Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

Nicht klassifiziert

Benutzervereinbarung und Nutzungsbedingungen für Zertifikate der Klasse A – Geregelte und qualifizierte Zertifikate gemäss ZertES (für juristische und natürliche Personen)

V2.3, 27.11.2023

Die Swiss Government 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 A für die geregelte oder qualifizierte Signatur (nachfolgend Zertifikate genannt) nach ZertES sind im Rahmen des Marktmodells «SD005 - Marktmodell Standarddienst: Identitäts- und Zugangsverwaltung (IAM)» definiert. Bezug und Nutzung dieser Zertifikate der Swiss Government PKI (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 www.pki.admin.ch publiziert. Alle Inhaberinnen 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 des Zertifikats.

Inhalt

1 Genauigkeit der Informationen

Die inhabende natürliche oder juristische Person[1] von Zertifikaten der Klasse A der Swiss Government PKI (in Folge «Inhaberin[2]» genannt) verpflichtet sich dazu, dem 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[3]» genannt) auf einer hohen Sicherheitsstufe festgestellt. So muss unter anderem vor der Ausstellung des Zertifikats die Antragstellerin bei persönlicher Anwesenheit anhand eines gültigen Reisedokuments zweifelsfrei identifiziert werden. Das Zertifikat ist untrennbar an die Inhaberin gebunden.

- Zertifikate für natürliche Personen:

  Vorname(n), Nachname(n), Suffix (seines Eintrages im Admin-Directory des Bundes) und E-Mailadresse der Inhaberin werden im Zertifikat immer aufgeführt. Es werden weitere persönliche

[1] Gemäss ZertES können geregelte Zertifikate für natürliche Personen und UID-Einheiten ausgestellt werden. SG-PKI stellt geregelte Zertifikate nur für juristische Personen aus, welche im UID-Register erfasst sind. Für natürliche Personen stellt SG-PKI qualifizierte Zertifikate aus.

[2] Der Begriff «Inhaberin» beschreibt die natürliche oder juristische Person, auf welche das Zertifikat ausgestellt wurde. Die juristische Person kann zum Beispiel eine Behörde sein.

[3] Der Begriff «Antragstellerin» beschreibt die natürliche Person, die das Zertifikat für sich oder für die von ihr in Vertretungsmacht vertretene juristische Person beantragt.

Angaben wie Geburtsdatum und Revokationspassphrasen, sowie der Scan des gültigen Reisedokumentes bei der SG-PKI erfasst und gespeichert.

- Zertifikate für juristische Personen:

  Die Antragstellerin muss bevollmächtigt sein, die Inhaberin zu vertreten. Die schriftlichen Vollmachtsurkunden und die Revokationspassphrase, sowie der Scan des gültigen Reisedokumentes der Antragstellerin werden bei der SG-PKI erfasst und gespeichert.

  Die Inhaberin wird in Form eines „Distinguished Name“ gemäss Standard X.509 im Zertifikat beschrieben. Das Zertifikat enthält die UID und den offiziellen Namen der juristischen Person (z.B. Behörde) in den entsprechenden Attributen „Organization“ und „OrganizationIdentifier“.

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

2 Schutz des privaten Schlüssels und des Zertifikats

Der private Schlüssel des Zertifikats der Klasse A wird auf einer Smartcard Klasse A oder einem zentralen Hochsicherheitsspeicher (HSM, Signaturdienst) der SG-PKI gespeichert.

- Smartcard:

  Für die Aktivierung des privaten Schlüssels zur Erzeugung einer elektronischen Signatur muss der Nutzer oder die Nutzerin die PIN der Smartcard Klasse A verwenden. Zur PIN gibt es einen PUK, der es ermöglicht, eine neue PIN zu setzen, wenn die PIN vergessen, oder zu oft falsch eingegeben wurde und die Smartcard deswegen blockiert ist. Läuft ein Zertifikat ab, muss eine neue PIN gewählt werden.

- BIT Signaturdienst:

  Für die Aktivierung des Schlüssels zur Erzeugung einer elektronischen Signatur muss der Nutzer oder die Nutzerin in der entsprechenden Anwendung das auf ihrer persönlichen Smartcard der Klasse B gespeicherte Authentisierungszertifikat mit der zugehörigen PIN oder die persönliche MobileID verwenden. Wird der Signaturdienst aus einer Fachanwendung genutzt und dabei zur Aktivierung des Schlüssels zur Erzeugung einer elektronischen Signatur ein gemeinsamer in der Anwendung hinterlegter Schlüssel genutzt, so muss der Schlüssel und die Zugangsdaten nachweislich sicher aufbewahrt werden.
  Bei Verwendung der MobileID sind die separaten Nutzungsbedingungen der MobileID integraler Bestandteil dieses Dokuments (https://www.mobileid.ch/de/dokumente).

