Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

Antragsformular für Standard Klasse C- Zertifikate der Swiss Government PKI V1.5

◉ *Antrag für (zusätzliche) Berechtigungsvergabe* ○ *Antrag für Berechtigungsentzug*

Ich beantrage im Namen der unten genannten Organisation die Berechtigung zu Ausstellung von Standard Klasse C-Zertifikaten der Swiss Government PKI:

Antragsteller	
Name, Vorname, Suffix	
Telefonnummer (Direktwahl Antragsteller)	
E-Mail	
Klasse B Zertifikat vorhanden	○ Ja ○ Nein
Seriennummer des Klasse B Zertifikates (Authentisierung) oder Ablaufdatum	

Organisation	
Kanton / Amt / Firma	
Geschäftsadresse/ Nr.	
PLZ/ Ort	
Telefonnummer	

Es stehen für die Ausstellung von Klasse C Standard-Zertifikate verschiedene Templates zur Verfügung. Pro Zeile wird **EIN** Template freigegeben. Für die Freigabe jeder bestellten Policy (=Template) werden CHF 50.- Bearbeitungsgebühren verrechnet.

Template-Bestellung:

Ausprägung	Client Authentisierung	Sever Authentisierung	Signatur	Verschlüsselung	Common Name (CN) Subjekt	Bestellung
Zertifikat Person Auth	Ja	explizit nicht	Nein	Nein	Person (Name)	☐
Zertifikat Person Auth/Sign	Ja	explizit nicht	Ja	Nein	Person (Name)	☐
Zertifikat Person Auth/Sign/Verschl	Ja	explizit nicht	Ja	Ja	Person (Name)	☐
Zertifikat Person Sign/Verschl	Nein	explizit nicht	Ja	Ja	Person (Name)	☐
Zertifikat Person Sign	Nein	explizit nicht	Ja	Nein	Person (Name)	☐
Zertifikat Person Verschl	Nein	explizit nicht	Nein	Ja	Person (Name)	☐
Zertifikat Organisation Auth	Ja	explizit nicht	Nein	Nein	Organisation (Name)	☐
Zertifikat Organisation Auth/Sign	Ja	explizit nicht	Ja	Nein	Organisation (Name)	☐
Zertifikat Organisation Auth/Sign/Verschl	Ja	explizit nicht	Ja	Ja	Organisation (Name)	☐
Zertifikat Organisation Sign/Verschl	Nein	explizit nicht	Ja	Ja	Organisation (Name)	☐
Zertifikat Organisation Sign	Nein	explizit nicht	Ja	Nein	Organisation (Name)	☐
Zertifikat Organisation Verschl	Nein	explizit nicht	Nein	Ja	Organisation (Name)	☐
Zertifikat System Auth	Ja	explizit nicht	Nein	Nein	System (Name)	☐
Zertifikat System Auth/Sign	Ja	explizit nicht	Ja	Nein	System (Name)	☐
Zertifikat System Auth/Sign/Verschl	Ja	explizit nicht	Ja	Ja	System (Name)	☐
Zertifikat System Sign/Verschl	Nein	explizit nicht	Ja	Ja	System (Name)	☐
Zertifikat System Sign	Nein	explizit nicht	Ja	Nein	System (Name)	☐
Zertifikat System Verschl	Nein	explizit nicht	Nein	Ja	System (Name)	☐

Bestätigungen:

Mit dem Anklicken des Formularfeldes bestätigen Sie die Guidelines (folgende Seiten), sowie die Vereinbarung/ Nutzungsbedingungen der Swiss Government PKI zum Bezug von Kl. C Standard Zertifikaten gelesen und akzeptiert zu haben: ☐

Mit dem Anklicken des Formularfeldes bestätigen Sie, die Schulung Klasse C besucht zu haben: ☐

Antragsteller Name / Vorname: Funktion:	**Datum:**	**elektronische Signatur:**
		.....

