NICHT KLASSIFIZIERT

Guidelines zum LRAO-Zertifikat der Swiss Government PKI

Erläuterungen zum Bezug und Einsatz vom LRAO-Zertifikat der Klassen A und B der Swiss Government PKI

V1.1, 19.02.2019

1 Zweck des LRAO-Zertifikats

Zweck

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 der Klasse A und B zuständig. Das LRAO-Zertifikat kann für folgende Zwecke verwendet werden:

- Ausstellung, Revokation und Pflege von Klasse A und/oder B Zertifikate der Swiss Government PKI.

Durch erweiterte Prüf- und Sicherheitsmechanismen während des Ausstellungsprozesses der Klassen A und B Zertifikate wird die Identität des Zertifikatsinhabers auf einer hohen Sicherheitsstufe festgestellt. Die Ausgabe von Klasse A und B Zertifikaten erfolgt immer persönlich und nur nach Identifizierung des Inhabers mittels eines gültigen, für die Einreise in die Schweiz zugelassenen Reisedokumentes.

Ausgeschlossener Zweck

Das LRAO-Zertifikat erfüllt ausschliesslich die oben genannten Zwecke und gibt keinerlei weitere Aufschlüsse, Versicherungen oder Garantien. Insbesondere garantiert das LRAO-Zertifikat nicht, dass der Inhaber im Umgang mit dem Zertifikat korrekt und legal handelt.

2 Qualität des LRAO-Zertifikats

Die SG-PKI hält sich an die in den Registrierrichtlinien vorgegebenen Prozesse, welche die notwendigen und zumutbaren Schritte zur Bestätigung folgender Tatsachen zum Zeitpunkt der Erstausstellung eines LRAO-Zertifikates festlegen:

- **Rechtlich gültige Existenz:** Der im LRAO-Zertifikat genannte Inhaber existiert als natürliche Person und verfügt über einen persönlichen Eintrag im AdminDirectory.
- **Identität:** Der Name des im LRAO-Zertifikats genannten Inhabers stimmt mit dem Namen im AdminDirectory und im aktuell gültigen Reisedokument überein.
- **Autorisierung:** Der im LRAO-Zertifikat genannte Inhaber ist zum Bezug des Zertifikates durch die unterschriftsberechtigte Person seines Amtes autorisiert worden.
- **Richtigkeit der Daten:** Alle im Zertifikat enthaltenen Daten und Informationen sind korrekt.
- **Vereinbarung/ Nutzungsbedingungen:** Der im LRAO-Zertifikat genannte Inhaber hat die in der «Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI» beschriebenen Rechte und Pflichten gelesen, verstanden und mit der Unterschrift auf dem Antragsformular für das LRA-Officer Zertifikat der SG-PKI akzeptiert. Seine Fragen diesbezüglich wurden von der SG-PKI verständlich beantwortet.
- **Status:** Die SG-PKI stellt den Status des Zertifikats sowie Informationen über dessen Gültigkeit/ Revokation online abrufbar zur Verfügung.

- **Revokation:** Die SG-PKI kann das LRAO-Zertifikat gegebenenfalls aus den in der/n «Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI» genannten Gründen unverzüglich revozieren.

3 Policies

Alle geltenden gesetzlichen Vorgaben, Policies (inkl. der CP/CPS der SG Root CA I für Klasse B und der SG Root CA IV für Klasse A – im Nachfolgenden «CP/CPS») und Registrierrichtlinien von Zertifikaten der SG-PKI, sowie die «Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI» und diese Guidelines sind im Internet auf der Website der SG-PKI publiziert: www.pki.admin.ch.

