Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

**Ufficio federale dell'informatica e della telecomunicazione UFIT**
Betrieb
Betrieb Frontend Services
PKI

# Autorizzazione per l'acquisizione di certificati (EV) SSL della Swiss Government PKI V2.0

**Il certificato di classe B personale è necessario per l'attivazione dell'autorizzazione!**

La persona menzionata in seguito richiede l'autorizzazione per l'acquisizione di certificati (EV) SSL (certificati per server e clienti) della *Swiss Government PKI* per le domain in seguito:

| **Richiedente** | |
|---|---|
| Titolo | |
| Nome, cognome, suffisso | |
| Cantone / ufficio | |
| Indirizzo completo | |
| N° di telefono | |
| Indirizzo e-mail | |

## Livello di verifica[1]:

**Esame:** **OV** ◯ **EV** ◯ (Non ancora disponibile)

**Conferma:**
Attivando il casello a destra, confermate die aver letto ed accettato le direttive (pagine seguenti), e le condizioni contrattuali della Swiss Government PKI: ☐

## Domain *admin.ch*:

Si esige la firma del proprietario della domain ***admin.ch*** (René Staudenmann OFIT)***:***

| **Il richiedente ha il diritto di acquisire certificati SSL per la domain admin.ch:** | |
|---|---|
| Firma del proprietario della domain ***admin.ch*** | |

[1] **OV:** *Organization Validated*: L'esame d'autorizzazione è effettuato a livello d'organizzazione.

**EV:** *Extended Validation*: Per la verifica dell'autorizzazione si effettua un esame approfondito della domain, dell'organizzazione e della persona richiedente. È necessaria una lettera d'autorizzazione dell'organizzazione. Certificati rilasciati con un'autorizzazione estesa si riconoscono alla linea verde nella URL. Per informazioni dettagliate si consulti le direttive della SG-PKI.

# Domain al di fuori della admin.ch:

Per le domain seguenti, i(l) proprietari(o) conferma(no) con la loro firma che:

1. Il richiedente è autorizzato ad acquisire certificati SSL presso la Swiss Government PKI per le domain menzionate in basso.
2. Il Proprietario della domain ha preso nota della CP/CPS (Certificate Policy and Certification Practice Statement) della „Swiss Government Root CA III". http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf
3. La Swiss Government PKI è autorizzata a rilasciare certificati SSL per i server menzionati nelle domain in basso.

| Domain | Luogo, data | Firma del titolare della domain secondo il registro *WhoIs* |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

| **Richiedente**<br>Nome, cognome: /Funzione: | **Data:** | **Firma: (elettronica)** |
|---|---|---|
| / | | |

Grazie per inviare il modulo completato e firmato all'indirizzo postale in basso. I moduli firmati elettronicamente vogliano essere inviati all'indirizzo e-mail: pki-info@bit.admin.ch.



Ufficio federale dell'informatica e della telecomunicazione UFIT
SwissGov-PKI Order Manager
Monbijoustrasse 74
CH-3003 Berna

# Direttive concernenti l'acquisizione di certificati (EV) SSL/TLS

## Spiegazioni relative all'acquisizione e all'impiego di certificati (EV) SSL/TLS della Swiss Government PKI

V1.0, 24.06.2016

## 1 Scopo dei certificati (EV) SSL/TLS

### Scopo

L'obiettivo principale dei certificati (EV) SSL/TLS consiste nell'autenticazione affidabile dei server. Esistono diverse varianti dei certificati (Server Authentication, Client Authentication e Server/Client Authentication). I certificati (EV) SSL/TLS sono emessi esclusivamente per sistemi aventi un Fully Qualified Domain Name (FQDN).

### Esclusione dallo scopo

I certificati (EV) SSL/TLS servono esclusivamente allo scopo sopracitato e non forniscono nessun'altra spiegazione, assicurazione o garanzia. In particolare, i certificati (EV) SSL/TLS non garantiscono che:

- grazie ai certificati i sistemi funzionino in modo corretto;
- il gestore e il contenuto del server menzionati nel certificato si attengano alle prescrizioni legali vigenti, oppure
- il gestore e il contenuto del server menzionati nel certificato siano affidabili e che il gestore si comporti adeguatamente nel contesto lavorativo.

