente und Vertragsbestandteile 5
9. Inhalt und Gültigkeit der fortgeschrittenen Zertifikate Klasse B 5
10. Antrag und Bezug von Zertifikaten Klasse B 6
11. Anerkennungs- und Einverständniserklärung 6

1. Vollständigkeit und Genauigkeit der Informationen

Die Inhabende natürliche Person von Zertifikaten der Klasse B der Swiss Government PKI (in Folge «Inhaberin» genannt) verpflichtet sich dazu, dem Trust Service Provider (TSP), die für den Ausstellungsprozess, sowie auch für den Inhalt des Zertifikats benötigten Informationen, jederzeit korrekt und vollständig zu liefern. Durch erweiterte Prüf- und Sicherheitsmechanismen während des Ausstellungsprozesses des Zertifikats wird die Identität der antragstellenden Person (in Folge «Antragstellerin» genannt) auf einer hohen Sicherheitsstufe festgestellt. So muss unter anderem vor der Ausstellung des Zertifikats die Antragstellerin bei persönlicher Anwesenheit anhand eines für die Einreise in die Schweiz, gültigen Reisedokuments identifiziert werden. Das Zertifikat ist untrennbar an die Inhaberin gebunden.

Vorname(n)/ Nachname(n), Suffix und E-Mailadresse der Inhaberin werden im Zertifikat immer aufgeführt (Eintrag im Admin-Directory des Bundes). Es werden weitere persönliche Angaben wie Geburtsdatum und Revokationspassphrasen, sowie der Scan des gültigen Identifikationsdokumentes bei der SG-PKI erfasst und gespeichert.

Die Inhaberin ist verpflichtet den TSP zu informieren, sobald sich ihre Daten, die im Zertifikat hinterlegt sind, ändern.

2. Schutz der privaten Schlüssel und der Zertifikate

Die privaten Schlüssel der Zertifikate der Klasse B werden auf einer persönlichen Smartcard gespeichert. Für die Aktivierung der privaten Schlüssel zur Erzeugung einer elektronischen Signatur, die Authentisierung und/oder die Entschlüsselung, muss die Inhaberin die PIN der Smartcard Klasse B verwenden. Die PIN der Smartcard kann bei Bedarf von Inhaberin selbständig im Safenet Authentication Client (SAC) geändert werden. Eine PIN darf nur für genau eine Smartcard verwendet werden, wird eine Smartcard ersetzt, muss eine neue PIN gewählt werden. Diese PIN soll für keine anderen Zwecke (z.B. Postcard) eingesetzt werden. Die PIN darf nicht weitergegeben werden und muss geändert werden, sobald der Verdacht besteht, dass eine andere Person Kenntnis davon erhalten hat. Die Zertifikate (und somit der Zertifikatsträger: Smartcard, USB-Stick, etc.) müssen mit einer mind. 6-stelligen PIN gesichert werden (max. 14 Zeichen), wobei rein numerische PINs, sowie gemischte PINs erlaubt sind. Sonderzeichen sind in der PIN der Klasse B Zertifikate explizit nicht erlaubt. Die Inhaberin verpflichtet sich dazu, alle angemessenen Vorkehrungen zu treffen, um die alleinige Kontrolle, die Vertraulichkeit und den Schutz vor Verlust und Missbrauch der privaten Schlüssel und der allfällig damit verbundenen Aktivierungsdaten (PIN) und Smartcard, zu gewährleisten. Die privaten Schlüssel der Zertifikate können und dürfen nur im Zusammenhang mit den Zertifikaten und nur für den in den Zertifikaten festgelegten Zwecken (Signatur, Authentifizierung, Verschlüsselung) eingesetzt werden.

Falls die Inhaberin die PIN vergisst oder mehrmals falsch eingibt, kann die Inhaberin eine neue PIN setzen, in- dem sie sich bei einem von der SG-PKI berechtigten PIN-Reset Superuser meldet und von diesem identifizieren lässt. Diese Identifikation kann mittels einer bei der Ausstellung festgelegten Passphrase und der passenden Antwort erfolgen. Der PIN-Reset Superuser gibt ein eTicket frei und die Inhaberin kann sich nach erneuter Identifikation bei einem von der Organisation festgelegten PIN-Reset User (PRU) eine neue PIN setzen.

Private Schlüssel von Zertifikaten der Klasse B sind nicht übertragbar und dürfen auf keinen Fall unberechtigten[1] Dritten zugänglich gemacht werden. Die privaten Schlüssel der Klasse B Zertifikate sind auf dem Zertifikatsträger (z. B. Smartcard) als nicht exportierbar gekennzeichnet.