Regeln in Bezug auf die PIN gelten auch für den PUK. Die PIN und PUK der Smartcard können bei Bedarf vom Nutzer oder der Nutzerin selbständig im Safenet Authentication Client (SAC) geändert werden. Eine PIN darf nur für genau eine Smartcard verwendet werden. Diese PIN darf für keine anderen Zwecke (z.B. Postcard) eingesetzt werden. Die PIN muss geändert werden, sobald der Verdacht besteht, dass eine andere unbefugte Person Kenntnis davon erhalten hat. Die Inhaberin verpflichtet sich, alle angemessenen Vorkehrungen zu treffen, um die Kontrolle, die Vertraulichkeit und den Schutz vor Verlust und Missbrauch des privaten Schlüssels und der allfällig damit verbundenen Zugangsdaten (z.B. PIN/PUK) und Token zu gewährleisten. Der private Schlüssel des Zertifikats kann und darf nur im Zusammenhang mit dem Zertifikat und nur für den im Zertifikat festgelegten Zweck (Signatur) eingesetzt werden.

Private Schlüssel von Zertifikaten für natürliche Personen sind nicht übertragbar und dürfen auf keinen Fall Dritten zugänglich gemacht werden.

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

Die eingesetzten Smartcards und HSM entsprechen den Anforderungen des ZertES. Alle Komponenten müssen ebenfalls vom BIT zugelassen worden sein. Eine Liste der zugelassenen Komponenten ist auf der Seite www.pki.admin.ch publiziert.

Der TSP behält sich vor, das Zertifikat bereits bei einem konkreten Verdacht auf Missbrauch oder unautorisierten Zugang zum privaten Schlüssel ohne Vorinformation 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 des Zertifikats

- Qualifizierte Zertifikate für natürliche Personen:

  Qualifizierte Zertifikate Klasse A für natürliche Personen werden ausschliesslich für die vertrauenswürdige, rechtsgültige, der eigenhändigen Unterschrift gleichgestellten, elektronischen Signatur eingesetzt. Sie bestätigen die Authentizität und Unversehrtheit von Dokumenten, sowie das Einverständnis des Signierenden mit dessen Inhalt. Die Inhaberin stellt sicher, dass ihr Inhalt, Zweck und Wirkung des Einsatzes des Zertifikats bekannt sind. Sie verpflichtet sich, das Zertifikat und dessen privaten Schlüssel unter Einhaltung aller geltenden gesetzlichen Vorschriften sowie den Bestimmungen dieses Dokuments und im Einklang mit den Vorgaben ihrer jeweils zuständigen Verwaltungseinheit / Arbeitgeberin einzusetzen.

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

  Des Weiteren garantieren qualifizierte Zertifikate Klasse A 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 Ausstellung eines qualifizierten Zertifikats Klasse A folgende Tatsachen:

  - Rechtlich gültige Existenz: Die im Zertifikat genannte Inhaberin existiert als natürliche oder juristische Person.
  - Identität: Der Name der im Zertifikat genannten Inhaberin (exkl. Suffix) stimmt mit dem Namen in ihrem gültigen Reisedokument 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 die gesetzlichen Vorgaben.
  - Nutzungsbedingungen: Die Antragstellerin wurde vom LRAO (Local Registration Authority Officer) über die im vorliegenden Dokument beschriebenen Rechte und Pflichten informiert. Ihre Fragen diesbezüglich wurden vom LRAO der SG-PKI verständlich beantwortet. Die Antragstellerin hat dieses gelesen, akzeptiert und unterzeichnet
  - Revokation: Die SG-PKI kann das Zertifikat gegebenenfalls aus den im vorliegenden Dokument genannten Gründen unverzüglich revozieren

- Geregelte Zertifikate für juristische Personen:

  Geregelte Zertifikate Klasse A für juristische Personen, oft auch Behördenzertifikate genannt, unterliegen den Bestimmungen des ZertES, VZertES und weiteren rechtlichen Vorgaben. Sie können ausschliesslich für das Signieren von elektronischen Dokumenten eingesetzt werden.