Unterschriftsberechtigte(r) der Organisation Name / Vorname: Funktion:	**Datum:**	**elektronische Signatur oder Unterschrift:**
		.....
		.....

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

Guidelines der Swiss Government PKI zu den Klasse C Standard Zertifikaten

Erläuterungen zu Ausstellung, Bezug und Einsatz von Klasse C Standard Zertifikaten der Swiss Government PKI

V1.0, 18.01.2016

1 Zweck von Klasse C Standard Zertifikaten

Zweck

Klasse C Standard Zertifikate werden für die vertrauenswürdige Authentisierung an Systemen oder Applikationen eingesetzt und um Dokumente oder Verbindungen vertrauenswürdig zu signieren und/oder zu verschlüsseln. Klasse C Standard Zertifikate werden für Personen, Organisationen oder Systeme ausgestellt. Zusätzlich bieten Klasse C Standard Zertifikate die Möglichkeit, aus Gruppenmailbox-Accounts Nachrichten vertrauenswürdig zu signieren oder zu verschlüsseln.

Klasse C Standard Zertifikate für Systeme können für Server, Clients, Router, etc. eingesetzt werden. Organisationszertifikate werden auf juristische Personen/Organisationen ausgestellt, Personenzertifikate dieser Klasse werden ausschliesslich auf natürliche Personen ausgestellt.

Zertifikate der Klasse C Standard können in folgender Ausprägung ausgestellt werden:

Ausprägung	Client Authentisierung	Server Authentisierung	Signatur	Verschlüsselung	Common Name (CN) Subjekt
Zertifikat Person Auth	Ja	explizit nicht	Nein	Nein	Person (Name)
Zertifikat Person Auth/Sign	Ja	explizit nicht	Ja	Nein	Person (Name)
Zertifikat Person Auth/Sign/Verschl	Ja	explizit nicht	Ja	Ja	Person (Name)
Zertifikat Person Sign/Verschl	Nein	explizit nicht	Ja	Ja	Person (Name)
Zertifikat Person Sign	Nein	explizit nicht	Ja	Nein	Person (Name)
Zertifikat Person Verschl	Nein	explizit nicht	Nein	Ja	Person (Name)
Zertifikat Organisation Auth	Ja	explizit nicht	Nein	Nein	Organisation (Name)
Zertifikat Organisation Auth/Sign	Ja	explizit nicht	Ja	Nein	Organisation (Name)
Zertifikat Organisation Auth/Sign/Verschl	Ja	explizit nicht	Ja	Ja	Organisation (Name)
Zertifikat Organisation Sign/Verschl	Nein	explizit nicht	Ja	Ja	Organisation (Name)
Zertifikat Organisation Sign	Nein	explizit nicht	Ja	Nein	Organisation (Name)
Zertifikat Organisation Verschl	Nein	explizit nicht	Nein	Ja	Organisation (Name)
Zertifikat System Auth	Ja	explizit nicht	Nein	Nein	System (Name)
Zertifikat System Auth/Sign	Ja	explizit nicht	Ja	Nein	System (Name)
Zertifikat System Auth/Sign/Verschl	Ja	explizit nicht	Ja	Ja	System (Name)
Zertifikat System Sign/Verschl	Nein	explizit nicht	Ja	Ja	System (Name)
Zertifikat System Sign	Nein	explizit nicht	Ja	Nein	System (Name)
Zertifikat System Verschl	Nein	explizit nicht	Nein	Ja	System (Name)
Zertifikat Gruppenmailbox Sign/Verschl	Nein	explizit nicht	Ja	Ja	Gruppenmailbox (Name)

Klasse C Standard Zertifikate erfüllen ausschliesslich die oben genannten Zwecke und geben keinerlei weitere Aufschlüsse, Versicherungen oder Garantien. Insbesondere garantieren Klasse C Standard Zertifikate nicht, dass:

- das im Zertifikat genannte Subjekt aktiv in die Geschäftstätigkeiten involviert ist;
- das im Zertifikat genannte Subjekt sich an die geltenden gesetzlichen Vorschriften hält;
- das im Zertifikat genannte Subjekt vertrauenswürdig ist und im Geschäftsumfeld seriös handelt;
- Systeme mit diesem Zertifikat fehlerfrei funktionieren.