Der angehende LRAO verpflichtet sich mit der Unterschrift auf dem Formular: «Klasse A: Antrag LRA-Officer», sich an die geltenden Richtlinien und Gesetzgebungen zu halten und seine Arbeiten danach auszuführen. Insbesondere sind dies:

- Die CP/CPS der SG Root CA I: («Certificate Policy and Certification Practice Statement of the Swiss Government Root CA I») (insbesondere zu erwähnen sind die in Kap. 5.3.1 und 5.5.2 beschriebenen Verpflichtungen)
- Und/oder: Die CP/CPS der SG Root CA IV: («Certificate Policy and Certification Practice Statement of the Swiss Government Root CA IV») (insbesondere zu erwähnen sind die in Kap. 5.3.1 und 5.5.2 beschriebenen Verpflichtungen)
- Die «Swiss Government PKI Registrierrichtlinien Klasse A - Qualifiziert»
- Die «Swiss Government PKI Registrierrichtlinien Klasse B»
- Die «Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI»
- Die «Guidelines zum LRAO-Zertifikat der Swiss Government PKI» (Dieses Dokument).

Inhalt

Das LRAO-Zertifikat der SG-PKI enthält Informationen betreffend:

- Herausgeber und ausstellender CA
- die Root CA der ausstellenden CA
- die angewandte Policy
- Ausstell- und Ablaufdatum des Zertifikates
- Seriennummer des Zertifikates
- Verwendungszweck des Zertifikates
- der CRL und dem OCSP
- die Auditoren der CA
- den Inhaber des Zertifikates gemäss Eintrag im AdminDirectory zum Zeitpunkt der Erstausstellung:
    1) Common Name des Inhabers
    2) E-Mail-Adresse
    3) UPN

Gültigkeit

Das LRAO-Zertifikat der SG-PKI ist max. 3 Jahre gültig. Nach Ablauf der Gültigkeit muss das LRAO-Zertifikat durch den LRAO-Officer neu bei der SG-PKI, analog dem Erstausstellungsprozess, beantragt und von der SG-PKI ausgestellt werden.

4 Bezug des LRAO-Zertifikats

Bezug

Für den Bezug des LRAO-Zertifikats der SG-PKI sind folgende Dokumente bzw. Registrierungen nötig:

- Ein gültiges, für die Einreise in die Schweiz zugelassenes Reisedokument (ID/ Pass), ausgestellt auf den Antragsteller. Die Identität wird während der obligatorischen LRAO-Schulung vom Kursleiter überprüft
- Ein persönlicher Eintrag im AdminDirectory, mit Nachname(n), Vorname(n) (gemäss Reisedokument), gültiger E-Mailadresse und optional einem UPN Eintrag (User Principal Name)
- Ein Attest, welches den erfolgreichen Besuch der obligatorischen LRA-Officer Schulung und die bestandene Prüfung bezeugt
- Ein ausgefülltes und (elektronisch) signiertes Antragsformular für LRA-Officer Zertifikate der Swiss Government PKI, in welchem

1) der angehende LRAO
   - eine Vertraulichkeitserklärung
   - die Benutzervereinbarung und Nutzungsbedingungen für LRA-Officer der SG-PKI
   - diese Guidelines

mit seiner Unterschrift als akzeptiert erklärt und die LRAO-Smartcard bestellt.

2) die Unterschriftsberechtigte Person der anstellenden Behörde die Vertrauenswürdigkeit des angehenden LRA-Officer, gemäss den Vorgaben im Antragsformular unter dem Kapitel «Vertrauenswürdigkeitsprüfung», mit seiner Unterschrift bestätigt.

Identifizierung

Um die antragstellende Person zu identifizieren, wird das Reisedokument auf Gültigkeit, Richtigkeit und Echtheit während der LRAO-Schulung überprüft. Die SG-PKI Kursleiter sind zudem verpflichtet, das Bild des Dokumentes mit der vor Ihnen stehenden und am Kurs teilnehmende Person zu validieren. Ebenso wird der Antrag vor der Ausstellung eines persönlichen Zertifikates von der SG-PKI plausibilisiert (Person arbeitet tatsächlich in der im AdminDirectory Eintrag zugewiesenen Organisationseinheit und benötigt das Zertifikat im geschäftlichen Alltag; der Antragsteller ist berechtigt ein Zertifikat zu beantragen).

Verbindlichkeit

Der Antrag muss durch die zuständigen Stellen freigegeben sein. Diese Guidelines und das Dokument « Benutzervereinbarung und Nutzungsbedingungen für LRAO der SG-PKI» müssen vom Antragsteller verstanden und im Antragsformular für LRAO mit der (digitalen) Unterschrift akzeptiert worden sein.