  Durch die Signatur mit einem geregelten Zertifikat Klasse A für juristische Personen werden elektronische Siegel erzeugt. Verwaltungsstellen und Behörden können amtliche Dokumente mit einem für die betreffende Amtsstelle ausgestellten Zertifikat zusammen mit einem qualifizierten Zeitstempel (ZertES, Art. 2j) digital signieren. Bürger und Unternehmen sollen die Möglichkeit haben amtliche Dokumente, die von Behörden elektronisch signiert (gesiegelt) worden sind zu prüfen, um sicherzustellen, dass diese Dokumente tatsächlich von der entsprechenden Behörde stammen. Durch den zusätzlich angebrachten Zeitstempel wird der Zeitpunkt der Signatur genau bestimmt.

  Geregelte Zertifikate Klasse A erfüllen ausschliesslich den oben genannten Zweck und geben keinerlei weitere Aufschlüsse, Versicherungen oder Garantien. Insbesondere garantieren diese nicht, dass die das Zertifikat nutzende natürliche Person im Umgang mit dem Zertifikat korrekt und legal handelt.

  Des Weiteren garantieren geregelte Zertifikate Klasse A nicht, dass:

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

  Die Swiss Government PKI bestätigt zum Zeitpunkt der Ausstellung eines geregelten Zertifikats Klasse A folgende Tatsachen:

  - Rechtlich gültige Existenz: Die im geregelten Zertifikat genannte juristische Person existiert und verfügt über einen Eintrag im öffentlichen UID-Register (www.uid.admin.ch)
  - Identität: Der Name, der im geregelten Zertifikat im Attribut „O=“ des Zertifikats angezeigt wird, stimmt mit dem Namen der im UID-Register registrierten juristischen Person überein.
  - Autorisierung: Die SG-PKI hat alle notwendigen und vom Gesetz (ZertES) verlangten Schritte unternommen, um zu verifizieren, dass die Antragstellerin 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.
  - Nutzungsbedingungen: Die Antragstellerin wurde vom LRAO (Local Registration Authority Officer) über die im vorliegenden Dokument beschriebenen Rechte und Pflichten informiert. Ihre Fragen diesbezüglich wurden vom LRAO der SG-PKI verständlich beantwortet. Die Antragstellerin hat dieses gelesen, akzeptiert und unterzeichnet.
  - Status: Die SG-PKI stellt den Status des Zertifikats sowie Informationen über dessen Gültigkeit/Revokation 7x24 Std. online abrufbar zur Verfügung und erfüllt die gesetzlichen Vorgaben der ZertES sowie der VZertES und weiteren rechtlichen Vorgaben.
  - Revokation: Die SG-PKI kann das Zertifikat gegebenenfalls aus den im vorliegenden Dokument genannten Gründen unverzüglich revozieren.

  Für dieselbe juristische Person können mehrere Zertifikate ausgestellt werden. Dabei können die Anträge von derselben berechtigten Person gestellt werden.

  - Smartcard:

    Ist der private Schlüssel auf einer Smartcard gespeichert, so dürfen die Zugangsdaten für die Nutzung des Zertifikats für eine juristische Person von der Antragstellerin geordnet an Mitarbeitende abgegeben werden, wobei die Antragstellerin im Namen der juristischen

Person persönlich die Verantwortung trägt. Die Weitergabe der Smartcard und der Zugangsdaten ist nachvollziehbar und lückenlos, schriftlich festzuhalten.

- Signaturdienst:
  Ist der private Schlüssel zur Nutzung mit dem Signaturdienst auf einem HSM gespeichert, so können entweder mehrere Benutzer mit ihrem persönlichen Klasse B Zertifikat oder der persönlichen MobileID authorisiert werden oder bei Fachanwendungen kann ein gemeinsames TLS-Zertifikat in der Fachanwendung hinterlegt werden. Dieses hinterlegte TLS-Zertifikat, welches die Nutzung des eigentlichen Signaturzertifikats für eine juristische Person freischaltet und die Zugangsdaten dazu können von der Antragstellerin geordnet an Mitarbeitende abgegeben werden, wobei die Antragstellerin im Namen der juristischen Person persönlich die Verantwortung trägt. Die Weitergabe der Zugangsdaten ist nachvollziehbar und lückenlos, schriftlich festzuhalten. Fachanwendungen mit Authentifikation über ein TLS-Zertifikat können nur nach einem Audit durch einen externen Auditor an den Signaturdienst angebunden werden.
  Bei Verwendung der MobileID sind die separaten Nutzungsbedingungen der MobileID integraler Bestandteil dieses Dokuments (https://www.mobileid.ch/de/dokumente).