Ausgeschlossener Zweck

Die Zertifikate dieser Ausprägungen dürfen explizit nicht für die Server Authentisierung eingesetzt werden. Dafür stehen die SSL/TLS Zertifikate der Swiss Government PKI zur Verfügung. SSL Server Zertifikate mit der Key Usage ‚Server Authentication' unterliegen speziellen Bedingung und werden nur von der CA ‚Swiss Government SSL CA 01' ausgestellt. Hierfür gelten separate Guidelines und Vereinbarungs-/Nutzungsbedingungen. Ebenso gehören die Code Signing Zertifikate der SG-PKI zu den Klasse C Standardzertifikaten, auch diese unterliegen aber anderen Guidelines und Vereinbarungs-/Nutzungsbedingungen. (Weitere Informationen zu den Code Signing Zertifikaten erhalten Sie unter: https://www.bit.admin.ch/adminpki/00240/00241/06072/index.html?lang=de).

2 Aufgaben/Verpflichtungen des Ausstellungsberechtigten

Vor Ausstellung eines Klasse C Standard Zertifikates müssen die Richtigkeit der Daten, Existenz, Authentizität und Autorisierung des im Zertifikat genannten Inhabers zwingend geprüft und bestätigt werden. Der Ausstellungsberechtigte ist deshalb zu folgendem Vorgehen verpflichtet:

- **Existenz:** Der Aussteller von Klasse C Standard Organisations-, System- und Personen-Zertifikaten prüft im Namen der SG-PKI die Existenz des im Common Name (CN) des Zertifikates genannten Subjektes und der im Zertifikat genannten Mailadresse.
- **Richtigkeit der Daten und Authentizität:** Der Aussteller unternimmt im Namen der SG-PKI alle notwendigen und zumutbaren Schritte, um sicherzustellen, dass alle im Zertifikat enthaltenen Daten und Informationen korrekt sind. Der Aussteller muss zudem sicherstellen, dass die Richtigkeit der im Zertifikat enthaltenen Attribute über die im Zertifikat enthaltene Mailadresse bestätigt wird.
- **Autorisierung:** Der Aussteller hat im Namen der SG-PKI alle notwendigen und zumutbaren Schritte zu unternehmen, um zu verifizieren, dass der im Klasse C Standard Zertifikat genannte Inhaber (Besteller) zum Bezug des Zertifikates autorisiert ist.

Weiter gilt es zu beachten:

- **Vereinbarungs- und Nutzungsbedingungen:** Der berechtigte Aussteller für Klasse C Standard Zertifikate hat die Vereinbarungs- und Nutzungsbedingungen für Klasse C Standard Zertifikate der Swiss Government PKI zu lesen, akzeptieren und zu unterzeichnen.
- **Status:** Die SG-PKI stellt die Status der erteilten Ausstellungsberechtigung, der Zertifikate sowie Informationen über deren Gültigkeit/Revokation 7x24 Std. online abrufbar zur Verfügung und erfüllt damit die gesetzlichen Vorgaben sowie die Richtlinien des CA/Browser Forums.

- **Revokation:** Die SG-PKI hält sich an die Vorgaben der CA/Browser Forum Richtlinien und der CP/CPS der Swiss Government PKI und kann die erteilte Ausstellungsberechtigung und die Klasse C Standard Zertifikate gegebenenfalls aus den in den Vereinbarungs- und Nutzungsbedingungen genannten Gründen unverzüglich revozieren.