## 2 Conferme

Al momento dell'emissione di un certificato (EV) SSL/TLS la Swiss Government PKI (SG-PKI) conferma quanto segue:

- **Validità legale**: il richiedente del certificato (EV) SSL/TLS, il relativo titolare del dominio e l'organizzazione costituiscono soggetti giuridici e sono registrati ufficialmente;
- **Identità:** il dominio e l'organizzazione del server e dell'OID menzionati nel certificato (EV) SSL/TLS corrispondono a quelli indicati nei registri pubblici e sono rappresentati da una o più persone fisiche responsabili e identificabili;
- **Autorizzazione:** la SG-PKI ha intrapreso tutti i passi necessari e ragionevolmente esigibili per accertare che il richiedente del certificato (EV) SSL/TLS sia autorizzato ad acquisirlo per il dominio e l'organizzazione;
- **Esattezza dei dati:** la SG-PKI ha intrapreso tutti i passi necessari e ragionevolmente esigibili per garantire che i dati e le informazioni contenute nel certificato siano corretti;
- **Condizioni contrattuali e d'impiego:** il richiedente del certificato (EV) SSL/TLS ha letto, accettato e firmato le *condizioni contrattuali e d'impiego EV SSL/TLS della Swiss Government PKI*;
- **Stato:** la SG-PKI rende lo stato del certificato e le informazioni sulla validità o la revoca accessibili online 24 ore su 24. Rispetta inoltre le disposizioni legali e le direttive del CA/Browser Forum;
- **Revoca:** la SG-PKI si attiene alle direttive del CA/B Forum e alle proprie CP/CPS. All'occorrenza può revocare immediatamente il certificato (EV) SSL/TLS basandosi sulle *condizioni contrattuali e d'impiego EV SSL/TLS*.

## 3 Linee di condotta

Tutte le vigenti disposizioni legali, linee di condotta (compresi i CP/CPS) e direttive concernenti i certificati (EV) SSL/TLS sono pubblicate sul sito Web della SG-PKI: https://www.bit.admin.ch/adminpki/00240/00241/05913/index.html?lang=de.

## 4 Contenuto e validità del certificato (EV) SSL/TLS

### Contenuto

Il certificato (EV) SSL/TLS contiene le seguenti informazioni:

- Autore (CSP) e CA emittente;
- Certificato root CA della CA emittente;
- Linea di condotta vigente;
- Data di emissione e di scadenza del certificato;
- Numero di serie del certificato;
- CRL e OCSP;
- Uditori della CA;
- OID dell'organizzazione;
- FQDN;
- Codice Paese;
- Stato, Cantone o luogo dell'organizzazione.

### Validità

I certificati (EV) SSL/TLS sono validi al massimo per 3 anni.

# 5 Acquisizione di certificati (EV) SSL/TLS

## Acquisizione

Per acquisire un certificato (EV) SSL/TLS devono essere soddisfatti i seguenti requisiti:

- Certificato di classe B valido, emesso a nome del richiedente;
- *Modulo di autorizzazione per certificati (EV) SSL/TLS della Swiss Government PKI* compilato e sottoscritto con firma digitale;
- *Condizioni contrattuali e d'impiego EV SSL/TLS* sottoscritte con firma digitale;
- *Authorization Letter by Organization (EV) SSL* debitamente firmata.

## Esclusione dall'acquisizione

In linea di principio non vengono emessi certificati (EV) SSL/TLS per server senza FQDN (ad es. indirizzi IP) o metacaratteri (ad es. **.bit.admin.ch*).

## Identificazione

L'identificazione del richiedente avviene mediante i processi dei certificati SG-PKI della classe B. Per emettere un certificato (EV) SSL/TLS il richiedente deve disporre di un certificato valido. Il modulo di autorizzazione per acquisire certificati deve essere firmato con il certificato personale di classe B. Per ogni dominio il richiedente deve essere autorizzato per scritto dal relativo titolare. Attraverso i processi della SG-PKI e il proprietario del dominio viene verificato se il richiedente è autorizzato ad acquisire certificati per un determinato dominio. Dopo la validazione positiva della firma, dell'autorizzazione, del FQDN, dell'OID o dell'organizzazione e della *Certificate Signing Request* (CSR) viene effettuata l'identificazione dell'organizzazione e della persona e quindi l'emissione e la trasmissione del certificato.