5 Schutz des privaten Schlüssels und des Zertifikates

Übertragbarkeit

Das LRAO-Zertifikat ist immer persönlich und nicht übertragbar. Die persönlichen Angaben über den Inhaber werden sowohl im Zertifikat wie auch bei der SG-PKI gespeichert.

PIN/PUK

Die PIN muss unabhängig von anderen Passwörtern gewählt werden und darf für Dritte nicht zugänglich sein. Sie muss nicht regelmässig geändert werden, ausser es besteht der konkrete Verdacht, dass ein Dritter Kenntnis davon erlangt hat.

Das Zertifikat (und somit der Zertifikatsträger: Smartcard, USB-Stick, etc.) muss mit einer mind. 6-stelligen PIN gesichert werden, wobei rein numerische PINs, sowie auch gemischte PINs erlaubt sind. Um den Missbrauch der eigenen elektronischen Identität zu vermeiden, darf die PIN niemals Dritten bekanntgegeben werden.

Meldepflicht

Ein allfälliger Verlust der Smartcard muss vom LRAO umgehend der SG-PKI gemeldet werden. In der Folge wird das betroffene Zertifikat gesperrt (revoziert) und die Sperrung auf einer öffentlichen elektronischen Sperrliste publiziert. Selbst wenn die Smartcard wiedergefunden werden sollte, bleibt das Zertifikat gesperrt und somit ungültig. Unmittelbar nach erfolgter Sperrung kann bei der SG-PKI die Ausstellung eines neuen LRAO-Zertifikates beantragt werden. Der Prozess der Ausstellung eines neuen LRAO-Zertifikats entspricht der Erstausstellung.

Organisationswechsel, Namenswechsel (z.B. nach Heirat) oder Änderung der E-Mail-Adresse bedingen die Ausstellung eines neuen Zertifikates (Erstausstellung).

6 Revokation

Revokationen müssen bei der SG-PKI beantragt werden. Dazu steht den befugten Personen (siehe abschliessende Liste unten) ein Formular auf der Homepage der SG-PKI www.pki.admin.ch zur Verfügung. Wird die Revokation per Telefon beantragt, wird die SG-PKI den Antragsteller mit Hilfe der Revokationspassphrase und den persönlichen Daten (Geburtstag, Geburtsort, etc.) identifizieren. Lediglich der Antragsteller selbst ist befugt, eine Revokation per Telefon zu beantragen. Weitere Personen, die eine Revokation beantragen dürfen, müssen die Anfrage schriftlich einreichen.

Befugte Personen sind:

- der Zertifikatsinhaber selbst
- der SG-PKI Verantwortliche
- SG-PKI Security Officer
- die für den Zertifikatsinhaber zuständigen:
  - Mitarbeiter des HR (Personaldienst),
  - Linienvorgesetzte
  - LRA Officer
  - ISBO
  - ISBD
  - PKI Verantwortliche der Organisation

7 Inhalt des Zertifikates

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

8 Akzept/ Bestätigung für Erhalt der Smartcard

Mit der Unterschrift auf dem Empfangsformular für LRAO-Zertifikate bestätigt der Zertifikatsinhaber nach Erhalt der LRAO-Smartcard:

- Die Korrektheit der im Zertifikat gespeicherten Daten.
- Den Erhalt der LRAO-Smartcard.
- Diese Guidelines und die Rechte und Pflichten, die aus diesen Guidelines erwachsen, verstanden und akzeptiert zu haben. Allfällige Fragen wurden von der SG-PKI verständlich beantwortet.
- Die Revokationspassphrase sowie die restlichen zur telefonischen Identifikation der Person und des Zertifikates benötigten Felder korrekt ausgefüllt zu haben.

Ausserdem verpflichtet sich der angehende LRAO, die hier beschriebenen Richtlinien, die in der «CP/CPS» beschriebenen, sowie auch die in den «Swiss Government PKI Registrierrichtlinien Klasse A oder B» Anforderungen und Aufgaben zu erfüllen und umzusetzen.
Zusätzliche Fragen können an die Swiss Government PKI unter der Mailadresse pki-info@bit.admin.ch gestellt werden.