



25.06.2025

# Condizioni contrattuali e di utilizzo per i certificati avanzati di classe B (per persone fisiche) della Swiss Government PKI

Entrata in vigore: 01.08.2025

V2.0

La Swiss Government PKI dell'Ufficio federale dell'informatica (UFIT), nel suo ruolo di Trust Service Provider (TSP), gestisce per conto del [TDI](#) (Trasformazione digitale e gestione delle TIC) la PKI (Public Key Infrastructure) delle autorità federali della Confederazione Svizzera. I certificati di classe B per la firma avanzata secondo la Legge sulla firma elettronica ([FiEle](#)), per l'autenticazione e la crittografia sono definiti nell'ambito del servizio standard «SD005 - Modello di mercato servizio standard: gestione delle identità e degli accessi (IAM)».

L'ottenimento e l'utilizzo di questi certificati della Swiss Government PKI (SG-PKI) sono soggetti alle disposizioni del presente documento. Queste vengono verificate annualmente dalla SG-PKI e, se necessario, adeguate alle disposizioni legali vigenti e ai requisiti normativi relativi alle infrastrutture a chiave pubblica.

La versione attualmente valida è pubblicata su [Swiss Government PKI](#). Tutti i titolari di tali certificati saranno informati tramite e-mail della pubblicazione di una versione aggiornata del presente documento. 30 giorni dopo l'invio di tale informazione, la nuova versione si considera tacitamente accettata, salvo che nel frattempo non venga emesso un ordine di revoca immediata dei certificati.

**Nota:** Il [glossario](#) è disponibile sulla homepage della PKI.

## Indice

|   |   |
|---|---|
| Condizioni contrattuali e di utilizzo per i certificati avanzati di classe B (per persone fisiche) della Swiss Government PKI | 1 |
| 1. Completezza e accuratezza delle informazioni   | 2 |
| 2. Protezione delle chiavi private e dei certificati  | 2 |
| 3. Accettazione del certificato   | 3 |
| 4. Utilizzo dei certificati   | 3 |
| 5. Segnalazione e revoca  | 4 |
| 6. Cessazione dell'utilizzo dei certificati   | 5 |
| 7. Responsabilità / Garanzia  | 5 |
| 8. Basi giuridiche, validità dei documenti e parti integranti del contratto   | 5 |
| 9. Contenuto e validità dei certificati avanzati di classe B  | 5 |
| 10. Richiesta e ottenimento dei certificati di classe B   | 6 |
| 11. Dichiarazione di riconoscimento e consenso  | 7 |

## 1. Completezza e accuratezza delle informazioni

Il titolare naturale dei certificati di classe B della Swiss Government PKI (di seguito denominato «titolare<sup>1</sup>») si impegna a fornire al TSP, in qualsiasi momento, tutte le informazioni necessarie per il processo di emissione e per il contenuto del certificato in modo corretto e completo. Grazie a meccanismi di controllo e sicurezza avanzati durante il processo di emissione del certificato, l'identità del richiedente (di seguito denominato «richiedente<sup>2</sup>») viene verificata con un elevato livello di sicurezza. Tra le altre cose, prima dell'emissione del certificato, il richiedente deve essere identificato di persona mediante un documento di viaggio valido per l'ingresso in Svizzera. Il certificato è indissolubilmente legato al titolare.

Il nome/i nomi, il cognome/i cognomi, il suffisso e l'indirizzo e-mail della titolare sono sempre riportati nel certificato (iscrizione nella Admin-Directory della Confederazione). Ulteriori dati personali quali la data di nascita e le passphrase di revoca, nonché la scansione del documento d'identità valido vengono registrati e memorizzati presso la SG-PKI.

La titolare è tenuta a informare il TSP non appena i dati riportati nel certificato subiscono modifiche.

## 2. Protezione delle chiavi private e dei certificati

Le chiavi private dei certificati di classe B sono memorizzate su una Smartcard personale. Per attivare le chiavi private per la creazione di una firma elettronica, l'autenticazione e/o la decrittografia, il titolare deve utilizzare il PIN della Smartcard di classe B. Il PIN della Smartcard può essere, se necessario, modificato autonomamente dal titolare nel Safenet Authentication Client (SAC). Un PIN può essere utilizzato solo per una Smartcard; se una Smartcard viene sostituita, è necessario scegliere un nuovo PIN. Questo PIN non deve essere utilizzato per altri scopi (ad es. Postcard). Il PIN non deve essere comunicato a terzi e deve essere modificato non appena si sospetta che un'altra persona ne sia venuta a conoscenza. I certificati (e quindi il supporto del certificato: Smartcard, chiavetta USB, ecc.) devono essere protetti con un PIN di almeno 6 cifre (max. 14 caratteri), dove sono ammessi PIN puramente numerici e PIN misti. I caratteri speciali non sono esplicitamente ammessi nel PIN dei certificati di classe B. Il titolare si impegna a prendere tutte le precauzioni adeguate per garantire il controllo esclusivo, la riservatezza e la protezione contro la perdita e l'uso improprio delle chiavi private e dei relativi dati di attivazione (PIN) e della Smartcard. Le chiavi private dei certificati possono e devono essere utilizzate solo in relazione ai certificati e solo per gli scopi specificati nei certificati (firma, autenticazione, crittografia).

