Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

Antragsformular für Code Signing Zertifikate der Swiss Government PKI Klasse E (Windows PKI)

V1.1

Ich beantrage im Namen der unten genannten Organisation die Ausstellung eines Code Signing Zertifikates:

Antragsteller	
Anrede	
Name, Vorname, Suffix	
Telefonnummer (Direktwahl Antragsteller)	
E-Mail	
AdminDir Eintrag vorhanden	☐ Ja ☐ Nein

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

Die **Schlüssellänge** des Zertifikates ist **2048 bit**. Das Zertifikat wird als **Softtoken** ausgestellt. Folgende **Optionen** stehen für das Zertifikat zur Verfügung:

a) Ich wünsche eine **Gültigkeitsdauer** von:
(Bitte Gültigkeitsdauer immer angeben) 1 Jahr ☐ 2 Jahre ☐

*Der **Distinguished Name** (DN) wird von der Swiss Government PKI gemäss folgendem Beispiel bestimmt:*

CN = ***Code Signing Officer #BFZ*** *(Amtsabkürzung gemäss UID-Register.)*
OU = ***Büroautomation***
O = ***Bundesamt für Zukunftsforschung BFZ*** *(Amtsbezeichnung gemäss UID-Register. ohne Kommas)*
L = ***Bern (BE)***
C = ***CH***

Bestätigung:

Der Inhaber verpflichtet sich dazu, das Zertifikat und den dazugehörigen privaten Schlüssel ausschliesslich für autorisierte und legale Zwecke einzusetzen. Es ist insbesondere untersagt, willentlich Schadcode oder -Software zu signieren. Der Inhaber stellt zudem sicher, dass ihm Inhalt, Zweck und Wirkung der zu signierenden Software bekannt sind. Das Code Signing Zertifikat und dessen privater Schlüssel dürfen nur für autorisierte (Unternehmens-) Geschäfte und unter Einhaltung aller geltenden gesetzlichen Vorschriften eingesetzt werden.

Der Inhaber trägt die im Umfang seines Arbeitsvertrags vereinbarte Verantwortung für alle durch ihn vorgenommenen Signierungen von Codes/Software sowie für allfällig daraus resultierende Schäden und deren Folgen. ☐

Antragsteller Name / Vorname: Funktion:	**Datum:**	**Elektronische Signatur:**
Unterschriftsberechtigte(r) der Organisation Name / Vorname: Funktion:	**Datum:**	**Elektronische Signatur:**

Nutzungsbedingungen der Swiss Government PKI zum Bezug von Code Signing Zertifikaten der Klasse E

Erläuterungen zum Bezug und Einsatz von Code Signing Zertifikate der Windows CA der Swiss Government PKI
V1.0, 15.09.2017

1 Zweck von Code Signing Zertifikaten

Zweck

Der Zweck von Code Signing Zertifikaten der Klasse E ist die vertrauenswürdige Signierung bei der Paketierung von Software, die innerhalb der Bundesverwaltung verteilt wird. Im gleichen Zug werden die Endanwender mit der Signatur über den Ursprung und die Integrität der BAB-Software informiert. Die Signatur ermöglicht es festzustellen, ob allfällige illegale Mutationen des ursprünglichen Paketes bestehen.

Ausgeschlossener Zweck

Code Signing Zertifikate der Klasse E erfüllen ausschliesslich den oben genannten Zweck und geben keinerlei weitere Aufschlüsse, Versicherungen oder Garantien. Insbesondere garantieren Code Signing Zertifikate der Klasse E nicht, dass der Code frei von Schwachstellen, Malwares, Bugs oder anderen Problemen ist.

2 Bestätigungen

Die Swiss Government PKI bestätigt zum Zeitpunkt der Ausstellung eines Code Signing Zertifikates folgende Tatsachen:

- **Gültige Registrierung:** Der Urheber des Code Signing Zertifikates ist im Admin-Directory des Bundes als Bundesangestellter registriert.
- **Identität:** Der rechtliche Name des im Code Signing Zertifikats genannten Objektes stimmt mit dem Namen im Admin-Directory überein.
- **Autorisierung:** Die Swiss Government PKI hat alle notwendigen und zumutbaren Schritte unternommen, um zu verifizieren, dass der Inhaber des Code Signing zum Bezug des Zertifikates autorisiert ist.
- **Richtigkeit der Daten:** Die Swiss Government PKI hat alle notwendigen und zumutbaren Schritte unternommen, um sicherzustellen, dass alle im Zertifikat enthaltenen Daten und Informationen korrekt sind.
- **Vereinbarung/ Nutzungsbedingungen:** Der Inhaber des Klasse E Code Signings hat diese Nutzungsbedingungen gelesen, akzeptiert und unterzeichnet.
- **Status:** Die Swiss Government PKI stellt den Status des Zertifikats sowie Informationen über dessen Gültigkeit/Revokation 7x24 Std. online abrufbar zur Verfügung und erfüllt damit die gesetzlichen Vorgaben.
- **Revokation:** Die Swiss Government PKI hält sich an die CP/CPS der Swiss Government PKI Klasse E und kann das Code Signing Zertifikat gegebenenfalls unverzüglich revozieren.