[1] Der Begriff «unberechtigte Dritte» beinhaltet in Kontext dieses Dokumentes jede weitere Person, welche nicht aufgrund eines Todesfalls oder richterlichen Verfahrens dazu ermächtigt wurde, Informationen zum Zertifikat wiederherzustellen.

Die Inhaberin haftet für jeden Schaden, der durch die Weitergabe der privaten Schlüssel, der Zugangsdaten zum Schlüssel oder der allfällig damit verbundenen Aktivierungsdaten oder Smartcard, an Dritte entstanden ist.

Die eingesetzten Smartcards entsprechen den Anforderungen des ZertES. Alle Komponenten müssen ebenfalls vom BIT zugelassen worden sein. Eine Liste der zugelassenen Komponenten ist auf der Seite der Swiss Government PKI Klasse B - Standards, Vorgaben und rechtliche Grundlagen publiziert.

Der Trust Service Provider (TSP) behält sich vor, die Zertifikate bereits bei einem konkreten Verdacht auf Missbrauch oder unautorisierten Zugang zum privaten Schlüssel ohne Vorinformation sofort zu revozieren.

3. Annahme des Zertifikats

Die Inhaberin überprüft den Inhalt des Zertifikats bei Erhalt und stellt sicher, dass dieser über die gesamte Laufzeit korrekt ist.

4. Nutzung der Zertifikate

Fortgeschrittene Zertifikate Klasse B für natürliche Personen können für folgende Zwecke verwendet werden:

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

Die Inhaberin stellt sicher, dass ihr Inhalt, Zweck und Wirkung des Einsatzes der Klasse B Zertifikate bekannt sind. Sie verpflichtet sich, die Klasse B Zertifikate und deren privaten Schlüssel nur für autorisierte Geschäfte und unter Einhaltung der geltenden gesetzlichen Vorschriften (s. Kapitel 8 Rechtliche Grundlagen, Gültigkeit der Dokumente und Vertragsbestandteile) sowie der Bestimmungen dieses Dokuments einzusetzen.

Fortgeschrittene Zertifikate Klasse B erfüllen ausschliesslich den oben genannten Zweck und geben keinerlei weitere Aufschlüsse, Versicherungen oder Garantien. Insbesondere garantieren fortgeschrittene Zertifikate der Klasse B nicht, dass die Inhaberin im Umgang mit dem Zertifikat korrekt und legal handelt.

Des Weiteren garantieren fortgeschrittene Zertifikate Klasse B nicht, dass:

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

Die Swiss Government PKI bestätigt zum Zeitpunkt der Erstausstellung eines fortgeschrittene Zertifikats Klasse B folgende Tatsachen:

- *Rechtlich gültige Existenz:* Die im Zertifikat genannte Inhaberin existiert als natürliche Person und verfügt über einen persönlichen Eintrag im Admin-Directory des Bundes.
- *Identität:* Der Name der im Zertifikat genannten Inhaberin stimmt mit dem Namen in ihrem gültigen Identifikationsdokument überein.

- *Autorisierung:* Die SG-PKI hat alle notwendigen und zumutbaren Schritte unternommen, um zu verifizieren, dass die im Zertifikat genannte Inhaberin zum Bezug des Zertifikats autorisiert ist.
- *Richtigkeit der Daten:* Die SG-PKI hat alle notwendigen und zumutbaren Schritte unternommen, um sicherzustellen, dass alle im Zertifikat enthaltenen Daten und Informationen korrekt sind.
- *Status:* Die SG-PKI stellt den Status des Zertifikats sowie Informationen über dessen Gültigkeit/Revokation 7x24 Std. online abrufbar zur Verfügung und erfüllt damit die gesetzlichen Vorgaben.

Bei Fragen oder Problemen in der Nutzung der Zertifikate kann ihr lokaler Service Desk oder der Service Desk BIT (Tel.: +41 (0)58 465 88 88) kontaktiert werden. Für ein Beschwerdeverfahren oder bei Fragen zu diesem Dokument, kann die SG-PKI unter der E-Mailadresse pki-info@bit.admin.ch kontaktiert werden.