Se la titolare dimentica il PIN o lo inserisce più volte in modo errato, può impostare un nuovo PIN rivolgendosi a un superutente autorizzato alla reimpostazione del PIN da SG-PKI e facendosi identificare da quest'ultimo. L'identificazione può avvenire tramite una passphrase stabilita al momento dell'emissione e la risposta corrispondente. Il superutente per il reset del PIN rilascia un eTicket e la titolare,

---

<sup>1</sup> Il termine «titolare» indica la persona fisica a cui è stato rilasciato il certificato.

<sup>2</sup> Il termine «richiedente» indica la persona fisica che richiede il certificato per sé stessa.

dopo aver effettuato una nuova identificazione presso un utente per il reset del PIN (PRU) designato dall'organizzazione, può impostare un nuovo PIN.

Le chiavi private dei certificati di classe B non sono trasferibili e non devono in nessun caso essere rese accessibili a terzi non autorizzati<sup>3</sup>. Le chiavi private dei certificati di classe B sono contrassegnate come non esportabili sul supporto del certificato (ad es. smartcard).

La titolare è responsabile per qualsiasi danno causato dalla divulgazione a terzi delle chiavi private, dei dati di accesso alla chiave o dei dati di attivazione o della Smartcard ad essa collegati.

Le Smartcard utilizzate soddisfano i requisiti della Legge sulla firma elettronica (FiEle). Anche tutti i componenti devono essere stati approvati dal BIT. Un elenco dei componenti approvati è pubblicato alla pagina Swiss Government PKI [Classe B - Standard, direttive e basi legali](#).

Il Trust Service Provider (TSP) si riserva il diritto di revocare immediatamente i certificati in caso di sospetto concreto di abuso o accesso non autorizzato alla chiave privata senza preavviso.

### 3. Accettazione del certificato

La titolare verifica il contenuto del certificato al momento della ricezione e garantisce che sia corretto per tutta la durata del certificato.

### 4. Utilizzo dei certificati

I certificati avanzati di classe B per persone fisiche possono essere utilizzati per i seguenti scopi:

- Firma affidabile dei dati. Ciò garantisce l'autenticità e l'integrità dei dati.
- Crittografia dei dati. Viene garantita la riservatezza dei dati.
- Autenticazione delle persone. Il certificato fornisce ai componenti di controllo, come ad esempio i portali di accesso, un'identità sicura del titolare.

La titolare garantisce di essere a conoscenza del contenuto, dello scopo e dell'effetto dell'utilizzo dei certificati di classe B. Si impegna a utilizzare i certificati di classe B e le relative chiavi private esclusivamente per operazioni autorizzate e nel rispetto delle disposizioni di legge vigenti (cfr. cap 8 Basi giuridiche, validità dei documenti e parti integranti del contratto) e delle disposizioni del presente documento.

I certificati avanzati di classe B soddisfano esclusivamente lo scopo sopra indicato e non forniscono ulteriori informazioni, assicurazioni o garanzie. In particolare, i certificati avanzati di classe B non garantiscono che il titolare agisca in modo corretto e legale nell'utilizzo del certificato.

Inoltre, i certificati avanzati di classe B non garantiscono che:

- la titolare indicata nel certificato è attivamente coinvolta nelle attività commerciali;
- la titolare indicata nel certificato rispetta le disposizioni di legge vigenti;
- la titolare indicata nel certificato è affidabile e agisce in modo serio nell'ambito commerciale; oppure

---

<sup>3</sup> Nel contesto del presente documento, il termine «terzi non autorizzati» indica qualsiasi altra persona che non sia stata autorizzata a recuperare informazioni relative al certificato a seguito di un decesso o di un procedimento giudiziario.

- la titolare indicata nel certificato possiede le competenze professionali, tecniche, organizzative o di altro tipo necessarie per utilizzare correttamente il presente certificato.