3 Policies

Alle geltenden gesetzlichen Vorgaben, Policies (inkl. der CP und CPS) und Richtlinien betreffend Klasse C Standard Zertifikaten sind im Internet auf der Website der SG-PKI publiziert unter: https://www.bit.admin.ch/adminpki/00240/00241/06111/index.html?lang=de.

4 Inhalt und Gültigkeit von Klasse C Standard Zertifikaten

Inhalt

Das Klasse C Standard Zertifikat der SG-PKI enthält Informationen betreffend:

- Herausgeber und ausstellende CA
- Informationen über die Root CA der ausstellenden CA
- Informationen über die geltende Policy
- Ausstell- und Ablaufdatum des Zertifikates
- Seriennummer des Zertifikates
- Informationen betreffend der CRL und dem OCSP
- Informationen betreffend der Auditoren der CA
- Informationen betreffend des Zertifikates (*DN=Distinguished Name, vgl. nächster Paragraph*):
  - Common Name
  - Organisation
  - Organisationseinheit
  - Ort

Distinguished Name

Klasse C Standardzertifikate unterscheiden sich in den anwendbaren DNs wie folgt:

Distinguished Name für Personenzertifikate*	
CN =	*CN= Common Name: Nachname(n) Vorname(n), Bsp.:* ***Mustermeier Hanspeter***
OU =	*OU= Organisationseinheit: Frei wählbar, z.B. Amt, Abteilung, Bereich, etc…* *Bsp.:* ***Bundesamt für Zukunftsforschung (BFZ)-Büroautomation***
O =	*O= Organisation: Auswählbar, zw. Administrative Einheit oder „Swiss Government PKI"* *Bsp.:* ***BFZ – Büroautomation*** *oder* ***Swiss Government PKI***
L =	*L= Location: Ort der Organisation, Bsp.:* ***Bern (BE)***
C =	*C= Country: Fixer Eintrag:* ***CH***
Distinguished Name für Systemzertifikate	
CN =	*CN= Common Name: System Name, Bsp.:* ***TUSER-SYSP-SCPP123***
OU =	*OU= Systemplattformname: Bsp.:* ***Systemplattform eDokumente***
O =	*O= Organisation: Fixer Eintrag:* ***Admin***
C =	*C= Country: Fixer Eintrag:* ***CH***
Distinguished Name für Organisationszertifikate*	
CN =	*CN= Common Name: Amtsbezeichnung (gemäss UID-Register), oder offizielle Übersetzung davon.* *Bsp.:* ***Bundesamt für Zukunftsforschung (BFZ)***
OU =	*OU= Organisationseinheit: Frei wählbar, z.B. UID gemäss UID-Register, Abteilung, Bereich, etc…* *Bsp.:* ***CHE-123.456.789*** *oder* ***Büroautomation***
O =	*O= Organisation: Frei wählbar, Bsp.:* ***Schweizerische Eidgenossenschaft*** *oder* ***BFZ – Büroautomation***
L =	*L= Location: Ort der Organisation, gegebenenfalls gemäss UID-Register, Bsp.:* ***Bern (BE)***
C =	*C= Country: Fixer Eintrag:* ***CH*** *(offen bei Org Zert. mit Auth/Sign/Enc Funktion, wird aber abgeraten)*
Distinguished Name für Gruppenmailboxzertifikate	
CN =	*CN= Common Name: Displayname der Gruppenmailbox: Bsp.:* ***_BIT-PKI-Info***
OU =	*OU= Organisationseinheit: Fixer Eintrag:* ***Group Mailboxes***
OU =	*OU= Organisationseinheit: Fixer Eintrag:* ***eGov-Services***
O =	*O= Organisation: Frei wählbar, Bsp.:* ***Schweizerische Eidgenossenschaft*** *oder* ***BFZ – Büroautomation***
L =	*L= Location: Ort der Organisation, Bsp.:* ***Bern (BE)***
C =	*C= Country: Fixer Eintrag:* ***CH***

