



## Lista di controllo per il rilascio dei certificati di classe B

[Swiss Government PKI - Direttive per la registrazione dei certificati di classe B per la LRA \(Local Registration Authority\) \(DdR\)](#)

→ **Capitolo No. 2.1** Processo per il rilascio dei certificati

V2.3 / 30.10.2025

**PUBLIC**

No.	Descrizione	Riferimento
<b>Passo 1 - Preparazione per il rilascio del certificato</b>		
1.1	<p>Verificare che siano ancora disponibili <b>sufficienti smartcards</b></p> <ul style="list-style-type: none"> <li>➤ <i>Se necessario, ordinare le smartcards</i></li> <li>➤ <i>Avvertenza relativa alla conservazione e allo smaltimento delle smartcards</i></li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">DdR Capitolo 5.2.3.7</a></li> <li>• <a href="#">Ordinare la Smart card - classe b</a></li> <li>• <a href="#">DdR Capitolo 3.9 und 3.11</a></li> </ul>
1.2	<p><b>Ordine</b> (e-mail firmata dall'ufficio risorse umane/superiore), ticket o <a href="#">modulo di richiesta</a> (firmato dall'utente) ricevuto?</p>	
1.3	<ul style="list-style-type: none"> <li>• La persona richiedente è autorizzata a richiedere un certificato di classe B?</li> <li>• In qualità di LRAO, si è responsabili del rilascio (stesso ramo della persona in AdminDirectory)? In qualità di LRAO, si dispone dell'autorizzazione corretta per il rilascio? <ul style="list-style-type: none"> <li>➤ <i>Se la persona richiedente non è autorizzata alla richiesta e/o non si è responsabili per lui, respingere la richiesta.</i></li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">DdR Capitolo 5.2.1</a></li> <li>• <a href="#">AdminDir</a></li> </ul>
1.4	<p>Le <b>informazioni contenute nella richiesta</b> sono complete e plausibili e il nome incluso di suffisso e l'indirizzo e-mail indicati nella richiesta corrispondono a quelli presenti nella AdminDirectory?</p> <ul style="list-style-type: none"> <li>➤ <i>Se le informazioni non sono corrette, rivolgersi al reparto Risorse umane competente e richiedere la correzione.</i></li> </ul>	<p><a href="#">DdR-Capitolo 5.2.3.1 e 5.2.3.2</a></p>
1.5	<p><b>Concordare un appuntamento</b> per il rilascio del certificato tramite l'indirizzo e-mail fornito dalla persona richiedente.</p> <ul style="list-style-type: none"> <li>• Informare la persona nell'invito all'appuntamento che dovrà portare con sé un documento di viaggio valido (carta d'identità/passaporto).</li> <li>• All'invito all'appuntamento devono essere allegati i link ai seguenti documenti; inoltre, la persona richiedente deve essere invitata a leggere il contratto di utilizzo e a prendere nota di eventuali domande:</li> </ul> <p><a href="#">Condizioni contrattuali e di utilizzo per i certificati avanzati di classe B della Swiss Government PK</a> / <a href="#">Guida rapida: Regole per il PIN delle smartcard</a> / <a href="#">Guida rapida: Possibili domande per le frasi di revoca</a></p>	<ul style="list-style-type: none"> <li>• <a href="#">DrD Capitolo 5.2.3.3</a></li> <li>• <a href="#">Identità dei richiedenti</a></li> <li>• <a href="#">Classe B - Libreria di moduli e documenti</a></li> </ul>



