Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Betrieb
Betrieb Frontend Services
PKI

Berechtigung zum Bezug von (EV)SSL Zertifikaten der Swiss Government PKI V2.0

Die Person muss für die Freischaltung im Besitz eines Klasse B Zertifikates sein!

Für die folgende Person wird die Berechtigung zum Bezug von SSL- Zertifikaten (Maschinen-/ Serverzertifikate) der *Swiss Government PKI* für die nachstehend aufgeführten Domänen beantragt:

Antragsteller	
Anrede	
Name, Vorname, Suffix	
Kanton / Amt / Firma	
Vollständige Adresse	
Telefonnummer	
E-Mail	

Verifikationsstärke[1]:

***Prüfung:** **OV** ☒ **EV** ☐

Bestätigung:
Mit dem Anklicken des Formularfeldes bestätigen Sie die Guidelines (folgende Seiten), sowie die Vereinbarung/ Nutzungsbedingungen der Swiss Government PKI gelesen und akzeptiert zu haben: ☐

Domäne *admin.ch*:

Für die Domäne ***admin.ch*** und die dazugehörigen *dotted-Hostnames* (Bsp.: *xy-blog.admin.ch*) muss die Unterschrift des Domain Owners (René Staudenmann BIT) eingeholt werden.

Die Person darf für Domänen unterhalb admin.ch SSL-Zertifikate beziehen:	
Unterschrift Domain Owner ***admin.ch***	

[1] **OV:** *Organization Validated*: Die Berechtigung wird auf Organisationsstufe Überprüft
EV: *Extended Validation*: Für die Berechtigung wird eine weitgehende Prüfung der Berechtigungen auf die Domäne, von der Organisation und für die Person durchgeführt. Es ist ein Autorisationsbrief der Organisation notwendig. Zertifikate die mit einer EV-Berechtigung ausgestellt werden, sind in der URL am grünen Balken erkenntlich. Siehe dazu auch nähere Informationen in den Guidelines.

Bundesamt für Informatik und Telekommunikation BIT
SwissGov-PKI Order Manager
Monbijoustrasse 74
CH-3003 Bern

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Betrieb
Betrieb Frontend Services
PKI

Domäne(n) ausserhalb admin.ch:

Für die nachstehenden Domänen bestätigt der Domain Owner mit seiner Unterschrift, dass

1. Der Antragsteller berechtigt ist, für den aufgeführte(n) Domäne(n) (EV) SSL-Zertifikate bei der Swiss Government PKI zu beantragen.
2. Der Domain Owner vom CP/CPS (Certificate Policy and Certification Practice Statement) der „Swiss Government Root CA III" Kenntnis genommen hat http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf
3. Die Swiss Government PKI berechtigt ist, für Server in der aufgeführten Domäne (EV) SSL-Zertifikate auszustellen.

Domäne	Ort, Datum	Unterschrift Domain Owner gemäss Eintrag im *WhoIs*

Antragsteller Name Vorname: / Funktion:	**Datum:**	**(Elektr.) Unterschrift:**
/		

Bitte senden sie die vollständig ausgefüllten und unterschriebenen Formulare an die untenstehende Postadresse. Elektronisch unterschriebene Formulare können an die Mail Adresse pki-info@bit.admin.ch eingereicht werden.

Bundesamt für Informatik und Telekommunikation BIT
SwissGov-PKI Order Manager
Monbijoustrasse 74
CH-3003 Bern

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

NICHT KLASSIFIZIERT

Guidelines zum Bezug von (EV) SSL/TLS Zertifikaten

Erläuterungen zum Bezug und Einsatz von (EV) SSL/TLS Zertifikaten der Swiss Government PKI

V 1.0, 01.06.2016

1 Zweck von (EV) SSL/TLS Zertifikaten

Zweck

Der Zweck von (EV) SSL/TLS Zertifikaten ist die vertrauenswürdige Authentisierung von Servern. Die Zertifikate werden in den Ausprägungen ‚Server Authentication', ‚Client Authentication' und ‚Server/Client Authentication' ausgestellt. (EV) SSL/TLS Zertifikate werden ausschliesslich für Systeme ausgestellt, die einen Fully Qualified Domain Name (FQDN) aufweisen können.