5. Berichterstattung und Revokation

Die Inhaberin verpflichtet sich dazu, die Zertifikate und die dazugehörigen privaten Schlüssel unverzüglich nicht mehr einzusetzen und beim TSP (z.B. Local Registration Authority Officer/LRAO der SG-PKI in der Organisation der Inhaberin) sofort die Revokation (Ungültigerklärung) der Zertifikate zu verlangen, wenn:

- der konkrete Verdacht besteht, dass mit einem Zertifikat verdächtige Aktivitäten (Kompromittierung/Missbrauch der Aktivierungsdaten, des Authentifizierungszertifikats, des Signaturzertifikats oder des Verschlüsselungszertifikats) unternommen wurden;
- die Informationen in den Zertifikaten nicht mehr korrekt oder ungenau sind, oder es in naher Zukunft sein werden;
- ein allfälliger Verlust der Smartcard bemerkt wird.

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

Die Inhaberin kann die Revokation persönlich oder per Telefon beantragen. Der TSP oder die von ihm beauftragte Person (z.B. LRAO) wird die Inhaberin identifizieren.

Weitere Personen, die eine Revokation beantragen dürfen, müssen die Anfrage schriftlich mittels (elektronischem) Revokationsformular einreichen. Befugte Personen sind:

- die Inhaberin selbst
- Linienvorgesetzte der Inhaberin
- der oder die SG-PKI Verantwortliche
- der/die SG-PKI Security Officer
- der oder die zuständige LRAO der SG-PKI
- der Informatiksicherheitsbeauftragter oder die Informatiksicherheitsbeauftragte der Organisationseinheit (ISBO) oder des Departements (ISBD)
- Mitarbeitende des für die Inhaberin zuständigen HR (Personaldienst)

Unmittelbar nach erfolgter Sperrung kann beim TSP die Ausstellung von neuen Zertifikaten beantragt werden. Der Prozess der Ausstellung von neuen Zertifikaten entspricht der Erstausstellung.

Informationen betreffend der Identifikation, der Ausstellung der Zertifikate und der Revokation werden durch den TSP aus Gründen der Nachvollziehbarkeit erfasst und gemäss den gesetzlichen Vorschriften bearbeitet und aufbewahrt. Die Aufbewahrungsfrist von 11 Jahren beginnt mit dem Ablauf der Zertifikate bzw. mit deren Ungültigerklärung.

Wenn aus Sicherheitsgründen erforderlich und aus datenschutzrechtlicher Sicht erlaubt, kann der TSP Daten über die Inhaberin, die Zertifikate und weitere in unmittelbarem Zusammenhang stehende Informationen an andere zuständige Stellen, TSPs, Firmen und industrielle Gruppen weiterleiten, wenn die

Zertifikate oder deren Inhaberin, welche die Zertifikate einsetzt, als Quellen einer missbräuchlichen Verwendung identifiziert werden.

6. Beendigung des Einsatzes der Zertifikate

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

7. Verantwortung / Haftung

Die Inhaberin ist dafür verantwortlich, dass ihre Zertifikate Klasse B und die zugehörigen privaten Schlüssel nur unter Einhaltung der Bestimmungen in Abschnitt Nutzung der Zertifikate (Kap.4)» dieses Dokuments eingesetzt werden. Ein Verstoss gegen diese Vorgabe hat eine Revokation der Zertifikate und allenfalls weitere administrative und juristische Massnahmen zur Folge. Die Inhaberin trägt die Verantwortung für alle durch sie vorgenommenen Signaturen, Authentisierungen und Verschlüsselungen sowie für allfällige, aus pflichtwidriger Verwendung resultierende Schäden und deren Folgen.

8. Rechtliche Grundlagen, Gültigkeit der Dokumente und Vertragsbestandteile

Die nachfolgenden rechtlichen Grundlagen und weiteren Vorgaben bilden integrierenden Bestandteil dieser Benutzervereinbarung. Sie sind in der anwendbaren Rangfolge aufgelistet:

1. Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate. ZertES, SR 943.03
2. Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate. VZertES, SR 943.032
3. Verordnung des BAKOM über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate. SR 943.032.1
4. CP/CPS Root CA I der SG-PKI
5. «Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B (für natürliche Personen) der Swiss Government PKI» (vorliegendes Dokument)
6. Normative Anforderungen an Public Key Infrastrukturen

Die geltenden gesetzlichen Vorgaben, Policies und Richtlinien für geregelte und fortgeschrittene Zertifikate Klasse B sind im Internet auf der Website der Swiss Government PKI Klasse B - Standards, Vorgaben und rechtliche Grundlagen publiziert oder verlinkt.