Die Antragstellerin haftet für jeden Schaden, der durch die Weitergabe der Zugangsdaten zum privaten Schlüssel und der allfällig damit verbundenen Medien, an Dritte entstanden ist.

Die Antragstellerin stellt sicher, dass ihr und allfälligen anderen berechtigten Nutzern Inhalt, Zweck und Wirkung des Einsatzes des geregelten Zertifikats der Klasse A bekannt sind. Sie verpflichtet sich, das Klasse A Zertifikat und dessen privaten Schlüssel unter Einhaltung aller geltenden gesetzlichen Vorschriften sowie den Bestimmungen dieses Dokuments einzusetzen. Die Antragstellerin setzt ihre Mitbenutzer und Mitbenutzerinnen nachweislich vollumfänglich über die Vorschriften und dieses Dokument in Kenntnis.

Das Signieren erfolgt mittels Zertifikats und einer Signatursoftware. Zum Zeitpunkt der Freigabe dieses Dokuments sind die dafür von der SG-PKI empfohlenen Anwendungen der DesktopSigner und der BIT-Signaturdienst. Die Prüfung der Signatur beim Empfänger erfolgt über den Validator (Service unter: www.validator.admin.ch. Eine elektronische Signatur ist nur dann gültig, wenn sie mit einem qualifizierten Zeitstempel durchgeführt wurde. Um eine Langzeitvalidierung (LTV) zu gewährleisten wird empfohlen die Signatur gemäss LTV Standard anzubringen, d.h. dass zusätzlich immer ein Zeitstempel anzubringen ist. Der Stempel kann von SG-PKI bezogen werden (Time-Stamping-Authority/TSA).

Bei Fragen oder Problemen in der Nutzung der Zertifikate kann ihr lokaler Service Desk oder der Service Desk BIT (Tel.: 058 465 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, das Zertifikat und den dazugehörigen privaten Schlüssel unverzüglich nicht mehr einzusetzen beziehungsweise nicht mehr zum Einsatz freizugeben und vom Einsatz zurückzuziehen und beim TSP (z.B. LRAO der SG-PKI in der Organisation des Inhabers) sofort die Revokation (Ungültigerklärung) des Zertifikats zu verlangen, wenn:

- der konkrete Verdacht besteht, dass mit dem Zertifikat verdächtige Aktivitäten (Kompromittierung/Missbrauch des Signaturzertifikats) unternommen wurden;
- die Informationen im Zertifikat nicht mehr korrekt oder ungenau sind, oder es in naher Zukunft sein werden;
- ein allfälliger Verlust der Smartcard bemerkt wird.
- Bei Verwendung der MobileID: Verlust des Smartphones

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

Die ursprüngliche Antragstellerin kann die Revokation persönlich, via signierte E-Mail oder per Telefon beantragen. Der TSP oder die von ihm beauftragte Person (z.B. LRAO) wird die Inhaberinzweifelsfrei identifizieren.

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

Befugte Personen sind:

- die Inhaberin selbst (für juristische Personen: eine bevollmächtigte Person der Inhaberin)
- die ursprüngliche Antragstellerin
- Linienvorgesetzte der Inhaberin oder Antragstellerin
- der oder die SG-PKI Verantwortliche
- ein SG-PKI Security Officer oder eine SG-PKI Security Officerin
- der oder die zuständige LRAO der SG-PKI
- der Informatiksicherheitsbeauftragter oder die Informatiksicherheitsbeauftragte der Organisationseinheit (ISBO)
- bei Zertifikaten für natürliche Personen: Mitarbeitende des für die Inhaberin zuständigen HR (Personaldienst)

Wenn aus Sicherheitsgründen erforderlich und aus datenschutzrechtlicher Sicht erlaubt, kann der TSP Daten über die Inhaberin, das Zertifikat und weitere in unmittelbarem Zusammenhang stehende Informationen an andere zuständige Stellen, TSP, Firmen und industrielle Gruppen weiterleiten, wenn das Zertifikat oder die Person, die das Zertifikat einsetzt, als Quelle verdächtiger Aktivitäten identifiziert wird.

Alle Informationen betreffend der Revokation werden durch den TSP aus Gründen der Nachvollziehbarkeit gemäss den gesetzlichen Vorschriften archiviert.