Ausgeschlossener Zweck

(EV) SSL/TLS Zertifikate erfüllen ausschliesslich den oben genannten Zweck und geben keinerlei weitere Aufschlüsse, Versicherungen oder Garantien.
Insbesondere garantieren (EV) SSL/TLS Zertifikate nicht, dass:

- Systeme mit diesem Zertifikat fehlerfrei funktionieren,
- der Betreiber des im Zertifikat genannten Servers und die Inhalte des Servers sich an die geltenden gesetzlichen Vorschriften halten oder
- der Betreiber des im Zertifikat genannten Servers und die Inhalte des Servers vertrauenswürdig sind und Ersterer im Geschäftsumfeld seriös handelt.

2 Bestätigungen

Die Swiss Government PKI (SG-PKI) bestätigt zum Zeitpunkt der Ausstellung eines (EV) SSL/TLS Zertifikates folgende Tatsachen:

- **Rechtlich gültige Existenz:** Der Antragsteller des (EV) SSL/TLS Zertifikates sowie der entsprechende Domain-Owner und die Organisation existieren als Rechtssubjekte und sind amtlich registriert.
- **Identität:** Die Domäne sowie die Organisation des im (EV) SSL/TLS Zertifikat genannten Servers und OID stimmen mit den Einträgen in den öffentlichen Registern überein und werden durch eine oder mehrere verantwortliche natürliche und identifizierbare Personen repräsentiert.
- **Autorisierung:** Die SG-PKI hat alle notwendigen und zumutbaren Schritte unternommen, um zu verifizieren, dass der Antragsteller des (EV) SSL/TLS Zertifikats zum Bezug eines Zertifikates für die Domäne und die Organisation autorisiert ist.
- **Richtigkeit der Daten:** Die SG-PKI hat alle notwendigen und zumutbaren Schritte unternommen, um sicherzustellen, dass alle im Zertifikat enthaltenen Daten und Informationen korrekt sind.
- **Vereinbarung/ Nutzungsbedingungen:** Der Antragsteller des (EV) SSL/TLS Zertifikates hat die *Vereinbarungs- und Nutzungsbedingungen EV SSL* der Swiss Government PKI gelesen, akzeptiert und unterzeichnet.
- **Status:** Die SG-PKI stellt den Status des Zertifikats sowie Informationen über dessen Gültigkeit/Revokation 7x24 Std. online abrufbar zur Verfügung und erfüllt 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 das (EV) SSL/TLS Zertifikat gegebenenfalls aus den in den *Vereinbarungs- und Nutzungsbedingungen (EV) SSL/TLS* genannten Gründen unverzüglich revozieren.

3 Policies

Alle geltenden gesetzlichen Vorgaben, Policies (inkl. der CP und CPS) und Richtlinien betreffend (EV) SSL/TLS Zertifikaten sind im Internet auf der Website der SG-PKI publiziert unter: https://www.bit.admin.ch/adminpki/00240/00241/05913/index.html?lang=de

4 Inhalt und Gültigkeit des (EV) SSL/TLS Zertifikates

Inhalt

Das (EV) SSL/TLS Zertifikat der SG-PKI enthält folgende Informationen:

- Herausgeber (CSP) und ausstellende CA
- Root CA der ausstellenden CA
- Die geltende Policy
- Ausstell- und Ablaufdatum des Zertifikates
- Seriennummer des Zertifikates
- CRL und OCSP
- Auditoren der CA
- OID der Organisation
- FQDN (Fully Qualified Domain Name)
- Ländercode
- Staat, Kanton oder Ortschaft der Organisation

Gültigkeit

Das (EV) SSL/TLS Zertifikat der Swiss Government PKI ist max. 3 Jahre gültig.

5 Bezug von (EV) SSL/TLS Zertifikaten

Bezug

Für den Bezug von (EV) SSL/TLS Zertifikaten der SG-PKI bestehen folgende Anforderungen:

- Gültiges Zertifikat der Klasse B, ausgestellt auf den Namen des Antragstellers.
- Ausgefülltes und elektronisch signiertes *Berechtigungsformular für (EV) SSL/TLS Zertifikate der Swiss Government PKI*
- Elektronisch signierte *Vereinbarungs- und Nutzungsbedingungen (EV) SSL/TLS*
- Rechtsgültig unterzeichneter *Authorization Letter by Organization (EV) SSL*

Ausgeschlossener Bezug

Es werden grundsätzlich keine (EV) SSL Zertifikate für Server ohne FQDN (z.B. *IP-Adressen*) oder Wild-Cards (z.B. **.bit.admin.ch*) vergeben.