*(*Das* C= Country *Feld ist bei den Policies mit Auth/Sign/Enc Funktion, offen. Es wird aber abgeraten Zertifikate mit allen 3 Funktionen auszustellen, sofern eine alternative Möglichkeit besteht. Die UID (Org. Zert.) ist bei nicht-schweizerischen Firmen nicht eruierbar, dieses Feld ist in der eben genannten Policy mit allen 3 Möglichkeiten ebenfalls wählbar. Der LRAO ist verantwortlich für jegliche im Zertifikat genannten Daten und hat die Pflicht die Ihm zugesandten Ausstelldaten vorgängig zu überprüfen.)*

Gültigkeit

Klasse C Standard Zertifikate der Swiss Government PKI sind max. 3 Jahre gültig. Die Ausstellungsberechtigung wird jährlich überprüft und muss für Folgejahr bestätigt jedes werden.

5 Bezug von Ausstellungsberechtigungen für Klasse C Standard Zertifikate

Bezug

Für den Bezug von Klasse C Standard Zertifikaten steht primär der Certificate Request Wizard (CRW) zur Verfügung. Ausnahme: Gruppenmailboxzertifikate werden in jedem Fall von der SG-PKI direkt ausgestellt und sind per Onlineformular auf: https://www.bit.admin.ch/adminpki/00240/00241/02370/02374/03685/index.html?lang=de bestellbar. Um Berechtigungen auf die CRW Applikation zu erhalten, sind folgende Dokumente nötig:

- Gültiges Zertifikat der Klasse B, ausgestellt auf den Namen des Antragstellers
- Ausgefülltes und elektronisch signiertes *Antragsformular für den Bezug von Ausstellungsberechtigungen Klasse C Standard Zertifikate der Swiss Government PKI*
- Elektronisch signierte *Vereinbarungs- und Nutzungsbedingungen für den Bezug von Ausstellungsberechtigungen für Klasse C Standard Zertifikate der Swiss Government PKI, der Bundesbehörden der Schweizerischen Eidgenossenschaft* (bei jeder Bestellung von Berechtigungen auf das CRW)
- Attest der Absolvierten *Schulung für Klasse C Standard Zertifikate*

Einzelne Organisationszertifikate können alternativ dazu auch direkt bei der SG-PKI bestellt werden. Dazu steht ein Bestellformular auf https://www.bit.admin.ch/adminpki/00240/00241/06111/06143/index.html zur Verfügung. Die Bestellung einzelner Organisations- und Gruppenmailbox-Zertifikate direkt über die SG-PKI, setzt die Bestätigung dieser *Guidelines* und die Akzeptierung der *Vereinbarungs-und Nutzungsbedingungen der Klasse C Standardzertifikate der SG-PKI voraus.*

Identifikation/Verifizierung

Die persönliche Identifizierung des Antragstellers wird durch die Prozesse der SG-PKI Zertifikate der Klasse B sichergestellt. Für die Berechtigungen auf das CRW muss der Antragsteller über ein gültiges Zertifikat der Klasse B verfügen und die Dokumente müssen mit diesem persönlichen Klasse B Zertifikat signiert werden. Die Signatur auf dem Dokument wird zum Zeitpunkt der Ausstellung validiert. Die Berechtigung zur Ausstellung von Klasse C Standard Zertifikaten wird auf das persönliche Klasse B Zertifikat aufgeschaltet und ist damit weder übertragbar, noch darf sie delegiert werden. Eine Änderung/ Erneuerung des persönlichen Klasse B Zertifikates bedingt eine Neuregistrierung beim CRW.

Schulung

Der Antragsteller muss vor der Freigabe der Berechtigungen eine halbtägige Schulung absolvieren. Die Schulungen für die Klasse C Standard Zertifikate sind auf der Seite https://www.bit.admin.ch/adminpki/00240/00241/06111/06141/index.html?lang=de publiziert. Der Nachweis der absolvierten Schulung ist für die Berechtigungserteilung zwingend notwendig.

