Guidelines zu Klasse B Zertifikaten der Swiss Government PKI

Erläuterungen zum Bezug und Einsatz von Klasse B Zertifikate der Swiss Government PKI

V1.0, 09.03.2017

1 Zweck von Klasse B Zertifikaten

Zweck

Die Zertifikate der Klasse B sind im Rahmen des Marktmodells «SD005 - Marktmodell Standarddienst: Identitäts- und Zugangsverwaltung (IAM)» definiert. Klasse B Zertifikate können für folgende Zwecke verwendet werden:

- Vertrauenswürdige Signierung von Daten. Dadurch wird 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 des Inhabers zur Verfügung.

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

Ausgeschlossener Zweck

Klasse B Zertifikate erfüllen ausschliesslich die oben genannten Zwecke und geben keinerlei weitere Aufschlüsse, Versicherungen oder Garantien. Insbesondere garantieren Klasse B Zertifikate nicht, dass der Inhaber im Umgang mit dem Zertifikat korrekt und legal handelt.
Des Weiteren garantieren Klasse B Zertifikate nicht, dass:

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

2 Qualität der Klasse B Zertifikate

Der LRA-Officer der 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 Klasse B Zertifikates festlegen:

- **Rechtlich gültige Existenz:** Der im Klasse B Zertifikat genannte Inhaber existiert als natürliche Person und verfügt über einen persönlichen Eintrag im AdminDir.
- **Identität:** Der Name des im Klasse B Zertifikats genannten Inhabers stimmt mit dem Namen in seinem gültigen Reisedokument überein.
- **Autorisierung:** Der im Klasse B Zertifikat genannte Inhaber ist zum Bezug des Zertifikates autorisiert.
- **Richtigkeit der Daten:** Alle im Zertifikat enthaltenen Daten und Informationen sind korrekt.
- **Vereinbarung/ Nutzungsbedingungen:** Der im Klasse B Zertifikat genannte Inhaber wurde vom LRAO (Local Registration Authority Officer) über die in der «Benutzervereinbarung und Nutzungsbedingungen

Klasse B» beschriebenen Rechte und Pflichten informiert. Seine Fragen diesbezüglich wurden vom LRAO verständlich beantwortet. Der Inhaber hat die «Benutzervereinbarung und Nutzungsbedingungen Klasse B» gelesen, akzeptiert und unterzeichnet.

- **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 Klasse B Zertifikat gegebenenfalls aus den in der/n «Benutzervereinbarung und Nutzungsbedingungen Klasse B» genannten Gründen unverzüglich revozieren.

3 Policies

Alle geltenden gesetzlichen Vorgaben, Policies (inkl. der CP/CPS) und Richtlinien von Klasse B Zertifikaten sind im Internet auf der Website der SG-PKI publiziert: www.pki.admin.ch.

4 Inhalt und Gültigkeit des Klasse B Zertifikates

Inhalt

Das Klasse B Zertifikat der SG-PKI enthält Informationen betreffend:

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

Gültigkeit

Das Klasse B Zertifikat der SG-PKI ist max. 3 Jahre gültig. Das Zertifikat kann vor Ablauf der 3-Jahres-Frist maximal zwei Mal vom Inhaber selbst für weitere drei Jahre erneuert werden. Für die Erneuerung des Zertifikates steht dem Inhaber der Rekeying Wizard zur Verfügung. Nach Ablauf der 3. Gültigkeitsperiode muss durch den LRA-Officer ein neues Zertifikat wie im Prozess der Erstausstellung ausgestellt werden.

5 Bezug von Klasse B Zertifikaten

Bezug

Für den Bezug von Klasse B Zertifikaten 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.
- Ein ausgefülltes und (elektronisch) signiertes Antragsformular für Klasse B Zertifikate der Swiss Government PKI, oder eine Anmeldung über die Linie des Amtes, bzw. über den internen festgelegten HR-Prozess.
- Die unterschriebene «Benutzervereinbarung und Nutzungsbedingungen Klasse B» (wird bei jeder Ausstellung von Klasse B Zertifikaten am Schluss vom LRA-Officer zusammen mit diesem Dokument ausgedruckt).
- Ein persönlicher Eintrag im AdminDir, mit Nachname(n), Vorname(n) (gemäss Reisedokument), gültiger E-Mailadresse und optional einem UPN Eintrag (User Principal Name)

Identifizierung

Die persönliche Identifizierung des Antragstellers wird durch die LRAOs 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 einem Delegierten des LRAOs, dem RIO (Registration Identification Officer) übernommen, der die Bestätigung der durchgeführten Identifizierung dem LRAO zur Freigabe des Antrages weiterleitet.

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

Verbindlichkeit

Der Antrag, oder der interne Prozess zur Beantragung muss durch die zuständigen Stellen freigegeben sein. Diese Guidelines und das Dokument «Benutzervereinbarung und Nutzungsbedingungen Klasse B» müssen vom Antragsteller akzeptiert und (digital) unterschrieben werden.

6 Schutz des privaten Schlüssels und des Zertifikates

Übertragbarkeit

Das Klasse B 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 gemischte PINs erlaubt sind. Um den Missbrauch der eigenen elektronischen Identität zu vermeiden, darf die PIN niemals Dritten bekanntgegeben werden.

Der PUK der Smartcard muss mindestens 8-stellig nach den oben genannten Regeln gewählt werden.

Meldepflicht

Ein allfälliger Verlust der SmartCard muss vom Inhaber umgehend dem zuständigen LRAO oder der IT-Serviceorganisation gemeldet werden. In der Folge werden die betroffenen Zertifikate gesperrt (revoziert) und die Sperrung auf einer öffentlichen elektronischen Sperrliste publiziert. Selbst wenn die SmartCard wieder gefunden werden sollte, bleiben die Zertifikate gesperrt und sind somit ungültig. Unmittelbar nach erfolgter Sperrung kann beim zuständigen LRAO die Ausstellung eines neuen Klasse B Zertifikates beantragt werden. Der Prozess der Ausstellung eines neuen Klasse B Zertifikats entspricht der Erstausstellung.

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

7 Revokation

Revokationen müssen beim LRAO 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 der LRAO 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

8 Inhalt des Zertifikates

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

Verschlüsselungszertifikat (Encryption Key)
Fingerprint (SHA-1):
Certificate Validity:
Serial #:

Unterschriftszertifikat (Signing Key)
Fingerprint (SHA-1):
Certificate Validity:
Serial #:

9 Akzept/ Bestätigung für Erhalt der SmartCard

Mit der Unterschrift bestätigt der Zertifikatsinhaber:

- Die Korrektheit der im Zertifikat gespeicherten Daten.
- Den Erhalt der SmartCard.
- Diese Guidelines gelesen und mit dem LRAO besprochen zu haben. Allfällige Fragen wurden vom LRAO verständlich beantwortet.
- Die Rechte und Pflichten, die aus diesen Guidelines erwachsen verstanden und akzeptiert zu haben.
- Die hier beschriebenen Richtlinien umzusetzen.

Zusätzliche Fragen können an die Swiss Government PKI unter der Mailadresse pki-info@bit.admin.ch gestellt werden[1].

Common Name (CN):

Ausstelldatum: **Unterschrift:** _____

[1] Bitte lesen Sie auch die Benutzer*vereinbarung und Nutzungsbedingungen für Klasse B Zertifikate der Swiss Government PKI*. Bei Ihrer Klasse B Bestellung wird eine signierte Kopie dieses Dokuments verlangt. www.pki.admin.ch .