## Verifica

Per verificare i certificati della Swiss Government PKI si consultano registri pubblici (www.whois.com; www.firestorm.ch ecc.), registri federali ed esterni (Admin-Directory, www.uid.admin.ch, FUSC) e la banca dati interna della SG-PKI per richiedenti autorizzati. Le persone di riferimento indicate nel modulo, in particolare i proprietari dei domini, vengono contattate per telefono, per scritto o invitate a presentarsi di persona al fine di verificare l'autenticità della firma sul modulo[1].

## Carattere vincolante

Il modulo di autorizzazione e le *condizioni contrattuali e d'impiego EV SSL/TLS* devono essere firmati e trasmessi in forma elettronica mediante un certificato SG-PKI di classe B.

# 6 Protezione della chiave privata e del certificato

## Trasferibilità

Il certificato (EV) SSL/TLS viene emesso per un server o client specifico e non è trasferibile.

## Chiave privata

Il richiedente s'impegna a prendere tutte le misure adeguate per garantire in qualsiasi momento l'integrità della chiave privata e la sicurezza nell'accesso al certificato. La chiave privata e il certificato non possono essere resi accessibili a terzi. Ciò non vale nel caso in cui il richiedente non è il titolare del certificato, ma chiede legittimamente l'emissione del certificato per un'altra persona dell'ufficio o del dipartimento nell'ambito di sua competenza interna. In questo caso il richiedente deve vincolare in forma scritta anche il relativo proprietario del certificato agli impegni di cui alle condizioni contrattuali e d'impiego EV SSL/TLS e alle presenti direttive.

## Obbligo di comunicazione

L'eventuale perdita del certificato deve essere comunicata senza indugio alla SG-PKI attraverso il Service Desk dell'UFIT (servicedesk@bit.admin.ch) che in seguito blocca il certificato e lo pubblica elettronicamente su una lista di blocco pubblica. Per il rinnovo di un certificato EV SSL/TLS si applica la procedura della prima emissione.

# 7 Revoca

La revoca deve essere richiesta presso la SG-PKI attraverso il Service Desk dell'UFIT con l'indicazione dei motivi di revoca.

# 8 Conferma

Contrassegnando il campo «Conferma» nel modulo di autorizzazione, il richiedente conferma di aver letto, compreso e accettato le relative direttive. Nel contempo si attiva il campo di firma in cui occorre firmare il modulo in forma elettronica con un certificato SG-PKI di classe B. In caso di domande rivolgersi alla SG-PKI all'indirizzo: pki-info@bit.admin.ch.

[1] **Certificati OV (SG-PKI Policy OIDs 2.16.756.1.17.3.62.1/2.16.756.1.17.3.62.2)**
In caso di certificati *Organisation Validated (OV)* si verifica l'organizzazione richiedente. Il nome dell'organizzazione figura nel certificato.

**Certificati EV (SG-PKI Policy OIDs 2.16.756.1.17.3.62.4/2.16.756.1.17.3.62.5)**
I certificati *Extended Validation (EV)* sono i più sicuri per l'utente. Richiedono un maggior onere dalla CA per validare la richiesta. Sono necessari ulteriori documenti per poter emettere un certificato EV.

**NON CLASSIFICATO**

# Condizioni contrattuali e d'impiego (EV) SSL/TLS

## per l'acquisizione di certificati di autenticazione (EV) SSL della Swiss Government PKI delle autorità federali della Confederazione Svizzera

V1.0, 02.06.2016

Nel suo ruolo di *Certification Service Provider* (CSP), la Swiss Government PKI gestisce, su incarico dell'Organo direzione informatica della Confederazione (ODIC), l'infrastruttura a chiave pubblica (*Public Key Infrastructure*, PKI) delle autorità federali della Confederazione Svizzera. Tra le prestazioni standard fornite dall'ODIC, rientra anche l'emissione di *certificati di autenticazione di classe C SSL/TLS* e di *certificati di autenticazione di classe C EV SSL/TLS* (qui di seguito certificati [EV] SSL) come pure il rilascio di *autorizzazioni per acquisire* siffatti certificati. L'emissione, l'acquisizione e l'impiego dei certificati (EV) SSL della Swiss Government PKI sottostanno alle presenti condizioni contrattuali e d'impiego. Ogni anno la Swiss Government PKI (SG-PKI) adegua queste condizioni alle prescrizioni legali vigenti e alle direttive del CA/B Forum (*CA/Browser Forum Guidelines*[1]). Quest'ultime costituiscono parte integrante delle presenti condizioni. Le versioni in vigore delle condizioni contrattuali e d'impiego e delle direttive del CA/B Forum sono pubblicate sul sito: https://www.bit.admin.ch/adminpki/00240/00241/05913/05914/index.html?lang=de (disponibile in francese e in tedesco).