Verbindlichkeit

Das vorliegende Formular und die *Vereinbarungs- und Nutzungsbedingungen für den Bezug von Ausstellungsberechtigungen für Klasse C Standardzertifikate der SG-PKI* müssen vom Antragsteller digital mit einem Klasse B Zertifikat der SG-PKI signiert und elektronisch eingereicht werden.

6 Schutz des CRW Zuganges

Übertragbarkeit

Der Zugang und die Berechtigungen zu den Policy-Templates im CRW sind persönlich und mit dem Klasse B Zertifikat gesichert. Es ist insbesondere untersagt, die Zugangsdaten oder gar das berechtigte Klasse B Zertifikat weiterzugeben.

Meldepflicht

Der Aussteller muss eine allfällige Beendigung seiner Aufgabe/Rolle der SG-PKI melden und die Sperrung der Berechtigungen zum CRW mittels Antragsformular anfordern.

7 Schutz des privaten Schlüssels und des Zertifikates

Übertragbarkeit

Klasse C Standard Zertifikate für Personen oder Systeme werden auf ein bestimmtes Subjekt bzw. Objekt ausgestellt und sind nicht übertragbar. Klasse C Standard Zertifikate für Organisationen oder Gruppenmailboxen sind für eine bestimmte Organisation oder auf eine bestimmte Mailadresse ausgestellt und dürfen nur im Namen dieser Subjekte eingesetzt werden, obschon sich das Zertifikat auf mehreren Clients bzw. User-Accounts befinden darf.

Schutz der privaten Schlüssel

Wird vom Inhaber (oder Antragsteller) die Erstellung der Schlüsselpaare dem Aussteller delegiert, muss der Transfer des P12-Paketes (Zertifikat und Schlüsselpaar) an den Inhaber zwingend in abgesicherter/verschlüsselter Form erfolgen (persönliche Übergabe, verschlüsselte Kommunikation, eingeschriebener Postversand inkl. Transportpin). Das Passwort zum privaten Schlüssel muss separat und ebenfalls in einer abhörsicheren Form kommuniziert werden (separate E-Mail, SMS, brieflich, persönlich, etc.). Es ist dem Aussteller strengstens untersagt den privaten Schlüssel bzw. das P12-File eines anderen Inhabers zu archivieren oder auf sonst eine Weise aufzubewahren. Nach der Übergabe des P12-Paketes an den Inhaber ist der private Schlüssel vom Client und/oder von weiteren Speichermedien des Ausstellers zu vernichten.

Passwort und Installation des privaten Schlüssels

Unabhängig davon, ob das Zertifikat auf einen Träger geschrieben wird oder als sog. „Softtoken“ eingesetzt wird, gelten für die privaten Schlüssel folgende Regelungen:

- Das Passwort zur Installation des privaten Schlüssels muss durch den Zertifikatsinhaber sicher aufbewahrt werden.
- Das Passwort des privaten Schlüssels muss mind. 8-stellig sein und mind. aus Gross-, Kleinbuchstaben und Zahlen zusammengesetzt sein. Das Passwort darf niemals unbefugten Dritten bekanntgegeben werden.
- Das Passwort zur Installation des privaten Schlüssels ist einmalig und darf nicht für weitere private Schlüssel wiederverwendet werden.
- Beim Installieren des Zertifikates darf der private Schlüssel nicht als exportierbar gekennzeichnet sein.

Publikation

Die öffentlichen Schlüssel der Gruppenmailboxzertifikate von bundesinternen Entitäten werden von der SG-PKI direkt nach der Ausstellung im Admin Directory publiziert. Auf Wunsch können auch die öffentlichen Schlüssel der Organisationszertifikate im AdminDir der Bundesverwaltung publiziert werden. Ebenso besteht die Möglichkeit, die öffentlichen Schlüssel der Organisationszertifikate und der Gruppenmailboxzertifikate auf einer Internetseite der SG-PKI zu publizieren. Die Publikation muss über die pki-info@bit.admin.ch beantragt werden. Die Aktualisierung der veröffentlichten Zertifikate liegt in der Verantwortung des Inhabers.