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

6 Beendigung des Einsatzes des Zertifikats

Die Inhaberin verpflichtet sich dazu, den Einsatz des Zertifikats nach dessen Ablauf oder Revokation (insbesondere aufgrund einer Kompromittierung) sofort zu unterlassen.

7 Verantwortung / Haftung

Die Inhaberin ist dafür verantwortlich, dass ihr Zertifikat Klasse A und die zugehörigen privaten Schlüssel nur unter Einhaltung aller geltenden gesetzlichen Vorschriften, sowie den Bestimmungen in Abschnitt «Nutzung des Zertifikats» dieses Dokuments eingesetzt wird. Ein Verstoss gegen diese Vorgabe hat eine Revokation des Zertifikats und allenfalls weitere administrative und juristische Massnahmen zur Folge. Die Inhaberin trägt die Verantwortung für alle durch sie vorgenommenen Signaturen sowie für allfällige, aus pflichtwidriger Verwendung resultierende Schäden und deren Folgen.

Die SG-PKI haftet gegenüber der Inhaberin des Zertifikats und Drittpersonen, die sich auf ein gültiges Zertifikat verlassen haben, gemäss Art. 17 ZertES für Schäden, die diese erleiden, weil die SG-PKI den Pflichten aus dem Bundesgesetz über die elektronische Signatur und den entsprechenden Ausführungsbestimmungen nicht nachgekommen ist.

Die Haftung der SG-PKI ist auf das nach dem anwendbaren Recht zulässige Mass beschränkt:

- bei Vertragsverletzungen haftet die SG-PKI für den nachgewiesenen Schaden, sofern sie nicht beweist, dass sie kein Verschulden trifft.
- bei grober Fahrlässigkeit auf höchstens Fr. 100'000.- je Schadenereignis und Kalenderjahr.
- bei leichter Fahrlässigkeit auf den Gegenwert der während des laufenden Vertragsjahres erbrachten Leistungen, höchstens aber Fr. 50'000.- je Schadenereignis und Kalenderjahr.

Die SG-PKI lehnt jede weitergehende Haftung ab. Insbesondere haftet sie nicht für Schäden, die entstehen, weil die Inhaberin die ausgestellten Zertifikate zu anderen als den in den geltenden gesetzlichen Vorschriften und in den Bestimmungen in Abschnitt «Nutzung des Zertifikats» dieses Dokuments festgelegten Zwecken nutzt.

Die Haftung für Folgeschäden, entgangenen Gewinn und Datenverluste ist ausdrücklich ausgeschlossen.

Die SG-PKI haftet des Weiteren nicht für Schäden und Verzugsfolgen, die durch höhere Gewalt, Naturereignisse (z.B. Blitzschlag, Elementarereignisse), Stromversorgungsausfälle, kriegerische Ereignisse, Streik, unvorhersehbare behördliche Restriktionen, Umgehung von Sperrsets, PC-Dialer, Hackerattacken, Virenbefall (inkl. Trojanische Pferde u. ä.) von Datenverarbeitungsanlagen usw. entstehen. Kann die SG-PKI ihren vertraglichen Pflichten infolge eines derartigen Ereignisses nicht nachkommen, wird die Vertragserfüllung oder der Termin für die Vertragserfüllung dem eingetretenen Ereignis entsprechend hinausgeschoben. Die SG-PKI haftet nicht für allfällige Schäden, die dem Kunden durch das Herausschieben der Vertragserfüllung entstehen.

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) Bundesgesetz über die Unternehmens-Identifikationsnummer 2010, SR 431.03
5) CP/CPS Root CA IV der SG-PKI (http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf)
6) «Benutzervereinbarung und Nutzungsbedingungen für Zertifikate der Klasse A – Geregelte und qualifizierte Zertifikate gemäss ZertES (für juristische und natürliche Personen)» (vorliegendes Dokument)
   Bei Verwendung der MobileID: die Nutzungsbedingungen der MobileID (https://www.mobileid.ch/de/dokumente)

Die geltenden gesetzlichen Vorgaben, Policies und Richtlinien für geregelte und qualifizierte Zertifikate Klasse A sind im Internet auf der Website der SG-PKI (www.pki.admin.ch) publiziert oder verlinkt.