Al momento del rilascio iniziale di un certificato avanzato di classe B, la Swiss Government PKI conferma quanto segue:

- *Esistenza giuridicamente valida*: il titolare indicato nel certificato esiste come persona fisica e dispone di una voce personale nella directory amministrativa della Confederazione.
- *Identità*: il nome del titolare indicato nel certificato corrisponde al nome riportato nel suo documento d'identità valido.
- *Autorizzazione*: la SG-PKI ha adottato tutte le misure necessarie e ragionevoli per verificare che il titolare indicato nel certificato sia autorizzato a ricevere il certificato.
- *Correttezza dei dati*: la SG-PKI ha adottato tutte le misure necessarie e ragionevoli per garantire che tutti i dati e le informazioni contenuti nel certificato siano corretti.
- *Stato*: la SG-PKI rende disponibile online 24 ore su 24, 7 giorni su 7, lo stato del certificato e le informazioni relative alla sua validità/revoca, soddisfacendo così i requisiti di legge.

In caso di domande o problemi relativi all'utilizzo dei certificati, è possibile contattare il servizio di assistenza locale o il servizio di assistenza BIT (tel.: +41 (0)58 465 88 88). Per una procedura di reclamo o per domande relative al presente documento, è possibile contattare SG-PKI all'indirizzo e-mail [pki-info@bit.admin.ch](mailto:pki-info@bit.admin.ch).

## 5. Segnalazione e revoca

Il titolare si impegna a cessare immediatamente l'utilizzo dei certificati e delle relative chiavi private e a richiedere immediatamente la revoca (dichiarazione di invalidità) dei certificati al TSP (ad es. Local Registration Authority Officer/LRAO della SG-PKI nell'organizzazione del titolare) qualora:

- esistono fondati dubbi che un certificato sia stato utilizzato per attività sospette (compromissione/uso improprio dei dati di attivazione, del certificato di autenticazione, del certificato di firma o del certificato di crittografia);
- le informazioni contenute nei certificati non sono più corrette o accurate, o lo saranno nel prossimo futuro;
- si nota un'eventuale perdita della Smartcard.

È necessario seguire immediatamente le istruzioni del TSP, in particolare in caso di sospetto compromissione o abuso dei certificati.

La titolare può richiedere la revoca personalmente o per telefono. Il TSP o la persona da lui incaricata (ad es. LRAO) identificherà la titolare.

Ulteriori persone autorizzate a richiedere la revoca devono presentare la richiesta per iscritto utilizzando il modulo di revoca (elettronico). Le persone autorizzate sono:

- la titolare stessa
- i superiori gerarchici della titolare
- il responsabile SG-PKI
- il responsabile della sicurezza SG-PKI
- il responsabile LRAO competente della SG-PKI
- il responsabile della sicurezza informatica dell'unità organizzativa (ISBO) o del dipartimento (ISBD)
- Collaboratori dell'HR (servizio del personale) competente per il titolare

Subito dopo il blocco è possibile richiedere al TSP il rilascio di nuovi certificati. Il processo di rilascio dei nuovi certificati è identico a quello della prima emissione.

Le informazioni relative all'identificazione, al rilascio dei certificati e alla revoca vengono registrate dal TSP per motivi di tracciabilità e trattate e conservate in conformità con le disposizioni di legge. Il periodo di conservazione di 11 anni decorre dalla scadenza dei certificati o dalla loro dichiarazione di invalidità.

Se necessario per motivi di sicurezza e consentito dalla normativa sulla protezione dei dati, il TSP può trasmettere dati relativi al titolare, ai certificati e altre informazioni direttamente correlate ad altri organismi competenti, TSP, aziende e gruppi industriali, qualora i certificati o il titolare che li utilizza siano identificati come fonte di un uso improprio.

## 6. Cessazione dell'utilizzo dei certificati

La titolare si impegna a cessare immediatamente l'utilizzo dei certificati dopo la loro scadenza o revoca (in particolare a seguito di compromissione).

## 7. Responsabilità / Garanzia

La titolare è responsabile dell'utilizzo dei propri certificati di classe B e delle relative chiavi private esclusivamente nel rispetto delle disposizioni contenute nella sezione Utilizzo dei certificati (cap. 4) del presente documento. La violazione di tale disposizione comporta la revoca dei certificati ed eventuali ulteriori provvedimenti amministrativi e legali. La titolare è responsabile di tutte le firme, autenticazioni e crittografie da lei effettuate, nonché di eventuali danni e conseguenze derivanti da un uso non conforme alle disposizioni.

## 8. Basi giuridiche, validità dei documenti e parti integranti del contratto

Le seguenti basi giuridiche e ulteriori disposizioni costituiscono parte integrante del presente accordo di utilizzo. Sono elencate nell'ordine di priorità applicabile:

1. Legge federale sui servizi di certificazione nel settore della firma elettronica e di altre applicazioni dei certificati digitali. FiEle, SR 943.03
2. Ordinanza sui servizi di certificazione nel campo della firma elettronica e di altre applicazioni di certificati digitali. OFiEle, SR 943.032
3. Ordinanza dell'UFCOM sui servizi di certificazione nel campo della firma elettronica e di altre applicazioni di certificati digitali. RS 943.032.1  
[CP/CPS](#) Root CA I della SG-PKI
4. Il presente documento
5. Requisiti normativi per le infrastrutture a chiave pubblica

Le disposizioni di legge, le politiche e le direttive vigenti per i certificati regolamentati e avanzati di classe B sono pubblicate o collegate tramite link sul sito Internet della Swiss Government PKI [Classe B - Standard, direttive e basi legali](#).