Identifikation

Die persönliche Identifizierung des Antragstellers wird durch die Prozesse der SG-PKI Zertifikate der Klasse B sichergestellt. Für die Ausstellung eines (EV) SSL/TLS Zertifikats muss der Antragsteller über ein gültiges solches Zertifikat verfügen. Das Berechtigungsdokument zum Bezug von Zertifikaten muss mit dem persönlichen Klasse B Zertifikat signiert werden. Für jede Domäne muss der Antragsteller vom jeweiligen Domain-Owner schriftlich ermächtigt worden sein, Zertifikate zu beziehen. Die Berechtigung zum Bezug der Zertifikate für eine bestimmte Domäne wird durch die Prozesse der SG-PKI verifiziert, bzw. über den Domain-Owner überprüft. Die Identifikation der Organisation und der Personen und somit die Ausstellung und Übergabe des Zertifikates erfolgt aufgrund einer positiven Validierung der Signaturen, der Berechtigung, des FQDNs, der OID bzw. Organisation und des CSRs (Certificate Signing Request).

Verifizierung

Um die Präsenz der Domäne und die Berechtigung zum Bezug von SSL/TLS Zertifikaten der Swiss Government PKI zu verifizieren, werden öffentliche Register (www.whois.com; www.firestorm.ch, etc.), Bundesinterne und externe Register (Admin-Directory, www.uid.admin.ch, SHAB) und die SG-PKI interne Datenbanken für berechtigte (EV) SSL/TLS Antragsteller konsultiert. Die im Formular angegebenen Kontakte, insbesondere die aufgeführten Domain-Owner, werden telefonisch, schriftlich oder persönlich auf die Richtigkeit ihrer Unterschrift auf dem Antragsformular befragt.[1]

Verbindlichkeit

Das Berechtigungsdokument und die *Vereinbarungs- und Nutzungsbedingungen (EV) SSL/TLS* müssen digital mit einem Klasse B Zertifikat der SG-PKI signiert und elektronisch eingereicht werden.

6 Schutz des privaten Schlüssels und des Zertifikates

Übertragbarkeit

Das (EV) SSL/TLS Zertifikat ist jeweils für einen spezifischen Server oder Client ausgestellt und nicht übertragbar. .

Privater Schlüssel

Der Antragsteller muss alle geeigneten und angemessenen Massnahmen treffen, damit die Integrität des privaten Schlüssels und der Zugriffschutz auf das Zertifikat jederzeit gewährleistet sind. Der private Schlüssel und das Zertifikat dürfen Dritten nicht zugänglich gemacht werden. Ausgenommen davon ist der Fall, in welchem der Antragsteller nicht selber Zertifikatsinhaber ist, sondern das Zertifikat gemäss seinem amtsinternen Zuständigkeitsbereich berechtigterweise für eine andere Person aus seinem Amt/Departement beantragt. In diesem Fall ist der Antragsteller dazu verpflichtet, die Verpflichtungen aus den Vereinbarungs- und Nutzungsbedingungen (EV) SSL/TLS sowie aus den vorliegenden Guidelines schriftlich auf den jeweiligen Zertifikatsinhaber zu überbinden.

Meldepflicht

Der allfällige Verlust des Zertifikates muss umgehend der SG-PKI über das Servicedesk BIT (servicedesk@bit.admin.ch) mitgeteilt werden. Die SG-PKI sperrt in der Folge die Zertifikate und publiziert die Sperrung auf einer öffentlichen elektronischen Sperrliste. Der Prozess der Erneuerung eines (EV) SSL/TLS Zertifikats entspricht der Erstausstellung.

7 Revokation

Revokationen müssen bei der SG-PKI unter Angabe der Revokationsgründe über das Servicedesk BIT beantragt werden.

8 Bestätigung / Akzept

Durch Ankreuzen des Feldes «Bestätigung» im Berechtigungsdokument bestätigt der Antragsteller, diese Guidelines gelesen, verstanden und akzeptiert zu haben. Zudem aktiviert sich dadurch das Signaturfeld, in welchem das Formular digital mit einem Klasse B Zertifikat der SG-PKI unterzeichnet werden muss. Bei Fragen steht die Swiss Government PKI unter der Mailadresse pki-info@bit.admin.ch zur Verfügung.