No.	Descrizione	Riferimento
1.6	<b>Creare un dossier dei clienti per la persona richiedente</b> (cartella digitale e/o cartacea)	<a href="#">DrD Capitolo 3.6</a>
<b>Passo 2 – Rilascio del certificato</b>		
2.1	<p>Le <b>informazioni</b> contenute nella <b>richiesta</b> corrispondono a quelle riportate nel <b>documento di viaggio</b> (carta d'identità/passaporto) e nell'<b>AdminDirectory</b>, in particolare il nome e il cognome della persona? (vedere il documento «Verifica dell'identità dei richiedenti per i certificati di classe B»)</p> <p>➤ <i>Se le informazioni non corrispondono, NON è possibile rilasciare alcun certificato. Rivolgersi al proprio reparto Risorse umane e richiedere la correzione</i></p>	<ul style="list-style-type: none"> <li>• <a href="#">DrD Capitolo 5.2.3.1 und 5.2.3.6</a></li> <li>• <a href="#">Identità dei richiedenti</a></li> </ul>
2.2	<p><b>Verificare l'autenticità dei documenti di viaggio (carta d'identità/passaporto)</b></p> <ul style="list-style-type: none"> <li>• <b>Tipo di documento di viaggio:</b> Si tratta di: <ul style="list-style-type: none"> <li>○ Una carta di identità / Passaporto? → OK</li> <li>○ Nel caso di un «permesso F», in qualità di LRAO è possibile rilasciare il certificato a questa persona richiedente solamente se è stato ricevuto dal responsabile della sicurezza del proprio ufficio/organizzazione (a livello federale si tratta dell'<a href="#">ISID/ISIU</a>) il «<a href="#">Modulo di richiesta complementare per i richiedenti con permesso F</a>» compilato.</li> </ul> </li> <li>• <b>Il documento di viaggio è valido</b> (data di scadenza)? <ul style="list-style-type: none"> <li>○ Se il documento di viaggio è scaduto (anche solo di un giorno), la persona richiedente deve richiedere un nuovo documento di viaggio. La smartcard verrà rilasciata solo con il nuovo documento di viaggio valido.</li> <li>○ Nota: è possibile richiedere un'autorizzazione speciale al Security Officer PKI tramite e-mail (<a href="mailto:pki-secoff@bit.admin.ch">pki-secoff@bit.admin.ch</a>). Tuttavia, il certificato può essere rilasciato solo dopo il rilascio di un'autorizzazione speciale (e-mail crittografata del Security Officer PKI).</li> </ul> </li> <li>• <b>Il documento di viaggio è autentico?</b> <ul style="list-style-type: none"> <li>○ Il numero della carta di identità è lo stesso sul fronte e sul retro / il numero del passaporto è lo stesso su ogni pagina?</li> <li>○ Caratteristiche dei documenti di viaggio (vedi documenti alla voce <a href="#">Identità dei richiedenti</a>).</li> <li>○ «Suono» della carta d'identità quando cade sul tavolo (il suono è diverso da quello di una carta di credito, ad esempio)</li> <li>○ Per i documenti di viaggio dell'UE, è possibile verificare le caratteristiche di sicurezza tramite <a href="#">PRADO</a>.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">DrD Capitolo 5.2.3.5</a></li> <li>• <a href="#">Identità dei richiedenti</a></li> </ul>



No.	Descrizione	Riferimento
2.3	<p><b>Identificazione della persona richiedente</b> I dati riportati nel documento di viaggio corrispondono a quelli della persona? La persona richiedente corrisponde a quella che figura sul documento?</p> <ul style="list-style-type: none"> <li>Vedi documento <a href="#">Identità dei richiedenti</a></li> <li>Confrontare il volto della persona con l'immagine riportata nel documento di viaggio (simmetria del volto)</li> <li>Altezza</li> </ul>	<ul style="list-style-type: none"> <li><a href="#">DrD Capitolo 5.2.3.5</a></li> <li><a href="#">Identità dei richiedenti</a></li> </ul>
2.4	<p><b>Digitalizzare</b> (scansionare) e salvare il <b>documento di viaggio</b> (carta d'identità/passaporto) ed eventuali altri documenti necessari.</p>	<a href="#">DrD Capitolo 5.2.3.8</a>
2.5	<p>Informare le persone richiedenti sulla scelta del PIN e della passphrase di revoca (come indicato nell'invito all'appuntamento e nelle relative guide rapide).</p>	<a href="#">DrD Capitolo 5.2.3.9</a>
2.6	<ul style="list-style-type: none"> <li>Emettere il certificato su smartcard con l'aiuto della procedura guidata WalkInWizard.</li> <li>La persona richiedente deve impostare autonomamente il PIN e la passphrase di revoca.</li> </ul>	<a href="#">DrD Capitolo 5.2.3.10</a>
2.7	<p>Informare la persona richiedente dei suoi diritti e doveri ai sensi del «<a href="#">Condizioni contrattuali e di utilizzo per i certificati avanzati di classe B (per persone fisiche) della Swiss Government PKI (V2.0)</a>», rispondere alle sue domande e far firmare il documento da parte sua.</p> <p>➤ Vedi «Punti principali (Pagina 4-5)»</p>	<ul style="list-style-type: none"> <li><a href="#">DrD Capitolo 5.2.3.11</a></li> <li><a href="#">Classe B - Libreria di moduli e documenti</a></li> </ul>
2.8	<p>La firma della persona richiedente sul «Contratto di utilizzo e condizioni d'uso Classe B» corrisponde a quella riportata sul documento di viaggio? <i>In caso contrario, chiarire il motivo.</i></p>	
2.9	<p>Consegnare alla persona richiedente la smartcard, il documento di viaggio (carta d'identità/passaporto) ed eventualmente una copia del documento «Accordo con l'utente e condizioni d'uso classe B».</p>	<a href="#">DrD Capitolo 5.2.3.12</a>
<b>Passo 3 - Documentazione (registrazione nel diario e archiviazione nel dossier del cliente)</b>		
3.1	<p>Effettuare una registrazione nel <a href="#">Journal</a> (in formato digitale e/o cartaceo)</p>	<a href="#">DrD Capitolo 5.2.3.13</a>
3.2	<p>Se necessario, cancellare dai sistemi locali i documenti di viaggio salvati, comprese le eventuali e-mail utilizzate per la loro spedizione.</p>	<a href="#">DrD Capitolo 5.2.3.14</a>
3.3	<p>Archiviare tutte le prove nel dossier cliente preparato. Si tratta di:</p> <ul style="list-style-type: none"> <li>«Accordo di utilizzo e condizioni d'uso Classe B» firmato (ultima pagina)</li> <li>Richiesta di certificato personale di Classe B o ordine HR</li> </ul>	<a href="#">DrD Capitolo 5.2.3.15 und 3.6</a>
<b>Nota: Termini di conservazione</b>		
	<p>È necessario garantire che le richieste possano essere chiaramente associate alle prove (documenti / evidenze) e che la documentazione relativa alle richieste e le prove utilizzate siano disponibili anche 11 anni dopo la scadenza del certificato. <b>Si consiglia un periodo di conservazione di 15 anni.</b></p>	<a href="#">DrD Capitolo 3.6 e 6.1</a>



