



Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI

Zur Ausstellung von persönlichen Zertifikaten der Klassen A (nach ZertES qualifizierte) und B (fortgeschrittene) Zertifikate der Swiss Government PKI, der Bundesbehörde der Schweizerischen Eidgenossenschaft

V1.1, 19.02.2019

Die Swiss Government PKI des BIT, in ihrer Rolle als Trust Service Provider (TSP), betreibt im Auftrag des ISB (Informatiksteuerungsorgan des Bundes) die PKI (Public-Key-Infrastruktur) der Bundesbehörden der Schweizerischen Eidgenossenschaft. Im Rahmen des Marktmodells «SD005 - Marktmodell Standarddienst: Identitäts- und Zugangsverwaltung (IAM)» werden die Zertifikate der Klasse A und B definiert. Die LRA-Officer (Local Registration Agency Officer) sind für die Ausstellung von Zertifikaten der Klasse A und B zuständig. Bezug und Nutzung der LRAO-Zertifikate der Klassen A und B unterliegen den Bestimmungen der «Benutzervereinbarung und Nutzungsbedingungen Klasse A/B». Diese werden durch die Swiss Government PKI (SG-PKI) jährlich den jeweils geltenden gesetzlichen Vorschriften und den normativen Anforderungen an Public Key Infrastrukturen angepasst. Letztere bilden die Basis dieser Benutzervereinbarung und Nutzungsbedingungen. Die jeweils gültige Version ist auf www.pki.admin.ch publiziert. Alle Inhaber von Zertifikaten werden über die Publikation einer aktualisierten Version der Dokumente per E-Mail informiert.

Zu beachten sind des Weiteren die «Guidelines zu den LRAO-Zertifikaten der SG-PKI». Diese müssen beim Bezug eines LRAO-Zertifikats ebenfalls akzeptiert werden.

Vollständigkeit und Genauigkeit der Informationen

Der Inhaber eines LRAO-Zertifikates der Swiss Government PKI (in Folge «Inhaber oder LRAO» genannt¹) verpflichtet sich dazu, dem TSP die für den Ausstellungsprozess sowie auch für den Inhalt des Zertifikats benötigten Informationen jederzeit korrekt und vollständig zu liefern. Vor der Ausstellung des Zertifikats muss der LRAO bei persönlicher Anwesenheit anhand eines gültigen Reisedokuments identifiziert werden. Das Zertifikat ist untrennbar an diesen LRAO gebunden. Vorname(n)/ Nachname(n), Suffix und e-Mailadresse des LRAO werden immer im Zertifikat aufgeführt.

Der Inhaber verpflichtet sich ebenfalls, die Daten seiner Kunden (=Bezüger von Zertifikaten der Klassen A und/ oder B) gemäss den «Registrierrichtlinien für die Klasse A bzw. B» zu prüfen.

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

Schutz des privaten Schlüssels

Der LRAO verpflichtet sich dazu, alle angemessenen Vorkehrungen zu treffen, um die alleinige Kontrolle, die Vertraulichkeit und den Schutz vor Verlust und Missbrauch des privaten Schlüssels und der allfällig damit verbundenen Aktivierungsdaten (z.B. PIN) und Medien (z.B. Smartcard), zu gewährleisten. Der private Schlüssel des Zertifikats kann und darf nur im Zusammenhang mit dem Zertifikat und nur für die im Zertifikat festgelegten Zwecke (Ausstellung/Revokation/Management von Klasse A und B Zertifikate) eingesetzt werden. Sie dürfen auf keinen Fall unberechtigten Dritten zugänglich gemacht werden. Der Inhaber haftet für jeden Schaden,

¹ Die männliche Form «Inhaber» wird in diesem Dokument der besseren Lesbarkeit dienend gleichermassen für das weibliche und das männliche Geschlecht benutzt.

der durch die Weitergabe des privaten Schlüssels und der allfällig damit verbundenen Aktivierungsdaten und Medien an Dritte entstanden ist.

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

Nutzung des Zertifikats

Der LRAO stellt sicher, dass ihm Inhalt, Zweck und Wirkung des Einsatzes des LRAO-Zertifikates bekannt sind. Er verpflichtet sich, den auf der LRAO-Smartcard vorhandenen Zertifikat und den privaten Schlüssel nur für autorisierte Geschäfte und unter Einhaltung aller geltenden gesetzlichen Vorschriften sowie den Bestimmungen dieses Dokuments einzusetzen.

Berichterstattung und Revokation

Der LRAO verpflichtet sich dazu, das Zertifikat und den dazugehörigen privaten Schlüssel unverzüglich nicht mehr einzusetzen und beim TSP die Revokation zu verlangen, wenn:

- der konkrete Verdacht besteht, dass mit dem Zertifikat verdächtige Aktivitäten (Missbrauch der Aktivierungsdaten) unternommen wurden;
- die Informationen im Zertifikat nicht mehr korrekt oder ungenau sind oder es in naher Zukunft sein werden;

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

Wenn aus Sicherheitsgründen erforderlich und aus datenschutzrechtlicher Sicht erlaubt, kann der TSP Daten über den LRAO, das Zertifikat und weitere in unmittelbarem Zusammenhang stehende Informationen an andere zuständige Stellen, TSPs, Firmen und industrielle Gruppen weiterleiten, wenn das Zertifikat oder die Person, die das Zertifikat einsetzt, als Quellen einer missbräuchlichen Verwendung identifiziert werden.

Alle Informationen betreffend die Revokation werden durch den TSP aus Gründen der Nachvollziehbarkeit archiviert.

Beendigung des Einsatzes des Zertifikats

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

Verantwortung / Haftung

Der LRAO ist dafür verantwortlich, dass das LRAO-Zertifikat und der zugehörige private Schlüssel nur unter Einhaltung der Bestimmungen in Abschnitt «Nutzung des LRAO-Zertifikates» dieses Dokuments eingesetzt werden. Ein Verstoss gegen diese Vorgabe hat eine Revokation und weitere administrative und gegebenenfalls juristische Massnahmen zur Folge. Der LRAO trägt die Verantwortung für alle durch ihn mit dem Zertifikat auf der LRAO-Smartcard vorgenommenen Tätigkeiten sowie für allfällig daraus resultierende Schäden und deren Folgen. Dem LRA-Officer ist bekannt, dass er nicht angewiesen werden kann qualifizierte Zertifikate auszustellen, insofern die Identifizierung des Antragstellers nicht korrekt vorgenommen werden kann.

Anerkennungs- und Einverständniserklärung

Der LRAO 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.

Der LRAO bezeugt mit seiner Unterschrift im jeweiligen Anmeldeformular «Klasse A/B: Antrag LRA-Officer», dass er das vorliegende Dokument «Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI» gelesen und verstanden hat und die darin aufgeführten Bestimmungen akzeptiert.