---

[1] **OV-Zertifikate (SG PKI Policy OIDs 2.16.756.1.17.3.62.1/2.16.756.1.17.3.62.2)**

Bei *Organisation Validated (OV)* Zertifikate wird die Organisation überprüft, welche das Zertifikat beantragt. Der Name der Organisation ist im Zertifikat aufgeführt.

EV-Zertifikate(SG PKI Policy OIDs 2.16.756.1.17.3.62.4/2.16.756.1.17.3.62.5)
Bei *Extended Validation (EV)* Zertifikate bieten das maximale Vertrauen für die Benutzer, und erfordern die meisten Bemühungen der CA, den Antrag zu validieren. Es müssen zusätzliche Unterlagen zur Verfügung gestellt werden, um ein EV-Zertifikat ausstellen zu können.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

NICHT KLASSIFIZIERT

Vereinbarungs- und Nutzungsbedingungen (EV) SSL/TLS

für den Bezug von (EV) SSL/TLS Authentisierungszertifikate der Swiss Government PKI der Bundesbehörden der Schweizerischen Eidgenossenschaft

V1.0, 02.06.2016

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 Standarddienste des ISB werden dabei auch *Klasse C SSL/TLS Authentisierungszertifikate* und *Klasse C EV SSL/TLS Authentisierungszertifikate* (im Folgenden (EV) SSL Zertifikate genannt) ausgestellt, sowie die *Berechtigungen zum Beantragen* von solchen Zertifikaten vergeben. Ausstellung, Bezug und Nutzung der (EV) SSL 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 integrierenden Bestandteil dieser Vereinbarungs- und Nutzungsbedingungen. Die jeweils gültigen Versionen, sowohl der vorliegenden Vereinbarungs- und Nutzungsbedingungen als auch der CA/Browser Forum Guidelines, sind publiziert auf:
https://www.bit.admin.ch/adminpki/00240/00241/05913/05914/index.html?lang=de.

Zu beachten sind des Weiteren die «Guidelines der Swiss Government PKI zum Bezug von Klasse C (EV) SSL/TLS Authentisierungszertifikaten». Diese müssen bei der Bestellung der Berechtigung zum Beantragen und bei jeder Mutation der Berechtigungen separat akzeptiert werden.

Vollständigkeit und Genauigkeit der Informationen

Der berechtigte Antragsteller von (EV) SSL Zertifikaten (in Folge «Antragsteller» genannt[2]) verpflichtet sich dazu, dem CSP beim Beantragen der Zertifikate die richtigen und vollständigen Informationen zu liefern und Änderungen zu melden. Insbesondere hat er darauf zu achten, dass alle Informationen/Daten, im speziellen der FQDN (Fully Qualified Domain Name) und die Einträge der *Location* (des Ortes [L=]), der *Organization* (der Organisation [O=]) und der *Organization Unit* (Organisationseinheit [OU=], im CSR (Certificate Signing Request) des Zertifikates vollständig und korrekt sind. Ausserdem ist der Antragsteller verpflichtet, den CSP zu informieren, wenn sich seine Rolle oder sein Zuständigkeitsbereich wesentlich ändert.

Schutz des Zugangs zur Bestellplattform und der Zertifikate

(EV) SSL Zertifikate können für (Web-)Server oder Clients ausgestellt werden. Die Angaben über den Antragsteller werden bei der Swiss Government PKI gespeichert. Der Antragsteller verpflichtet sich, alle angemessenen Vorkehrungen zu treffen, um die Zugangssicherheit, die Vertraulichkeit und den Schutz vor Missbrauch der Bestellplattform jederzeit sicherzustellen. Die Zugangsberechtigung zur Bestellplattform darf auf keinen Fall unberechtigten Dritten zugänglich gemacht werden und die Plattform kann und darf nur für die dafür vorgesehenen Zwecke im Zusammenhang mit der Beantragung von Zertifikaten verwendet werden.

Auch der private Schlüssel darf Dritten nicht zugänglich gemacht werden. Ausgenommen davon ist der Fall, in welchem der Antragsteller nicht selber Zertifikatsinhaber ist, sondern das Zertifikat in Erfüllung seines Aufgaben-/Zuständigkeitsbereich berechtigterweise für eine andere Person beantragt und dieser dann übergibt.