Occorre inoltre tenere conto delle direttive della Swiss Government PKI concernenti l'acquisizione di certificati (EV) SSL/TLS di classe C. Queste devono essere accettate separatamente in occasione dell'ordinazione dell'autorizzazione per acquisire i certificati nonché in occasione di qualsiasi adeguamento di tali autorizzazioni.

### Esattezza e completezza delle informazioni

Il sottoscritto autorizzato ad acquisire i certificati (EV) SSL (qui di seguito sottoscritto[2]) s'impegna a fornire al CSP informazioni esatte e complete e a comunicare eventuali cambiamenti. Deve in particolare provvedere affinché tutti i dati e le informazioni, soprattutto il *Fully Qualified Domain Name* (FQDN) e la registrazione dell'organizzazione (O=*Organization*), Unità organizzativa (OU=*Organization Unit*), e del luogo (L=*Location*), siano indicati in maniera esatta e completa nel *Certificate Signing Request* (CSR). Il sottoscritto è inoltre tenuto a informare il CSP qualora la sua funzione o il suo settore di competenza cambi in modo significativo.

### Protezione dei certificati e dell'accesso alla piattaforma di ordinazione

I certificati (EV) SSL possono essere emessi per i server (web) o i client. I dati relativi al sottoscritto sono archiviati presso la Swiss Government PKI. Il sottoscritto s'impegna a prendere tutte le misure adeguate per garantire in qualsiasi momento la sicurezza nell'accesso, la confidenzialità e la protezione dall'impiego abusivo della piattaforma di ordinazione. La piattaforma non deve in nessun caso essere resa accessibile a terzi non autorizzati. Inoltre può e deve essere impiegata esclusivamente per scopi legati alla richiesta di certificati.
Nemmeno la chiave privata può essere resa accessibile a terzi. Ciò non vale nel caso in cui il sottoscritto non è il titolare del certificato, ma chiede legittimamente l'emissione del certificato per poi trasmetterlo a un'altra persona, conformemente al suo compito o alla sua competenza.
Il sottoscritto risponde di qualsiasi danno causato dalla trasmissione a terzi non autorizzati dei dati di accesso alla piattaforma di ordinazione o dalla trasmissione dei certificati e delle chiavi a lui affidati e degli eventuali media pertinenti.
Il CSP si riserva il diritto di revocare, senza preavviso, l'autorizzazione di accesso alla piattaforma di ordinazione già in caso di un sospetto concreto di abuso, di accesso non autorizzato o di trasmissione a terzi non autorizzati dei dati di accesso, dei certificati e delle chiavi.

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

[2] Per una migliore leggibilità nella designazione delle persone le presenti condizioni menzionano unicamente la forma maschile.

**Impiego dei certificati e della piattaforma di ordinazione basata sul web**

Il sottoscritto s'impegna a garantire che i certificati e la piattaforma di ordinazione vengano impiegati esclusivamente per scopi autorizzati e legali. È in particolare vietato ordinare intenzionalmente certificati contenenti informazioni false o inesatte. Inoltre, i certificati sono emessi unicamente per i domini esplicitamente autorizzati dai relativi titolari (modulo di autorizzazione firmato). Il sottoscritto garantisce altresì di conoscere il contenuto, lo scopo e l'effetto dei certificati da lui richiesti. La piattaforma di ordinazione, i certificati (EV) SSL e le rispettive chiavi private devono essere impiegati esclusivamente per operazioni (aziendali) autorizzate e nel rispetto delle prescrizioni legali vigenti, delle presenti condizioni contrattuali e d'impiego e delle direttive del CA/B Forum.

**Comunicazione e revoca**

Il sottoscritto s'impegna a chiedere al CSP immediatamente la revoca del certificato se:

- sussiste il sospetto concreto di un impiego abusivo o errato del certificato;
- le informazioni contenute nel certificato non sono aggiornate o esatte o non lo saranno più prossimamente;
- sussiste il sospetto concreto di un impiego abusivo o di trasmissione illecita dei dati di attivazione o della chiave privata in relazione alla chiave pubblica connessa al certificato;
- sussiste il sospetto concreto che il certificato sia impiegato per compromettere il CSP o che il relativo impiego possa farlo.