## 9. Contenuto e validità dei certificati avanzati di classe B

I certificati della SG-PKI contengono informazioni relative a:

- Herausgeber (TSP) und ausstellender Certificate Authority (CA)
- Editore (TSP) e autorità di certificazione (CA, Certificate Authority) emittente
- Informazioni sulla CA radice (Root CA) della CA emittente
- Informazioni sulla politica applicabile
- Data di emissione e scadenza del certificato
- Numero di serie del certificato
- Informazioni relative alla CRL e all'OCSP
- Informazioni relative al titolare del certificato al momento del primo rilascio:
- Nome(i), cognome(i) e suffisso provenienti dalla directory amministrativa Admin-Directory (nome comune del titolare (CN))

- Indirizzo e-mail del titolare
- Facoltativamente, il nome utente principale (UPN)
- Chiave pubblica

I certificati hanno una validità massima di 3 anni. Prima della scadenza del periodo di 3 anni, i certificati possono essere rinnovati al massimo due volte dal titolare stesso per altri tre anni. Per il rinnovo del certificato, il titolare ha a disposizione il Renewal Wizard. Alla scadenza del terzo periodo di validità, l'ufficiale LRA deve rilasciare un nuovo certificato secondo la procedura di prima emissione. Anche in questo caso, la procedura di emissione rimane la stessa della prima emissione. È necessario presentarsi di persona con un documento di identità e i documenti necessari.

## 10. Richiesta e ottenimento dei certificati di classe B

Per ottenere certificati avanzati di classe B della SG-PKI sono necessari i seguenti documenti o registrazioni:

- Un documento di viaggio valido per l'ingresso in Svizzera (carta d'identità/passaporto) intestato alla futura titolare. La data di scadenza non deve essere superata.
- Modulo di richiesta compilato e firmato (elettronicamente, almeno con classe B) per i certificati di classe B della SG-PKI o una richiesta scritta tramite la linea dell'organizzazione o tramite il processo HR interno stabilito.
- Iscrizione personale nella directory amministrativa della Confederazione, con cognome(i), nome(i) (come indicato nel documento di viaggio), indirizzo e-mail valido e, facoltativamente, un nome utente principale (cosiddetta iscrizione UPN).
- Documento «Condizioni contrattuali e di utilizzo per i certificati avanzati di classe B (per persone fisiche) della Swiss Government PKI» (documento allegato).

L'identificazione personale del richiedente è garantita dal Local Registration Authority Officer (LRAO) di classe B della SG-PKI al momento del rilascio iniziale e al più tardi dopo la scadenza del terzo periodo di validità. In caso di rilascio decentralizzato di certificati di classe B, l'identificazione personale viene effettuata da una persona delegata dall'LRAO, il RIO (Registration Identification Officer), che inoltra la conferma dell'identificazione effettuata all'LRAO per l'approvazione della domanda. Il richiedente deve presentarsi personalmente per il rilascio del certificato. Al fine di verificare e identificare il richiedente, il documento di viaggio viene controllato dal LRAO o dal RIO al momento del rilascio per verificarne la validità, la correttezza e l'autenticità. Il LRAO e il RIO sono inoltre tenuti a confrontare l'immagine del documento con la persona che hanno davanti. Allo stesso modo, prima del rilascio di un certificato avanzato, viene verificata la plausibilità della domanda (la persona lavora effettivamente nell'unità organizzativa indicata, ha bisogno del certificato per la sua attività lavorativa quotidiana; il richiedente è autorizzato a richiedere un certificato).

Se per la presentazione della domanda sono necessarie ulteriori informazioni, la richiedente ha 10 giorni di tempo per inviarle alla SG-PKI. Trascorso tale termine, la domanda scade automaticamente.

## 11. Dichiarazione di riconoscimento e consenso

La richiedente prende atto che il TSP revoca immediatamente i certificati in caso di sospetto fondato di abuso, violazione delle disposizioni del presente documento o di qualsiasi altra violazione delle disposizioni di legge vigenti.

Con la propria firma, la richiedente attesta di aver letto e compreso il presente documento «Condizioni contrattuali e di utilizzo per i certificati avanzati di classe B (per persone fisiche) della Swiss Government PKI» e di accettare le disposizioni in esso contenute.

|                              |   |
|------------------------------|---|
| Nome, cognome (richiedente): | (classe elettronica B) Firma della richiedente:<br>Firma richiedente: |
| Luogo/Data:                  |   |