Der Antragsteller haftet für jeden Schaden, der durch die Weitergabe der Zugangsberechtigung zur Bestellplattform oder durch die Weitergabe der ihm anvertrauten Zertifikate und Schlüssel, sowie der allfällig damit verbundenen Medien an unberechtigte Dritte entstanden ist.

---

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

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

Der CSP behält sich vor, dem Antragsteller bereits bei einem konkreten Verdacht auf Missbrauch, unautorisierten Zugang oder Weitergabe der vorangehend beschriebenen Zugangsdaten, Zertifikate und Schlüssel an unberechtigte Dritte, die Zugangsberechtigungen zur Bestellplattform ohne Vorinformation zu entziehen.

Nutzung der webbasierten Bestellplattform und der Zertifikate

Der Antragsteller verpflichtet sich sicherzustellen, dass die Bestellplattform und die Zertifikate ausschliesslich für autorisierte und legale Zwecke eingesetzt werden. Es ist insbesondere untersagt, willentlich Zertifikate mit falschen oder ungenauen Informationen zu bestellen. Des Weiteren dürfen Zertifikate ausschliesslich für Domänen ausgestellt werden, für die er vom Inhaber der Domäne explizit autorisiert wurde (unterzeichnetes Berechtigungsdokument). Der Antragsteller stellt zudem sicher, dass ihm Inhalt, Zweck und Wirkung der von ihm beantragten Zertifikate bekannt sind. Bestellplattform und (EV) SSL 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.

Berichterstattung und Revokation

Der Antragsteller 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 Antragsteller, den Inhaber der Domäne, 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 Antragsteller die Bestellplattform missbraucht, fahrlässig einsetzt oder sich nicht an die vorliegenden Vereinbarungs- und Nutzungsbedingungen hält
- das Zertifikat, die Person, die das Zertifikat einsetzt, oder der Server/Client, worauf das Zertifikat installiert ist, als Ursprung einer missbräuchlichen Verwendung oder einer schädlichen Software identifiziert wird
- der Inhaber, welcher das Zertifikat beantragt, oder der Server/Client, worauf das Zertifikat installiert wird, nicht identifiziert oder verifiziert werden kann, oder
- das Zertifikat aus weiterführenden Gründen als vom Antragsteller 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 Antragsteller verpflichtet sich, nach Ablauf der Gültigkeit oder nach der Revokation eines Zertifikates (insbesondere aufgrund einer Kompromittierung) den Einsatz des Zertifikates sofort zu unterlassen, oder, falls er nicht selber Inhaber des Zertifikats ist, mit dem jeweiligen 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 berechtigter Antragsteller

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

Verantwortung / Haftung

Der Antragsteller ist dafür verantwortlich, dass die (EV) SSL 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 (EV) SSL/TLS Authentisierungszertifikaten» und den «CA/Browser Forum Guidelines» beantragt und genutzt werden. Ein Verstoss gegen diese Vorgabe hat den Entzug der Zugangsberechtigung zur Bestellplattform, eine Revokation der vom Antragsteller bestellten Zertifikate und weitere administrative und juristische Massnahmen zur Folge. Der Antragsteller trägt die Verantwortung für alle durch ihn bestellten 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.

Wenn der Antragsteller nicht selber Zertifikatsinhaber ist, sondern das Zertifikat in Erfüllung seines amtsinternen Aufgaben-/Zuständigkeitsbereichs berechtigterweise für eine andere Person aus seinem Amt beantragt, ist er dazu verpflichtet, die Verpflichtungen aus diesen Vereinbarungs- und Nutzungsbedingungen (EV) SSL/TLS sowie aus den vorgenannten Guidelines schriftlich auf den jeweiligen Zertifikatsinhaber zu überbinden.

Änderungen der Vereinbarungs- und Nutzungsbedingungen

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

Anerkennungs- und Einverständniserklärung

Der Antragsteller nimmt zu Kenntnis, dass der CSP die Berechtigung zur Antragstellung 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 Antragsteller bezeugt mit seiner Unterschrift, dass er diese Vereinbarungs- und Nutzungsbedingungen gelesen und verstanden hat und diese akzeptiert.

Ort, Datum: _____ Digitale Signatur: _____