9. Inhalt und Gültigkeit der fortgeschrittenen Zertifikate Klasse B

Die Zertifikate der SG-PKI enthalten Informationen betreffend:

- Herausgeber (TSP) und ausstellender Certificate Authority (CA)
- Informationen über die Root CA der ausstellenden CA
- Informationen über die geltende Policy
- Ausstell- und Ablaufdatum des Zertifikats
- Seriennummer des Zertifikats
- Informationen betreffend der CRL und dem OCSP
- Informationen betreffend der Inhaberin des Zertifikats zum Zeitpunkt der Erstausstellung:
  - Vorname(n), Nachname(n) und Suffix aus dem Admin-Directory (Common Name der Inhaberin (CN))
  - E-Mail-Adresse der Inhaberin
  - Optional den User Principal Name (UPN)
  - öffentlicher Schlüssel

Die Zertifikate sind max. 3 Jahre gültig. Vor Ablauf der 3-Jahres-Frist können die Zertifikate maximal zwei Mal von der Inhaberin selbst für weitere drei Jahre erneuert werden. Für die Erneuerung des Zertifikates steht der Inhaberin der Renewal Wizard zur Verfügung. Nach Ablauf der 3. Gültigkeitsperiode muss durch den LRA-Officer ein neues Zertifikat gemäss dem Prozess der Erstausstellung ausgestellt werden. Das Ausstellverfahren bleibt auch im diesem Fall dasselbe wie bei der Erstausstellung. Eine persönliche Vorsprache mit einer Neuidentifizierung und den nötigen Dokumenten ist dabei Voraussetzung.

10. Antrag und Bezug von Zertifikaten Klasse B

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

- Ein für die Einreise in die Schweiz gültiges Reisedokument (ID/ Pass), ausgestellt auf die zukünftige Inhaberin. Das Ablaufdatum darf nicht überschritten sein.
- Ausgefülltes und (elektronisch, min. mit Klasse B) signiertes Antragsformular für Zertifikate Klasse B der SG-PKI oder eine schriftliche Anmeldung über die Linie der Organisation, bzw. über den internen festgelegten HR-Prozess.
- Persönlicher Eintrag im Admin-Directory des Bundes, mit Nachnamen(n), Vorname(n) (gemäss Reisedokument), gültiger E-Mailadresse und optional einem (User Principals Name = UPN-Eintrag).
- Unterschriebene «Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B (für natürliche Personen) der Swiss Government PKI» (vorliegendes Dokument).

Die persönliche Identifizierung der antragstellenden Person, wird durch die Local Registration Authority Officer (LRAO) der Klasse B der SG-PKI bei der Erstausstellung und spätestens nach Ablauf der dritten Gültigkeitsperiode sichergestellt. Bei einer dezentralen Ausstellung von Zertifikaten der Klasse B wird die persönliche Identifizierung von einer delegierten Person des LRAO, dem RIO (Registration Identification Officer) übernommen, der die Bestätigung der durchgeführten Identifizierung dem LRAO zur Freigabe des Antrages weiterleitet. Die Antragstellerin muss für die Ausstellung des Zertifikats persönlich erscheinen. Um die Antragstellerin zu verifizieren und zu identifizieren, wird das Reisedokument durch den LRAO oder den RIO bei der Ausstellung auf Gültigkeit, Richtigkeit und Echtheit überprüft. Die LRAO und RIO sind zudem angewiesen, das Bild des Dokuments mit der vor Ihnen stehenden Person zu vergleichen. Ebenso wird der Antrag vor der Ausstellung eines fortgeschrittenen Zertifikates plausibilisiert (Person arbeitet tatsächlich in der angegebenen Organisationseinheit, benötigt das Zertifikat im geschäftlichen Alltag; die Antragstellerin ist berechtigt ein Zertifikat zu beantragen).

Sind für die Antragstellung noch zusätzliche Informationen nötig, so hat die Antragstellerin 10 Tage Zeit diese der SG-PKI nachzureichen. Danach erlischt der Antrag automatisch.

11. Anerkennungs- und Einverständniserklärung

Die Antragstellerin nimmt zur Kenntnis, dass der TSP 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.

Die Antragstellerin bezeugt mit ihrer Unterschrift, dass sie das vorliegende Dokument «Benutzervereinbarung und Nutzungsbedingungen für fortgeschrittene Zertifikate der Klasse B (für natürliche Personen) der Swiss Government PKI» gelesen und verstanden hat und die darin aufgeführten Bestimmungen akzeptiert.

Name, Vorname (Antragsteller/in):	(elektronische Kl. B) Signatur Antragstellerin:
Ort/Datum:	