3 Inhalt und Gültigkeit des Code Signing Zertifikates

Inhalt

Das Code Signing Zertifikat der Swiss Government PKI enthält Informationen betreffend:

- Herausgeber und ausstellenden 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 den Inhaber des Zertifikates:
  - Common Name der Organisation
  - Kategorie der Geschäftstätigkeit des Inhabers

Gültigkeit

Der Antragsteller kann im Formular die Gültigkeitsdauer von 1 bzw. 2 Jahre wählen. Das Code Signing Zertifikat der Swiss Government CA der Klasse E ist max. 2 Jahre Gültig.

4 Bezug von Code Signing Zertifikaten der Klasse E

Bezug

Für den Bezug von Code Signing Zertifikaten der Swiss Government PKI sind folgende Dokumente nötig:

- Gültiges Zertifikat der Klasse B, ausgestellt auf den Namen des Antragstellers.
- Ausgefülltes und elektronisch signiertes *Antragsformular für Code Signing Zertifikate der Swiss Government PKI Klasse E*
- Eintrag der Bestellenden Person im Admin-Directory des Bundes
- Bewilligung/Freigabe des/der Unterschriftsberechtigten der Organisation mittels elektronischer Signatur

Identifikation

Die persönliche Identifizierung des Antragstellers wird durch die Prozesse der Swiss Government PKI Zertifikate der Klasse B sichergestellt. Für die Ausstellung eines Code Signing Zertifikats muss der Antragsteller über ein gültiges Zertifikat verfügen und die Dokumente müssen mit dem persönlichen Klasse B Zertifikat signiert werden. Die Signatur auf dem Dokument wird zum Zeitpunkt der Ausstellung validiert. Die Personenidentifikation und somit die Ausstellung und Übergabe des Zertifikates erfolgt aufgrund einer positiven Validierung der Signatur.

Verifizierung

Um die persönliche Präsenz an der angegebenen Geschäftsadresse zu verifizieren, ist der Eintrag im AdminDirectory des Bundes, zudem ein Organisationsausweis (z.B. Bundesausweis mit Foto) oder eine Zugehörigkeitsbestätigung erforderlich.

Verbindlichkeit

Dieses Formular muss digital mit einem Klasse B Zertifikat der Swiss Government PKI signiert und elektronisch eingereicht werden.

5 Schutz des privaten Schlüssels und des Zertifikates

Übertragbarkeit

Das Code Signing Zertifikat ist immer auf eine Person ausgestellt, auch wenn der Name der Person im Zertifikat nicht aufgeführt und durch eine Organisationsbezeichnung substituiert ist. Die persönlichen Angaben über den Inhaber werden bei der Swiss Government PKI geführt. Das Zertifikat ist somit persönlich und nicht übertragbar.

PIN

Das Zertifikat (und somit der Zertifikatsträger /-Medium: SmartCard, USB-Stick, etc.) muss mit einem mind. 8-stelligem PIN gesichert werden, wobei rein numerische PINs sowie gemischte PINs erlaubt sind. Der PIN darf niemals Dritten bekanntgegeben werden.

Kommt ein Transport-PIN zum Einsatz, muss dieser mindestens 16-stellig sein und den oben genannten Regelungen folgen (*Ist bei einer brieflichen Lieferung des Zertifikates die Regel*).

Meldepflicht

Melden Sie einen allfälligen Verlust des Zertifikatsträgers umgehend der Swiss Government PKI über das Servicedesk BIT (servicedesk@bit.admin.ch). Die SG-PKI sperrt in der Folge Ihre Zertifikate und publiziert die Sperrung auf einer öffentlichen elektronischen Sperrliste. Selbst wenn Sie den Trägermedium des Zertifikates wieder finden sollten, bleiben die Zertifikate gesperrt und sind somit ungültig. Sie können nach erfolgter Sperrung bei der Swiss Government PKI die Ausstellung eines neuen Code Signing Zertifikates verlangen. Der Prozess der Ausstellung eines neuen Code Signing Zertifikats entspricht der Erstausstellung.

Funktionswechsel in der Organisation, Namenswechsel (z.B. nach Heirat) oder Änderung der E-Mail Adresse bedingen die Revokation des ausgestellten Zertifikates und ggf. eine Ausstellung eines neuen Zertifikates.

6 Revokation

Revokationen müssen der Swiss Government PKI gemeldet werden. Dazu steht Ihnen ein Formular auf der PKI-Homepage: www.pki.admin.ch zur Verfügung. Das Formular muss mit einem Klasse B Zertifikat der Swiss Government PKI signiert und elektronisch dem Servicedesk BIT (servicedesk@bit.admin.ch) eingereicht werden.

7 Bestätigung

Mit dem Kreuzchen im Formularfeld «Bestätigung» auf der Formularseite bestätigen Sie, diese Nutzungsbedingungen gelesen und verstanden zu haben. Das Signaturfeld aktiviert sich nur nachdem Sie dieses Formularfeld aktiviert haben. Sollten Sie Fragen haben, steht Ihnen die Swiss Government PKI über das Servicedesk BIT (servicedesk@bit.admin.ch) zur Verfügung.