Meldepflicht

Ein allfälliger Verlust des Zertifikates muss umgehend der SG-PKI über das Servicedesk BIT (servicedesk@bit.admin.ch) gemeldet werden. Die SG-PKI sperrt in der Folge das Zertifikat und publiziert die Sperrung auf einer öffentlichen elektronischen Sperrliste. Selbst wenn das Zertifikat wieder gefunden wird, bleiben die Zertifikate gesperrt und sind somit ungültig. Nach erfolgter Sperrung im CRW kann ein neues Klasse C Standard Zertifikat bestellt werden. Der Prozess der Ausstellung eines neuen Klasse C Standard Zertifikates entspricht der Erstausstellung.

Funktionswechsel in der Organisation, Namenswechsel (z.B. nach Heirat (Personen), aber auch von Systemen) oder Änderung der E-Mail Adresse und der Bezeichnung einer Organisation bedingen die Revokation des bestehenden und die Ausstellung eines neuen Zertifikates.

8 Revokation

Revokationen müssen der SG-PKI gemeldet werden. Dazu steht Ihnen ein Formular auf der Seite: https://www.bit.admin.ch/admin-pki/00240/00241/06111/index.html?lang=de zur Verfügung. Das Formular muss mit einem Klasse B Zertifikat der SG-PKI signiert und elektronisch dem Servicedesk BIT (servicedesk@bit.admin.ch) eingereicht werden. Revokationen können von folgenden Instanzen und Personen beantragt werden:

- vom Inhaber;
- von der Linie;
- vom Sicherheitsbeauftragten der Organisation;
- vom Aussteller;
- vom Serververantwortlichen;
- vom Mailboxverantwortlichen;
- vom Security Officer der SG-PKI;
- vom Verantwortlichen der SG-PKI.

9 Preise

CRW Berechtigungen

Die Berechtigung für die Ausstellung von Zertifikaten im CRW wird mit jährlichen Kosten von CHF 250.- pro Person in Rechnung gestellt. Diese Kosten decken den Betrieb der Plattform und den Support der Berechtigten ab.

Zertifikatspreise

Zertifikate, die über das CRW im Self-Service Prozedere ausgestellt wurden, werden jährlich mit CHF 30.-/Zertifikat fakturiert.
Zertifikate, die von der SG-PKI ausgestellt werden, sind mit jährlichen Kosten von CHF 175.- pro ausgestelltes Zertifikat verbunden.

Die Kosten der ausgestellten Zertifikate sind für die ganze Dauer der Gültigkeit (max. 3 Jahre), auch nach einer allfälligen vorzeitigen Revokation, fällig.

10 Bestätigung / Akzeptierung

Mit dem Ankreuzen des Formularfelds «Bestätigung» auf der Formularseite wird bestätigt, dass diese Guidelines gelesen, verstanden und akzeptiert wurden. Zudem aktiviert sich dadurch das Signaturfeld, in welchem das Formular digital mit einem Klasse B Zertifikat der SG-PKI unterzeichnet werden muss. Bei Fragen kann die Swiss Government PKI unter der Mailadresse pki-info@bit.admin.ch kontaktiert werden[1].

[1] Bitte lesen Sie auch die *Vereinbarungs- und Nutzungsbedingungen für den Bezug von Ausstellungsberechtigungen für Klasse C Standard Zertifikate der Swiss Government PKI*. Bei Ihrer Berechtigungsbestellung für das CRW wird eine signierte Kopie dieses Dokuments verlangt. https://www.bit.admin.ch/adminpki/00240/00241/06111/index.html?lang=de

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: _____