In caso di sospetto di trasmissione illecita o di abuso di un certificato, è necessario seguire senza indugio le indicazioni del CSP. Per necessità legate alla sicurezza e se ammesso dal punto di vista della protezione dei dati, il CSP può trasmettere ad altri servizi competenti, ad altri CSP, a imprese e gruppi industriali, compreso il CA/B Forum, i dati concernenti il sottoscritto, il titolare del dominio, il certificato e altre informazioni direttamente correlate, se:

- il sottoscritto impiega la piattaforma di ordinazione in modo abusivo, negligente o senza rispettare le presenti condizioni contrattuali e d'impiego;
- il certificato, la persona che lo impiega o il server/client sul quale il certificato è installato viene identificato come origine di un impiego abusivo o di un software dannoso;
- il titolare che richiede il certificato o il server/client sul quale il certificato è installato non può essere identificato o verificato; o
- il certificato è stato revocato per motivi diversi da quelli indicati dal sottoscritto (ad es. compromissione ecc.).

Per ragioni di tracciabilità il CSP archivia tutte le informazioni legate alla revoca.

**Fine dell'impiego di un certificato**

Alla scadenza della validità o dopo la revoca di un certificato (in particolare a causa di una compromissione), il sottoscritto deve cessare immediatamente di impiegarlo oppure, se non è il titolare, contattare il rispettivo titolare e intraprendere tutti i passi necessari e ragionevolmente esigibili per impedire immediatamente un ulteriore impiego del certificato.

**Fine dell'attività che autorizza di richiedere i certificati**

Il sottoscritto s'impegna a comunicare alla SG-PKI la fine della sua attività o del suo ruolo che l'autorizza a richiedere i certificati (ad es. modifica del rapporto di lavoro o della funzione) e a chiedere, mediante il relativo modulo, il blocco dei suoi diritti d'accesso alla piattaforma di ordinazione basata sul web.

**Responsabilità**

Il sottoscritto è responsabile affinché i certificati (EV) SSL e le relative chiavi private vengano richiesti e impiegati soltanto nel rispetto delle prescrizioni legali vigenti, delle direttive delle presenti condizioni contrattuali e d'impiego, delle direttive della Swiss Government PKI concernenti l'acquisizione di certificati di autenticazione (EV) SSL/TLS e delle direttive del CA/B Forum. Un'infrazione a queste prescrizioni comporta il ritiro dell'autorizzazione di accesso alla piattaforma di ordinazione, la revoca dei certificati ordinati dal sottoscritto e altre misure di natura giuridica e amministrativa. Il sottoscritto è responsabile di tutti i certificati da lui ordinati nonché di eventuali danni e conseguenze che ne risultano, qualora possa essere dimostrato che ha violato intenzionalmente o per grave negligenza le prescrizioni legali vigenti, le direttive contenute nelle presenti condizioni o le altre direttive summenzionate.

Se il sottoscritto non è il titolare del certificato, ma chiede legittimamente l'emissione del certificato per un'altra persona dell'ufficio o del dipartimento, conformemente al suo compito o alla sua competenza

interna, deve vincolare in forma scritta anche il relativo titolare del certificato agli impegni di cui alle presenti condizioni contrattuali e d'impiego e alle summenzionate direttive.

**Modifiche delle condizioni contrattuali e d'impiego**

Eventuali modifiche o adeguamenti successivi delle presenti condizioni contrattuali e d'impiego sono considerati accettati se entro 30 giorni dalla comunicazione delle disposizioni modificate il sottoscritto non presenta alcuna opposizione scritta.

**Dichiarazione di riconoscimento e di consenso**

Il sottoscritto prende atto del fatto che il CSP revoca immediatamente l'autorizzazione di richiesta già in caso di un sospetto fondato di abuso, di inosservanza delle presenti condizioni contrattuali e d'impiego o di un'altra violazione delle prescrizioni legali vigenti (ad es. frode, divulgazione di certificati compromessi).
Il sottoscritto conferma con la propria firma di aver letto, compreso e accettato le presenti condizioni.

Luogo, data: _____ Firma: