Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

Vereinbarungs- und Nutzungsbedingungen

für den Bezug von Ausstellungsberechtigungen für Klasse C Standard Zertifikate der Swiss Government PKI der Bundesbehörden der Schweizerischen Eidgenossenschaft

Die Swiss Government PKI, in ihrer Rolle als Certification Service Provider (CSP), betreibt im Auftrag des ISB (Informatikstrategieorgan Bund) die PKI (Public-Key-Infrastruktur) der Bundesbehörden der Schweizerischen Eidgenossenschaft. Als Teil der Standarddienstleistungen werden dabei auch *Klasse C Standard Zertifikate* ausgestellt, sowie die *Berechtigungen zum Ausstellen* von solchen Zertifikaten vergeben. Ausstellung, Bezug und Nutzung der Klasse C Standard Zertifikate der Swiss Government PKI unterliegen den nachfolgend aufgeführten Vereinbarungs- und Nutzungsbedingungen. Diese werden durch die Swiss Government PKI (SG-PKI) jährlich den geltenden gesetzlichen Vorschriften und den Bestimmungen der «CA/Browser Forum Guidelines[1]» angepasst. Letztere bilden einen integrierenden Bestandteil dieser Vereinbarungs- und Nutzungsbedingungen. Die jeweils gültigen Versionen, sowohl der vorliegenden Vereinbarungs- und Nutzungsbedingungen als auch der CA/Browser Forum Guidelines, sind auf https://www.bit.admin.ch/adminpki/00240/00241/06111/index.html?lang=de publiziert.

Zu beachten sind des Weiteren die «Guidelines der Swiss Government PKI zum Bezug von Klasse C Standard Zertifikaten». Diese müssen bei der Bestellung der Ausstellungsberechtigungen und bei jeder Mutation der Berechtigungen separat akzeptiert werden.

Vollständigkeit und Richtigkeit der Informationen

Der durch den CSP berechtigte Aussteller von Klasse C Standard Zertifikaten (in Folge «Aussteller» genannt[2]) verpflichtet sich dazu, dem CSP beim Bezug seiner Ausstellungsberechtigung sowie bei jeder durch ihn vorgenommenen Ausstellung von Zertifikaten die richtigen und vollständigen Informationen zu liefern und Änderungen zu melden. Insbesondere hat er darauf zu achten, dass alle Informationen/Daten sowie im speziellen die E-Mail-Adressen der durch ihn bedienten Zertifikats-Inhaber im dafür vorgesehenen Tool (aktuell der Certificate Request Wizard (CRW)) korrekt eingetragen werden. Ausserdem ist der Aussteller verpflichtet, den CSP zu informieren, wenn sich seine Rolle oder sein Zuständigkeitsbereich wesentlich ändert.

Schutz des CRW-Zugangs, der Zertifikate und der privaten Schlüssel

Klasse C Standard Zertifikate können für Personen, Organisationen, Systeme oder Mailboxen ausgestellt werden. Die Angaben über den Aussteller und über die durch ihn bedienten Zertifikats-Inhaber werden bei der Swiss Government PKI gespeichert. Der Aussteller verpflichtet sich, alle angemessenen Vorkehrungen zu treffen, um die Zugangskontrolle, die Vertraulichkeit und den Schutz vor Missbrauch der Ausstellungssoftware (CRW) jederzeit sicherzustellen. Ebenso hat er die Zugangskontrolle, die Vertraulichkeit und den Schutz vor Verlust und Missbrauch der privaten Schlüssel und der allfällig damit verbundenen Aktivierungsdaten zu gewährleisten. Der CRW kann und darf nur für die dafür vorgesehenen Zwecke im Zusammenhang mit der Beantragung von Zertifikaten sowie der Weiterbearbeitung der durch den Aussteller erstellten Zertifikate und der dazugehörigen privaten Schlüssel eingesetzt werden. Der CRW, die privaten Schlüssel und die Zertifikate dürfen auf keinen Fall unberechtigten Dritten zugänglich gemacht werden. Der Aussteller haftet für jeden Schaden, der durch die Weitergabe der Zugangsberechtigungen zum CRW oder durch die Weitergabe der privaten Schlüssel mit den allfällig damit verbundenen Aktivierungsdaten und Medien an unberechtigte Dritte entstanden ist.

Der CSP behält sich vor, dem Aussteller bereits bei einem konkreten Verdacht auf Missbrauch, unautorisierten Zugang oder Weitergabe der vorangehend beschriebenen Zugangsdaten und Schlüssel an unberechtigte Dritte, die Berechtigungen für die Ausstellung von Klasse C Standard Zertifikaten ohne Vorinformation zu entziehen.

Nutzung des CRWs und der Zertifikate

Der Aussteller verpflichtet sich sicherzustellen, dass der CRW und die Zertifikate mit den dazugehörigen privaten Schlüsseln ausschliesslich für autorisierte und legale Zwecke eingesetzt werden. Es ist insbesondere untersagt, willentlich Zertifikate mit falschen oder ungenauen Informationen auszustellen. Der Aussteller stellt zudem sicher, dass ihm Inhalt, Zweck und Wirkung der von ihm ausgestellten Zertifikate bekannt sind. CRW und Klasse C Standard Zertifikate mit deren privaten Schlüsseln dürfen nur für autorisierte (Unternehmens-)Geschäfte und unter Einhaltung aller geltenden gesetzlichen Vorschriften sowie der Vorgaben aus diesen Vereinbarungs- und Nutzungsbedingungen und den «CA/Browser Forum Guidelines» eingesetzt werden.