## Punti principali:

### Condizioni contrattuali e di utilizzo per i certificati avanzati di classe B (per persone fisiche) della Swiss Government PKI (V2.0)

#### Capitolo 1: Completezza e accuratezza delle informazioni

- La persona titolare di un certificato di classe B (utente) deve garantire che le informazioni necessarie per il processo di emissione e il contenuto del certificato siano corrette e complete.
- L'identità della persona richiedente viene accertata tramite un'identificazione personale e una verifica del documento di viaggio.

#### Capitolo 2: Protezione delle chiavi private e dei certificati

- Le chiavi private dei certificati di classe B devono essere protette da un PIN che può essere utilizzato solo per una smart card.
- Il titolare deve adottare tutte le misure adeguate per garantire il controllo esclusivo, la riservatezza e la protezione dalla perdita e dall'uso improprio delle chiavi private e della smart card.

#### Capitolo 3: Accettazione del certificato

La persona titolare deve verificare il contenuto del certificato al momento della ricezione e assicurarsi che sia corretto per tutta la durata di validità.

#### Capitolo 4: Utilizzo dei certificati

I certificati di classe B possono essere utilizzati per

- la firma affidabile dei dati
- la crittografia dei dati e
- l'autenticazione delle persone.

La persona titolare deve garantire che i certificati e le chiavi private siano utilizzati solo per operazioni autorizzate e nel rispetto delle disposizioni di legge vigenti.

#### Capitolo 5: Segnalazione e revoca

La persona titolare

- deve informare immediatamente il Trust Service Provider (TSP), ovvero la Swiss Government PKI BIT, se sospetta un abuso o un accesso non autorizzato alla chiave privata.
- può richiedere la revoca di persona o per telefono.

Il Trust Service Provider (TSP), ovvero la Swiss Government PKI BIT, ha il diritto di trasmettere dati e informazioni ad altri organismi competenti, TSP, aziende o gruppi industriali in caso di danni.



## **Capitolo 6: Cessazione dell'utilizzo dei certificati**

La persona titolare deve cessare immediatamente l'utilizzo dei certificati dopo la loro scadenza o revoca.

## **Capitolo 7: Responsabilità**

La persona titolare

- è responsabile di garantire che i certificati di classe B e le relative chiavi private siano utilizzati solo in conformità con le disposizioni della sezione Utilizzo dei certificati.
- è responsabile di tutte le firme, autenticazioni e crittografie da lui effettuate, nonché di eventuali danni e conseguenze derivanti da un uso non conforme ai propri doveri.

## **Capitolo 8: Basi giuridiche, validità dei documenti e parti integranti del contratto**

Il documento «Accordo con l'utente e condizioni d'uso per certificati avanzati di classe B» è parte integrante delle basi giuridiche.

## **Capitolo 9: Contenuto e validità dei certificati avanzati di classe B**

I certificati della Swiss Government PKI contengono informazioni relative all'emittente, all'autorità di certificazione che li ha rilasciati, alla politica applicabile, alla data di emissione e di scadenza del certificato, al numero di serie del certificato e informazioni relative al persona titolare del certificato.

## **Capitolo 10: Richiesta e ottenimento di certificati di classe B**

Per ottenere certificati avanzati di classe B sono necessari un documento di viaggio valido per l'ingresso in Svizzera, un ordine firmato (ad es. modulo di richiesta, e-mail firmata dall'HR, ecc.), una registrazione personale nella directory amministrativa della Confederazione e un accordo di utilizzo e condizioni d'uso firmati.

## **Capitolo 11: Dichiarazione di riconoscimento e consenso**

La persona richiedente

- prende atto che il Trust Service Provider (TSP), ovvero la Swiss Government PKI BIT, revoca immediatamente i certificati in caso di fondato sospetto di abuso, violazione delle disposizioni del presente documento o altra violazione delle disposizioni di legge vigenti.
- attesta con la propria firma di aver letto e compreso il presente documento e di accettare le disposizioni in esso contenute.