9 Inhalt und Gültigkeit der geregelten und qualifizierten Zertifikate Klasse A

Die Zertifikate der SG-PKI enthalten Informationen betreffend:

- Informationen über die Root CA und die ausstellende 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:
  - Nachname Vorname gemäss Reisepass/Identitätskarte beziehungsweise UID und offiziellen Namen der Inhaberin bei juristischen Personen
  - Common Name der Inhaberin (Nachname(n) Vorname(n) Suffix)
  - E-Mail-Adresse
- öffentlicher Schlüssel

Das Zertifikat ist max. 3 Jahre gültig. Nach Ablauf der 3 Jahre muss durch den TSP ein neues Zertifikat mit persönlicher Neuidentifizierung ausgestellt werden. Es kann von der Inhaberin nicht selbst erneuert werden. Das Ausstellverfahren bleibt auch im Erneuerungsfall 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 A

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

- Qualifizierte Zertifikate für natürliche Personen:

  Für den Bezug von qualifizierten Zertifikaten der Klasse A 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
  - Ausgefülltes und (elektronisch, min. mit Klasse B) signiertes Antragsformular für qualifizierte Zertifikate Klasse A der SG-PKI
  - Persönlicher Eintrag im Admin-Directory des Bundes, mit Nachname(n), Vorname(n) (gemäss Reisedokument), E-Mailadresse
  - Unterschriebene «Benutzervereinbarung und Nutzungsbedingungen für Zertifikate der Klasse A – Geregelte und qualifizierte Zertifikate gemäss ZertES (für juristische und natürliche Personen)» (vorliegendes Dokument)

  Um die zukünftige Inhaberin zweifelsfrei zu identifizieren, wird das Reisedokument bei der Identifizierung auf Gültigkeit, Richtigkeit, Echtheit und Übereinstimmung des Bildes mit der anwesenden Person überprüft. Ebenso wird der Antrag vor der Ausstellung eines persönlichen qualifizierten Zertifikats plausibilisiert (Person arbeitet tatsächlich in der im Admin-Directory Eintrag zugewiesenen Organisationseinheit und benötigt das Zertifikat im geschäftlichen Alltag; die zukünftige Inhaberin ist berechtigt ein Zertifikat zu beantragen).

- Geregelte Zertifikate für juristische Personen:

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

  - Die zukünftige Inhaberin ist eine UID-Einheit im Sinne von Artikel 3 Absatz 1 Buchstabe c des Bundesgesetzes vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer (UIDG).
  - Die Antragstellerin muss für die jeweilige UID-Einheit vertretungsberechtigt sein. Diese Berechtigung muss sie entweder durch einen beglaubigten Handelsregisterauszug oder durch eine rechtswirksam unterzeichnete Vertretungsermächtigung nachweisen können.
  - Ausgefülltes und durch die Antragstellerin signiertes Antragsformular für geregelte Zertifikate Klasse A der SG-PKI. Die Antragstellerin kann den Antrag mit ihrem persönlichen qualifizierten Signaturzertifikat Klasse A elektronisch unterschreiben.
  - Durch die Antragstellerin unterschriebene «Benutzervereinbarung und Nutzungsbedingungen für Zertifikate der Klasse A – Geregelte und qualifizierte Zertifikate gemäss ZertES (für juristische und natürliche Personen)» (vorliegendes Dokument)
  - Ein für die Einreise in die Schweiz gültiges Reisedokument (ID/ Pass), ausgestellt auf die Antragstellerin

  Die Antragstellerin muss für die Ausstellung des Zertifikats persönlich erscheinen. Um die antragstellende Person zu verifizieren und identifizieren, wird das Reisedokument durch den oder die LRAO der Klasse A der SG-PKI bei der Ausstellung auf Gültigkeit, Richtigkeit und Echtheit überprüft. Die LRAO sind zudem angewiesen, das Bild des Dokuments mit der vor Ihnen stehenden Person zu vergleichen. Ebenso wird der Antrag vor der Ausstellung eines geregelten Zertifikats plausibilisiert (Person arbeitet tatsächlich in der angegebenen Organisationseinheit, ist bevollmächtigt das geregelte Zertifikat Klasse A für juristische Personen zu erhalten sowie zu nutzen und benötigt das Zertifikat im geschäftlichen Alltag).

  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 das Zertifikat 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 Zertifikate der Klasse A – Geregelte und qualifizierte Zertifikate gemäss ZertES (für juristische und natürliche Personen)» gelesen und verstanden hat und die darin aufgeführten Bestimmungen akzeptiert.

Name, Vorname (Antragstellerin):		
Inhaberin (nur für juristische Personen)		
Ort/ Datum:		**Elektronische Signatur Antragstellerin:**
		Die Antragstellerin (für die Inhaberin)