---

[1] *CA/Browser Forum – Guidelines (http://cabforum.org/documents.html)*

[2] Die männliche Form «Inhaber/ Aussteller» wird in diesem Dokument der besseren Leserlichkeit dienend gleichermassen für das weibliche und das männliche Geschlecht benutzt.

Berichterstattung und Revokation

Der Aussteller verpflichtet sich, unverzüglich beim CSP die Revokation des Zertifikates zu verlangen, wenn:

- der konkrete Verdacht besteht, dass das Zertifikat absichtlich missbraucht oder falsch eingesetzt wird;
- die Informationen im Zertifikat nicht mehr korrekt oder ungenau sind, oder es in naher Zukunft sein werden;
- ein konkreter Verdacht auf Missbrauch oder Kompromittierung der Aktivierungsdaten oder des privaten Schlüssels in Verbindung mit dem im Zertifikat eingebundenen öffentlichen Schlüssel besteht;
- der konkrete Verdacht besteht, dass das Zertifikat zur Kompromittierung des CSPs eingesetzt wird oder dessen Einsatz dazu führen könnte.

Den Anweisungen des CSPs ist bei Verdacht auf Kompromittierung oder Missbrauch eines Zertifikates unmittelbar Folge zu leisten. Wenn aus Sicherheitsgründen erforderlich und aus datenschutzrechtlicher Sicht erlaubt, kann der CSP Daten über den Aussteller, den Zertifikats-Inhaber, das Zertifikat und weitere in unmittelbarem Zusammenhang stehende Informationen an andere zuständige Stellen, CSPs, Firmen und industrielle Gruppen, inklusive dem CA/Browser Forum, weiterleiten, wenn:

- der Aussteller den CRW missbraucht, fahrlässig einsetzt oder sich nicht an die vorliegenden Vereinbarungs- und Nutzungsbedingungen hält
- das Zertifikat oder die Person, die das Zertifikat einsetzt, als Ursprung einer missbräuchlichen Verwendung identifiziert wird
- der Inhaber, welcher das Zertifikat beantragt, nicht identifiziert oder verifiziert werden kann, oder
- das Zertifikat aus weiterführenden Gründen als vom Aussteller oder Inhaber angegeben (wie z.B.: Kompromittierung, etc.) revoziert wurde.

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

Beendigung des Einsatzes eines Zertifikates

Der Aussteller verpflichtet sich, nach Ablauf der Gültigkeit oder der Revokation eines Zertifikates (insbesondere aufgrund einer Kompromittierung) mit dem Zertifikats-Inhaber in Kontakt zu treten und alle notwendigen und zumutbaren Schritte zu unternehmen, um den Einsatz des Zertifikates sofort zu unterbinden.

Beendigung des Amtes als Ausstellungsberechtigter

Der Aussteller verpflichtet sich, die allfällige Beendigung seiner Aufgabe/Rolle als Ausstellungsberechtigter (z.B. aufgrund von Änderungen in seinem Arbeitsverhältnis/seiner Funktion), der SG-PKI zu melden und die Sperrung der Zugangsberechtigungen zum CRW mittels Antragsformular anzufordern.

Verantwortung / Haftung

Der Aussteller ist dafür verantwortlich, dass die Klasse C Standard Zertifikate und deren private Schlüssel nur unter Einhaltung aller geltenden gesetzlichen Vorschriften, der Vorgaben aus diesen Vereinbarungs- und Nutzungsbedingungen, den «Guidelines der Swiss Government PKI zum Bezug von Klasse C Standard Zertifikaten» und den «CA/Browser Forum Guidelines» ausgestellt werden. Ein Verstoss gegen diese Vorgabe hat den Entzug der CRW-Zugangsberechtigung, eine Revokation der vom Aussteller ausgestellten Zertifikate und weitere administrative und juristische Massnahmen zur Folge. Der Aussteller trägt die Verantwortung für alle durch ihn ausgestellten Zertifikate sowie für allfällig daraus resultierende Schäden und deren Folgen, wenn nachgewiesen werden kann, dass er vorsätzlich oder grobfahrlässig gegen gesetzliche Vorschriften, Vorgaben aus diesen Vereinbarungs- und Nutzungsbedingungen oder Bestimmungen aus den vorgenannten Guidelines verstossen hat.

Änderungen der Vereinbarungs- und Nutzungsbedingungen

Nachträgliche Änderungen oder Ergänzungen dieser Vereinbarungs- und Nutzungsbedingungen gelten als vom berechtigten Aussteller akzeptiert, wenn er nicht innert 30 Tagen seit Kenntnisnahme der geänderten Bestimmungen widerspricht.

Anerkennungs- und Einverständniserklärung

Der Aussteller nimmt zu Kenntnis, dass der CSP die Ausstellungsberechtigungen bereits bei einem begründeten Verdacht eines Missbrauchs, einer Verletzung der vorliegenden Vereinbarungs- und Nutzungsbedingungen oder eines sonstigen Verstosses gegen geltende gesetzliche Bestimmungen (bspw. Betrug, Vertrieb von kompromittierenden Zertifikaten etc.) unverzüglich entzieht.

Der Aussteller bezeugt mit seiner Unterschrift, dass er diese Vereinbarungs- und Nutzungsbedingungen gelesen und verstanden hat und diese akzeptiert.

Ort / Datum: _____ Unterschrift: _____